

S. HRG. 114-881

**PROTECTING TRADE SECRETS: THE IMPACT
OF TRADE SECRET THEFT ON AMERICAN
COMPETITIVENESS AND POTENTIAL
SOLUTIONS TO REMEDY THIS HARM**

HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
ONE HUNDRED FOURTEENTH CONGRESS
FIRST SESSION

DECEMBER 2, 2015

Serial No. J-114-42

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

52-555

WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

ORRIN G. HATCH, Utah	PATRICK J. LEAHY, Vermont, <i>Ranking</i>
JEFF SESSIONS, Alabama	<i>Member</i>
LINDSEY O. GRAHAM, South Carolina	DIANNE FEINSTEIN, California
JOHN CORNYN, Texas	CHARLES E. SCHUMER, New York
MICHAEL S. LEE, Utah	RICHARD J. DURBIN, Illinois
TED CRUZ, Texas	SHELDON WHITEHOUSE, Rhode Island
JEFF FLAKE, Arizona	AMY KLOBUCHAR, Minnesota
DAVID VITTER, Louisiana	AL FRANKEN, Minnesota
DAVID PERDUE, Georgia	CHRISTOPHER A. COONS, Delaware
THOM TILLIS, North Carolina	RICHARD BLUMENTHAL, Connecticut

KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

KRISTINE LUCIUS, *Democratic Chief Counsel and Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Grassley, Hon. Charles E.	1
Prepared statement	31
Leahy, Hon. Patrick J.	3
Prepared statement	33

WITNESSES

Beall, Thomas R.	6
Prepared statement	35
Responses to written questions	93
Cochran, Karen	4
Prepared statement	41
Responses to written questions	98
Pooley, James	9
Prepared statement	47
Responses to written questions	104
Sandeen, Sharon K.	8
Prepared statement	86
Responses to written questions	112

APPENDIX

Items submitted for the record	125
--------------------------------------	-----

PROTECTING TRADE SECRETS: THE IMPACT OF TRADE SECRET THEFT ON AMERICAN COMPETITIVENESS AND POTENTIAL SOLUTIONS TO REMEDY THIS HARM

WEDNESDAY, DECEMBER 2, 2015

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:07 a.m., in Room 226, Dirksen Senate Office Building, Hon. Charles E. Grassley, Chairman of the Committee, presiding.

Present: Senators Grassley [presiding], Hatch, Flake, Perdue, Tillis, Leahy, Whitehouse, Klobuchar, and Coons.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman GRASSLEY. The United States is the world's leader in innovation. We have cutting-edge technologies and products that improve our daily lives. This occurs in a good measure because of our robust system of intellectual property protection and the enforcement.

Trade secrets are a lesser known but increasingly important form of intellectual property. Trade secrets allow for the legal protection of commercially valuable and proprietary information. Some famous and often cited examples of trade secrets include the formula for Coca-Cola or the recipe for Kentucky Fried Chicken.

In fact, a broad range of valuable information may be protected as a trade secret, including complex financial and technical information and computer algorithms. These trade secrets hold immense value for American companies. I would like to quote the U.S. Chamber of Commerce recently releasing a report stating that, quote, "publicly traded U.S. companies own an estimated \$5 trillion worth of trade secrets."

Trade secrets encompass an expanding portion of the firms' intellectual property portfolios, particularly in knowledge-centric areas of the economy such as technology and manufacturing.

However, the theft of trade secrets of American companies is increasing, and this hurts the U.S. economy and costs American jobs. Globalization, the emergence—emergence of the digital economy, and the increasing frequency with which trade secret thieves utilize technology and cyber capabilities has made it more difficult for trade secret owners and law enforcement to guard against theft and to fight back.

Last year, the FBI's Assistant Director of the Counterintelligence Division, Randall Coleman, testified before the Committee, quote, "economic espionage and theft of trade secrets are increasingly linked to insider threat and the growing trend of cyber-enabled trade secret theft," end of quote.

In February 2013, the White House released a report detailing, and I quote, "emerging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating," end of quote.

Then-Attorney General Eric Holder underscored these findings when he stated that, and I quote again, "There're only two categories of companies affected by trade-secret theft: those that know they have been compromised and those that don't know yet," end of quote. The result is that, according to a recent report of the Commission on the Theft of American Intellectual Property, annual losses owing to trade secret theft are likely comparable to the current annual level of U.S. exports to Asia, that being over \$300 billion. The referred-reporter further estimates that trade secret theft is responsible for the loss of two and one tenth million jobs.

Unlike other areas of intellectual property, the protection of trade secrets in the United States has mainly been a matter of State law, with 47 States having enacted some variation of the Uniform Trade Secrets Act.

While differing—differing trade secret laws share many features, State legislatures often made changes as they enacted the uniform legislation. This has led some to argue that the existing patchwork of State laws imposes difficult procedural hurdles in the many cases where a trade secret is taken across State lines. Federal law, through the Economic Espionage Act of 1996, allows Federal law enforcement authorities to criminally prosecute trade secret thieves, but it doesn't give trade secret owners a private right of action in Federal court.

As companies increasingly utilize trade secrets and as trade secret theft has soared, the FBI reports that their caseload for economic espionage and trade secret theft cases increased more than 60 percent between the 4 years of '09 and '13. In fact, some commentators point out that in the face of the FBI—what the FBI has described as an "immense threat," the Bureau's Counterintelligence Division's Economic Espionage Unit, which is tasked with investigating offenses under the EEA, does not have the resources and necessary bandwidth to bring prosecution of all trade secret cases.

Now, I've heard from a broad coalition of stakeholders, large and small, representing job-creating businesses in innovative sectors—sectors of the economy about the need for such a Federal law to protect their valuable trade secrets.

In my own State of Iowa, we've seen firsthand how some of our most innovative agricultural companies, like DuPont Pioneer, have become targets of trade secret thieves who seek to profit from the hard work and research of others. In one recent case, foreign nationals were indicted for engaging in a scheme to steal proprietary test seeds from Iowa fields to benefit a foreign agricultural company.

So, I look forward to learning more about this important issue and look forward to potential legislative solutions. I now call on Senator Leahy.

**OPENING STATEMENT OF HON. PATRICK J. LEAHY,
A U.S. SENATOR FROM THE STATE OF VERMONT**

Senator LEAHY. Thank you very much, Mr. Chairman, and the hearing today really is a topic that is essential to our Nation's economy. It's also more than just the economy; is our status as the leading source of innovation around the world.

You mentioned Iowa. I would mention also in the State of Vermont, trade secrets have protected the specialized knowledge of woodworkers who have crafted heirloom products for generations. They protect the secret recipes for Vermont craft brews, some that now have made Vermont a destination State. They also protect the closely guarded customer lists for our top tourist services. But we also have cutting-edge technologies that we are developing in Vermont in plastics, software, and green technology that we not only use in our State but export around the world. Trade secrets are relied on by countless businesses to help keep their products and services unique.

Now, I think they are especially important to small businesses. Small businesses often lack the resources that they need to seek patent protection for their inventions.

In the United States, trade secret law is the one form of intellectual property protection that currently lacks a Federal civil remedy. I think carefully written legislation will fill this gap in the law. It can provide businesses not only in Vermont but throughout the country with an improved tool to protect their intellectual property.

One priority for me has been ensuring that any seizure remedy to protect trade secrets is narrowly tailored. For example, so that actions to protect confidential information on a computer server do not unintentionally impact other content on the server that is unrelated to the theft. I want to thank Senator Coons and Senator Hatch for working with me and also with some of our top technology—technology companies to address this concern.

In 2012, we passed the Theft of Trade Secrets Clarification Act. I introduced that to close a very troubling loophole in the law, and I'm glad that the Committee is continuing its bipartisan work in this area. I have told Chairman Grassley I will work with him and, of course, with Senator Hatch and Senator Coons and all Members of the Committee on this issue because it is important to American businesses, but also just as an American, I would like to see us keep our innovative edge, and I don't want to see it eroded.

So, thank you for holding this hearing, Mr. Chairman.

Chairman GRASSLEY. We have a distinguished panel and a lot of expertise. Our first witness is Karen Cochran, chief intellectual property counsel at DuPont and DuPont Pioneer. She is responsible for leading the global intellectual property team and managing the procurement counsel and litigation of the company's IP assets. Prior to joining DuPont, she was senior patent director at AstraZeneca Pharmaceuticals. She also served as a member of the Intellectual Property Owners Association Board of Directors. She

received her bachelor's degree in chemistry, Temple University, and her law degree from Widener University School of Law.

Thomas—I don't know if it was Beell or Bell, Beall is vice president and chief intellectual property counsel for Corning Corporation. Mr. Beall has worldwide responsibility for Corning intellectual property, including all matters involving patents, trademarks, trade secrets, and copyrights. He has held numerous positions of responsibility throughout Corning, beginning in 1996 as a patent attorney for the Life Sciences Division. Prior to becoming an attorney, he worked for 4 years as an analytical chemist for Bristol-Myers Squibb. Mr. Beall served—earned his B.S. degree in biology at Syracuse University and juris doctorate from the University of New Hampshire School of Law.

Sharon Sandeen a professor of law at Hamline University School of Law in St. Paul with a focus on trade secret law. She has written numerous articles, book chapters, and books on the topic of trade secret law and information policy. She co-authored the first casebook on trade secret law in our country. Prior to teaching, Professor Sandeen practiced law for more than 15 years in Sacramento, handling a variety of intellectual property cases. Professor Sandeen received B.A. from the University of California, Berkeley, her law degree from the University of the Pacific, McGeorge School of Law, and a master's of law from the University of California, Berkeley, Boalt School of Law.

Finally, we're joined by Mr. Pooley, who is an independent lawyer specializing in trade secrets and patents. He has written extensively on the subject of trade secrets and information management. He recently completed a 5-year term as deputy director general of the World Intellectual Property Organization in Geneva, where he managed the international patent system. Before his service at the United—UN, Mr. Pooley was a lawyer in Silicon Valley for 37 years, most recently a partner in Morrison & Foerster. Mr. Pooley received a bachelor's degree from Lafayette College and a juris doctorate degree from Columbia University School of Law.

We will start with Ms. Karen, and then we'll go just in the way you are seated at the table there. Thank you very much. Please proceed. Push the red button.

**STATEMENT OF KAREN COCHRAN, GENERAL COUNSEL
AND CHIEF INTELLECTUAL PROPERTY COUNSEL,
E.I. DUPONT DE NEMOURS AND COMPANY,
WILMINGTON, DELAWARE**

Ms. COCHRAN. Good morning, Chairman Grassley and Members of the Committee. My name is Karen Cochran, associate general counsel and chief intellectual property counsel for DuPont. Thanks for the opportunity to testify on an important topic not only for my company but for the American economy.

I want to express my appreciation for the leadership of Senators Hatch and Coons for this bipartisan legislation, the Defend Trade Secrets Act. I also want to thank the Committee for your interest in trade secret protection. DuPont has extensive experience in defending our trade secrets, and we support S. 1890.

Throughout our history, DuPont's research locations have been the birthplace of innovations found in homes, farms, and busi-

nesses across the United States and around the world. Our products and technologies have included a broad spectrum, from nylon, Kevlar, and Tyvek, to seed, crop protection, and enzymes that help produce cellulosic ethanol.

The process for realizing the full potential of our innovation comprises a continuum of knowledge-based activities that can span decades. Advancement of our innovation depends on intellectual property protection, including trade secrets.

DuPont recently defended the trade secrets for one of our well-known products, Kevlar. This experience brought about our realization of the importance of S. 1890. I will share some highlights and learnings from that experience.

The technology behind DuPont Kevlar is a high-strength fiber used in a range of applications from fiber-optic cables to protective body armor, like this Kevlar vest here. Many of us recognize it. Some are probably wearing it even in the room here. Which—they protect our military and law enforcement officers not only here in the United States but around the world. DuPont invested over 50 years of research and development to master the technology that goes into these vests and all of the applications associated with this fiber. Our product quality and the manufacturing expertise that we've been able to build over that time has been unparalleled.

DuPont safeguards much of its valuable Kevlar technology as trade secrets. It was in 2006, however, that DuPont suspected that it had been a victim of trade secret theft. What we initially thought to be the misconduct of a single ex-employee turned out to be a sophisticated, large-scale trade secret theft of one of the most recognized and ground-breaking products in history. The Federal criminal investigation led to indictments of Kolon Industries. The civil matter that filed—that was filed by *DuPont v. Kolon* would not be resolved until 2015, over 9 years later.

As stated in the record, which I will read here, Kolon “undertook various efforts to learn DuPont’s trade secrets...[and] find out how DuPont...operated...to produce a high quality...fiber at a profitable and price-competitive production level,” and essentially they wanted to avoid doing the research that we had done throughout the year and short-circuit that. To accomplish their goal, they recruited former DuPont employees who had access to Kevlar trade secrets throughout the employment that they had with DuPont.

Fortunately, our case was able to access Federal court. But even there, we experienced difficulty in determining the depth of the trade secret theft that had happened. DuPont pursue allegations Kolon had destroyed evidence, and the court found that Kolon had destroyed or deleted considerable volumes of relevant evidence, and this evidence destruction created significant delays and severely hampered DuPont’s ability to defend our case.

Our experience defending Kevlar trade secrets exemplifies the importance of S. 1890 and its modernization of trade secret law. We urge the Committee to consider two points that we learned from this experience. One, the need for assured, direct access to Federal court; and, two, the need to reduce the risk of further trade secret dissemination and evidence destruction.

First, the court’s experience with litigating complex technologies for other intellectual property disputes is a valuable tool in ad-

addressing the complexities in trade secret cases. Existing State laws, unfortunately, are inadequate to address the interstate and international nature of trade secret theft. A Federal civil remedy would eliminate jurisdictional complications which occur in these cases and provide the full spectrum of options available to owners of other forms of intellectual property. Our ability to be in Federal court was a significant help in advancing the *Kolon* case.

Second, paper copies and locked cabinets are no longer the standard medium of storage for information. Information is now in portable and electronic. It can be hidden and rapidly shared, or it can be quickly deleted, as in the case with *Kolon*. The seizure provisions of S. 1890 enable a trade secret owner under limited, controlled conditions, to proactively contain a theft before it progresses and a trade secret is lost. A seizure mechanism may have prevented *Kolon's* comprehensive destruction of evidence and reduced the need for a lengthy, expensive litigation.

In conclusion, I urge the Committee to consider moving forward S. 1890, the Defend Trade Secrets Act. It would represent a gold standard for national trade secret theft globally. Again, thank you for the opportunity to testify today. I will be pleased to answer your questions. Thank you.

[The prepared statement of Ms. Cochran appears as a submission for the record.]

Chairman GRASSLEY. Thank you. Now, Mr. Beall.

**STATEMENT OF THOMAS R. BEALL,
VICE PRESIDENT AND CHIEF INTELLECTUAL
PROPERTY COUNSEL, CORNING INCORPORATED,
CORNING, NEW YORK**

Mr. BEALL. Thank you. Good morning, Chairman Grassley, Ranking Member Leahy, and Members of the Committee. My name is Tom Beall. I'm the vice president and chief intellectual property counsel to Corning Incorporated. I appreciate the opportunity to testify today about the importance of trade secret protection.

For contexts, let me give you a little background on Corning Incorporated. We have been in business as an American manufacturer for over 160 years and take great pride in our heritage as one of America's oldest and most innovative companies. We operate in 26 States and have manufacturing in 11 of those States.

Corning's strategy for success is based on two key foundations. First, we invent and innovate with tenacity, consistently investing 10 percent of our sales in research, development, and engineering. Second, we manufacture efficiently. Today we are the world's low-cost manufacturer for 80 percent of the products we make.

Here is an example. I have got a spool here of Corning's optical fiber. This is an invention that was made in 1970. We have got 50 kilometers of fiber here in front of me. This invention——

Senator LEAHY. I am sorry. How long is that?

Mr. BEALL. Fifty kilometers of fiber here. This invention, an American invention, is one that revolutionized telecommunications and forms the backbone of the internet today. The original patents are long expired. Now, there are a number of companies around the world who make this product. But we continue as the global leader. We make millions of kilometers of product every year and ship it around the globe.

So, how do you maintain a leading market position with a 45-year-old product? Two ways, one, we constantly improve the product through research and innovation; and, second, we make it more efficiently than others, which depends in large part upon trade secrets, lessons learned over the years, in fact, lessons learned over decades of production.

Therefore, our trade secrets are very valuable. Protecting our trade secrets allows us to maintain our edge, maintain profits, and keep workers on the job.

Unfortunately, trade secrets are increasingly the targets of misappropriation. Currently, the legal tools available to protect trade secrets in the United States include the Economic Espionage Act and civil remedies available under various State laws. The EEA is an essential statute, but it is not a panacea. Federal investigators and prosecutors—prosecutors have limited resources and are unable to bring charges in all cases of trade secret theft.

At the State level, most States have enacted laws modeled on the Uniform Trade Secrets Act. Although these laws may work effectively, as to intra—intrastate theft, their State border limitations restrict their usefulness in matters of interstate and international misappropriation.

As you know, today many companies operate across State and international borders. For these companies, the existing patchwork of State laws is inadequate for several reasons.

First, State secret theft often requires immediate action to preserve the value of the stolen property, particularly when a stolen trade secret is taken across State lines, or when the thief seeks to leave the country. State courts lack the tools at the Federal court's disposal to act quickly to prevent dissemination of stolen trade secrets across State lines.

Second, State courts are not able to effect prompt, nationwide service of process to seamlessly conduct cross-jurisdictional discovery.

Third, variation in State laws creates challenges for companies seeking an efficient, unified compliance plan and results in the additional unnecessary cost of investigating different State laws.

The Defend Trade Secrets Act will create a uniform standard for the protection of trade secrets nationwide, improving the efficiency and predictability of litigation and allowing companies to create one set of best practices to protect their intellectual property in every jurisdiction. With a Federal cause of action available, litigants can streamline multi-jurisdictional discovery and service of process, resulting in faster and less costly litigation. The legislation will also provide a mechanism for obtaining expedited relief when a company's trade secret is threatened with imminent destruction or dissemination. In extraordinary cases, this includes ex parte seizure of the stolen trade secret when necessary to preserve the value of the property.

The Defend Trade Secrets Act also contains safeguards to prevent abuse, including damages in the event of wrongful seizure.

We thank Chairman Grassley and Ranking Member Leahy for their leadership on trade secret issues and intellectual property more generally. We thank Senators Hatch, Coons, and Flake for introducing this important legislation and the Committee Members

who have Co-Sponsored the Defend Trade Secrets Act; Senators Durbin, Tillis, Blumenthal, Sessions, Klobuchar, and Perdue. Your consensus-oriented approach to this legislation has helped to attract support from all industry sectors, and we look forward to continuing to work together on this issue that is so important to the American economy. Thank you for the opportunity to testify today. I would be happy to take questions.

[The prepared statement of Mr. Beall appears as a submission for the record.]

Chairman GRASSLEY. Professor Sandeen.

**STATEMENT OF SHARON K. SANDEEN, PROFESSOR
OF LAW, HAMLINE UNIVERSITY SCHOOL
OF LAW, ST. PAUL, MINNESOTA**

Professor SANDEEN. Thank you, Chairman Grassley, Ranking Member Leahy, and the other Members of the Senate Judiciary Committee. I am honored to be here today.

As a trade secrets scholar, I certainly agree that trade secrets are very important, and for the record, I am against trade secret misappropriation and think that we need to have strong laws against trade secret misappropriation. I just happen to believe that the existing laws are sufficient and the proposed Defend Trade Secrets Act doesn't—will cause more problems than it solves.

I want to speak particularly from the perspective that I don't think has been adequately represented in discussions about the legislation, and that is of the numerous startup companies, entrepreneurs, mobile employees, and small and medium-sized businesses that are sued for trade secret misappropriation and forced to defend themselves, often when there are no legitimate trade secrets or little or no evidence of misappropriation. And I should point out an empirical study that was conducted about 5 years ago revealed that more than 50 percent of the time, the defendants win on dispositive motions and at trial.

I'm happy that over 40 law professors from across the country have joined me and my co-authors in expressing their concerns in two letters written in opposition to the proposed legislation, one in 2014 and one just recently.

Now, the reason why there is potential for abuse is that trade secrecy and the scope of trade secret protection is misunderstood. When considering whether the DTSA actually addresses cyber espionage and would be a solution to trade secret misappropriation, it is very important to understand that trade secret law does not protect all business information. It does not even protect all secret business information. It only protects a subset of secret business information which can meet stringency—stringent requirements imposed by the UTSA.

Now, the trade secret doctrine has long recognized, for instance, that information that's known generally among the public and within particular industries is not protected by trade secret law. Also, the general skill and knowledge that employees learn on the job, often including highly specialized knowledge and skills, is not protected by trade secret law, at least as it is written under the UTSA.

Now, the reason why trade secret law is limited is very important. There are two principal reasons. First, there's a strong public policy, repeated in numerous Supreme Court cases, that the law cannot and should not protect information that is in the public domain. Additionally, there is a long-standing policy in this country that inventors should seek patent protection rather than keeping their inventions as trade secrets.

As the U.S. Supreme Court stated, trade secret protection must be limited because, otherwise, it interferes with the patent policy of disclosure of information, and this is a disclosure of information upon which others can build and ultimately compete.

The DTSA, when coupled with recent changes to patent law as a result of the American—America Invents Act, threatens to disrupt this long-standing policy and I believe is the real motivation behind calls for a Federal law. Enabling companies to threaten Federal trade secret litigation, particularly with respect to formulas and processes that can be used while still being kept hidden, will undermine the disclosure purposes of both U.S. patent law and State trade secret laws.

Now, I have also written—and I will limit my comments here—that I believe the Defend Trade Secrets Act will increase litigation costs significantly. One reason is because there is no current Federal jurisprudence on trade secrecy. That will have to be developed.

I am also—I'm particularly concerned that well-established principles of trade secret law discussed in the comments to the UTSA are not included in the proposed legislation. And, of course, I am also concerned about the seizure remedy, which would be unprecedented in the United States and I think is going to be used abusively. I will end there and entertain any questions. Thank you very much.

[The prepared statement of Professor Sandeen appears as a submission for the record.]

Chairman GRASSLEY. Thank you, Professor. Now, Mr. Pooley.

**STATEMENT OF JAMES POOLEY, PRINCIPAL,
JAMES POOLEY, PLC, MENLO PARK, CALIFORNIA**

Mr. POOLEY. Good morning, Chairman Grassley, Ranking Member Leahy, and Members of the Committee. My name is James Pooley. Since the beginning of my legal career in 1973, I have handled hundreds of trade secret disputes, representing mostly smaller companies, startups, and individuals in the technology industry and acting both for plaintiffs and defendants. Thank you for holding this hearing and examining this critical subject.

Recent studies have shown that businesses increasingly rely on trade secrets to protect their competitive advantage, and this is particularly true for small businesses. While trade secrets have become more important, advances in electronics, like flash drives and smartphones, have made data theft almost infinitely easier and faster. And unlike the threats of a generation ago, when trade secret theft typically benefited a local competitor, globalization of business means that today's insiders often steal on behalf of companies located in another State or country.

Traditional State remedies for trade secret misappropriation are too inefficient to fully meet this new challenge. The Uniform Trade

Secrets Act has been widely adopted, but with many deviations. In addition, State procedural laws were not designed for efficiency and cross-border disputes. If a case in Illinois requires testimony of a witness in California, getting the required orders from both States can take weeks or months.

The Economic Espionage Act makes some trade secret theft a Federal crime, but relying on U.S. attorney to file criminal actions would only deal with a small fraction of the cases. So, neither State law nor the EEA offers a satisfactory solution to the time-critical nature of interstate and international misappropriation of a company's know-how.

Federal courts, however, can provide the necessary resource. They can provide a national standard for trade secret misappropriation and a transparent set of procedural rules, allowing nationwide service of process and enabling quick action by trade secret owners, even when confronted with actors in multiple jurisdictions.

American businesses both small and large operate across State and national borders, and they deserve a Federal civil remedy when their know-how is taken.

I strongly disagree with those who argue that we don't need Federal legislation because State laws are uniform enough, that the DTA's seizure provisions—DTSA's seizure provisions are too broad, or that the legislation would increase costs and interfere with the right of individuals to change jobs.

First, the variations in the UTSA today are in some cases worse than had existed before it was proposed. These inconsistencies burden companies, including small ones, that have interstate or international business. The DTSA will provide a level of uniformity across the Federal system that we had hoped for but didn't get with the UTSA.

Second, the ex parte seizure language in the DTSA is narrow and designed to avoid abuse. The application must clearly and specifically demonstrate all the required facts. Only property necessary to prevent the propagation or dissemination of the trade secret can be seized. The order has to minimize interruption to the defendant's business. These protections are greater than exist for the other ex parte form of relief, the TRO.

So, getting a seizure order will be extremely difficult, and the consequences of a careless petition can be severe, including damages that are not limited by the amount of bond that must be posted. Third, the DTSA will not increase the cost of trade secret litigation. We have had decades of experience with Federal courts handling these cases under supplemental or diversity jurisdiction, and there is no evidence of any difference in costs.

Finally, the DTSA presents no danger to the mobility of labor. It uses precisely the same language as the UTSA in permitting injunctions against threatened misappropriation. And it adds language barring injunctions against taking a job under conditions that avoid actual or threatened misappropriation. This provides additional assurance and is consistent with the law in every State that has enacted the UTSA, including California.

In conclusion, we need the DTSA to fill a gap in remedies available to U.S. businesses operating in an information-based and globalized economy. The DTSA has been carefully fashioned to

deter and punish abuse. Using well-established definitions and terms, it provides businesses a choice to file a familiar claim in an effective forum. And it does this without creating any new risks for small businesses or individuals.

I applaud the authors, Co-Sponsors, and the Chairman and Ranking Member for their leadership on this issue. As an experienced practitioner, I can say that the DTSA will improve the efficiency of trade secret litigation. Thank you.

[The prepared statement of Mr. Pooley appears as a submission for the record.]

Chairman GRASSLEY. We will have 5-minute rounds of questions. I will start with Ms. Cochran. Senator Leahy will follow me. Then I want to announce that I am going to go to the Agriculture Committee meeting, and Senator Hatch is going to take over at that point.

So, I have had an opportunity to visit Pioneer several times there in Iowa and see firsthand the impressive technological advancements that are taking place within the company. So, my question gives you an opportunity to expand on what probably your printed testimony says you didn't have an opportunity to go into in your 5 minutes. When it comes to property—protecting your proprietary research, how important are trade secrets as a part of DuPont's intellectual property portfolio?

Ms. COCHRAN. Thank you, Chairman. They are exceptionally important to us. We use the whole range of intellectual property from patents to trade secrets, but trade secrets have always been important to us. They've been, as I mentioned with the Kevlar technology, 50 years in the making. Without them we couldn't continue to bring new technology, and we couldn't attract collaborators, customers. We couldn't bring the quality that we bring to the table.

So, we see it to not only help us to—to have the quality and the research that enable us to partner and collaborate, but it also enables us to continue to build on what we have. Without it, we wouldn't be able to stay competitive either.

Chairman GRASSLEY. Mr. Beall, we have heard staggering numbers when it comes to the impact of trade secret theft on the economy overall. So, share with the Committee how trade secret theft affects your company, and maybe the most important part of this question would be the potential economic consequences that result from the theft of trade secrets.

Mr. BEALL. Yes, thank you, Chairman. Trade secrets are absolutely critical as an economic lever for Corning's success. Just to give you an example of a situation that has occurred in our business, we make LCD glass for televisions, big-screen televisions, which are ubiquitous throughout American and worldwide society. That glass is critical to those televisions, and we are the world leader in manufacturing that particular product.

Now, when you take a piece of that glass, which is approximately 10 feet by 10 feet, so a massive piece of glass, it's half a millimeter thick, and our specifications, our requirements for making that glass require that if the glass itself, the half-millimeter thick, were the depth of the Pacific Ocean, 5 miles, we would not be able to tolerate a wave on top of the ocean more than 10 centimeters. So, there are extreme, stringent requirements on us to make a piece

of glass that thin, that big, with very few defects on the surface of the glass in order to make these LCD televisions.

And part of our experience is that we have had two or three companies, or glass companies, who have knowledge in making glass, try to enter this business and have spent enormous amounts of resources trying to become competitive in this particular business, and they have failed. They have packed up and left and said, "Forget it. I can't do it." And the reason? The reason they packed up and not moved forward is because of the trade secrets and the intellectual property contained in our process that makes it work for us, that has been built up over the course of years.

And does that save American jobs? You bet it does. The jobs that we have at Corning maybe not—maybe would not exist were it not for the protection of those assets.

Chairman GRASSLEY. Thank you very much. I'll go to Mr. Pooley, and I compliment Senators Hatch and Coons on their legislation. I do want to ask about S. 1890 for this Federal civil remedy that we're talking about. Some opponents of the Federal civil rights of action have argued that there isn't a need for a Federal civil law. We've heard that argument already this morning. Why is a Federal civil law necessary from your point of view? And why aren't current Federal criminal and State civil statutes sufficient?

Mr. POOLEY. Thank you, Senator. The answer to that is, first of all, that State remedies are too varied, too unpredictable, to address the problem. Years ago, when trade secret theft was mainly local, on behalf of a local competitor, those laws were generally adequate. Today, when most trade secret theft, although still done by insiders, is prompted by global competition, competitors outside the State, and can be done with technologies that allow the transportation of information that before might have taken a truck but today only takes a USB key slipped in somebody's pocket, requiring a completely different set of remedies. It used to work years ago. It can't work today. We need a common remedy across the United States for companies to choose when they have a case that isn't entirely local and that affects their interstate business. And that's what S. 1890 will provide.

Chairman GRASSLEY. Senator Leahy.

Senator LEAHY. Thank you, Mr. Chairman.

Let me follow-up on that, Mr. Pooley. What you were saying about the truck backing up or the flash drive or something stuck in your pocket, unfortunately it applies to so many things. We've discovered that even in Government agencies that pride themselves on keeping their secrets until somebody walks off with all of them.

The—what I hear from small businesses in Vermont—and some of them are really cutting-edge in what they're coming up with—is that a Federal trade secrets bill is important because they rely on trade secrets as an easier, more affordable tool to protect their intellectual property.

Now, Professor Sandeen said that this bill could have unintended consequences for small businesses. Now, you have represented and do represent small startups in your legal practice. What do you say to that?

Mr. POOLEY. Thank you, Senator. My observation has been that small businesses need effective trade secret protection at least as

much, and often more so, than large ones because they depend on it, for—in an existential way, for the existence of their business. They need to have a remedy—

Senator LEAHY. In some ways it is their business.

Mr. POOLEY. It is their business, and they need a remedy that will work for them. And so, when you have businesses like those in Vermont that have leading technologies but they have markets across the country, they can't afford to go hiring lawyers in different States to run after someone before they leave the country and lock down that trade secret. They need something that will work immediately to get relief in—and that is, in Federal court—to stop the propagation or the destruction of the secret. It is Federal court that gives the efficient remedy for that kind of need.

Senator LEAHY. Thank you.

Mr. Beall, one of my priorities—and I have been looking at this legislation, which I want to be able to join. One of my priorities has been ensuring the seizure provisions of any trade secret bill that is narrowly tailored, make sure there are legal checks in place so they are not being abused.

Now, you've been involved in helping to craft the text of this bill. How are those kind of concerns addressed?

Mr. BEALL. Thank you, Senator. That's a very good question, and the seizure—ex parte seizure provision is intended to be very narrow and for use in only limited circumstances. So, some of the things that were concerning were that the seizure provision was intended to address rogue employees. That was the main intent behind it. But concerns were raised by companies that it might be used against them as recipients of information.

So, for example, a cloud-based business who may end up having the information stored on their server, would they be subject to the ex parte seizure provision? The intent was no. So, safeguards were added. Basically, third parties are not subject to the seizure, only the misappropriator he or himself. The seizure applies only in those circumstances where a court order is likely to be—is unlikely to be complied with and the misappropriator is likely to be a flight risk. The seizure itself will include only property necessary to prevent propagation or dissemination of the trade secret, and it will be very narrowly tailored.

Now, on the flip side, the party who is harmed by wrongful or excessive seizure has a remedy for damages and fees. And I can tell you this is not a seizure—this is not an item that we would take lightly. We certainly do not want to raise the ire of a district court judge and take any of these matters flippantly.

Senator LEAHY. You would feel, as I do, those kind—that kind of tailored specificity is important to the bill.

Mr. BEALL. Yes, I do.

Senator LEAHY. Incidentally, I am still impressed at the 50 kilometers. I keep looking at it.

Mr. BEALL. It is good for fishing, too.

[Laughter.]

Senator LEAHY. I don't ever get that far away, at least not in Vermont.

Ms. Cochran, you testified about the importance of trade secret protection to DuPont's Kevlar technology. You may know that the

law that is used to provide bulletproof vests, a Federal law to provide bulletproof vests to police officers around this country, was written by myself and a former Senator from Colorado, Senator Campbell. And some people say you do not need new legislation to protect a trade secret because you could use State laws or seek help from law enforcement. I assume you disagree with that. Why do we need a Federal law?

Ms. COCHRAN. Absolutely, we do. Thank you, Senator. Well, for some of the same reasons that have been pointed out. Today the information that is out there can be moved very quickly and deleted. For that reason, we need to be able to have a greater sophistication with the Federal system that could handle that, could handle the multinational and the multi-State impact.

Senator LEAHY. My time is up, and, Chairman Hatch, I know there are questions for Professor Sandeen and others. I can submit those for the record, I assume.

Senator HATCH [presiding]. If you want to go ahead, I—

Senator LEAHY. No, that is all right. We have others waiting.

Senator HATCH. Without objection, no question. Thank you, Senator Leahy.

Before I begin with my questions, I want to thank Chairman Grassley for holding this hearing. For years, Senator Coons and I have worked on crafting the Defend Trade Secrets Act, a bill to create a Federal private right—private right of action to protect trade secrets. Today there are 15 bipartisan Co-Sponsors to the bill, including 9 Members of this Committee. And on our side, I want to particularly pay—pay tribute to Senators Flake, Tillis, and Perdue for the work that they have done in helping to get this—this far.

Now, I count over 40 companies and associations that have endorsed the Defend Trade Secrets Act, including Corning, DuPont, the American Bar Association, the Information Technology Industry Council, Microsoft, Intel, General Electric, Adobe, and the Internet Commerce Coalition, just to name a few. I'm not aware of any stakeholder opposition to this bill. And those who operate businesses in the real world and have to protect their trade secrets on a regular basis are strong supporters of the Defend Trade Secrets Act.

Now, this bill is ready to move, not just through the Committee but also on the Senate floor. I think now is the time to act, and it's the right thing to do. So, I ask unanimous consent to insert into the record letters from the Protect Trade Secrets Coalition, the American Bar Association's Section of Intellectual Property Law, the Intellectual Property Owners Association, the National Alliance for Jobs and Innovation, the American Intellectual Property Law Association, and a blog post by Microsoft Corporation. So, we will add those to the record.

[The information appears as a submission for the record.]

Senator HATCH. Let me start with you, Ms. Cochran, and Mr. Beall as well. It is very important that people understand how this bill will address certain problems. Let me ask you about this in two ways.

First, in her prepared statement, Professor Sandeen says that "the vast majority of trade secret claims...involve former employees

or other business associates.” Do you agree this bill would address that category of bad actors?

And, second, in her prepared statement, Professor Sandeen says that the bill does not directly address the problem of cyber espionage. Do you agree with her that cyber espionage is not the primary focus of the bill?

Ms. COCHRAN. Thank you, Senator. Yes, we do believe that many of the trade secret claims do involve former employees and internal actors. No question about that. That’s been our experience throughout the major cases that we have had over the last several years.

With regard to your second question, while cyber espionage is, of course, a concern for us, we don’t see the bill as focused on that. It’s focused on trade secret theft generally. Cyber espionage is but one facet of that.

Senator HATCH. Mr. Beall.

Mr. BEALL. I would agree wholeheartedly with Ms. Cochran. Corning’s view is that the trade secret bill is geared toward situations where there are rogue employees, bad actors, and 95 percent of the situations that occur within Corning are just those situations, where an individual is collecting information in a protected way with the intent of leaving with it and selling it or otherwise using it elsewhere. That is the main focus, that is the main situation that we need some help on. And certainly cyber espionage is an issue, but that is not the thrust or the main point not only of this bill but of our concern at this point.

Senator HATCH. Well, thank you. In her prepared statement, Professor Sandeen refers to what she calls a, quote, “trade secret troll problem,” unquote. I will ask you this, Mr. Pooley. Is there such a thing as that, a trade secret troll problem?

Mr. POOLEY. Thank you, Senator. No, there is not. In fact, what makes a troll derives from the child’s fable about the troll sitting under the bridge waiting for some unsuspecting person to come by, jumping up and demanding a toll to get across the bridge. And that’s been applied to patents because patents are a no-fault liability, and hundreds of unsuspecting people and companies can be potentially infringing a patent. But that doesn’t apply in trade secrets. Under trade secret law, there can only be liability if you have a confidential relationship or if the actor has deliberately, using improper means, gotten access to the information.

So, these are one-off cases. It makes no sense at all to try to apply this metaphor of the troll that we use in certain patent cases to the trade secret environment. None at all.

Senator HATCH. Okay. Thank you.

Now, today U.S. businesses have—I will direct this again to you, Ms. Cochran, and you, Mr. Beall. U.S. businesses today have two tools to protect their trade secrets. State civil statutes and a Federal criminal statute. Now, the Defend Trade Secrets Act would simply add a Federal civil statute to complete the picture. Since this bill would not preempt State law, would State law continue to be valuable in protecting your trade secrets? And, also, do you agree that States should continue to enforce their own laws to protect trade secrets as they see fit? We will start with you, Ms. Cochran.

Ms. COCHRAN. Thank you, Senator. Yes, we believe that if the trade secret theft took place and it's a matter that is within State borders, then the State law should still apply.

Senator HATCH. Sure. Do you agree with that, Mr. Beall?

Mr. BEALL. I do agree with that. As you mentioned, Senator, this particular law is not intended to preempt State law, so there's certainly a place for State law. That is a weapon and a tool at our disposal and should not change based on this legislation.

Senator HATCH. Well, thank you.

Now, just one last question to Mr. Pooley. I wanted to follow-up on what Senator Leahy mentioned about how the Defend Trade Secrets Act would impact small businesses and startups. Some argue that the ex parte provision in the bill would be costly for small businesses and startups, especially to defend against wrongful seizure or abuse. How do you respond to this concern?

Mr. POOLEY. Thank you, Senator. Small businesses would not be harmed by the ex parte seizure provision. It is so limited, particularly after the changes that were introduced this time around. To add additional safeguards and to limit the kind of property that can be made subject to the seizure, the sort of information that has to be presented to the court, the quality of that information, and, in addition, of course, the consequences of making an improper application for seizure are so severe that small businesses would have nothing to be concerned about because it would apply only to very specific information; and if it turned out that there was some mistaken identity and the whole application was improperly filed, the court has very very adequate remedies to punish the applicant.

So, small entities really have nothing to fear from this. In fact, small entities need this in order to be able to get protection for the property that they depend on their secret information.

Senator HATCH. Well, thank you. I want to thank all the Co-Sponsors of this bill, and I think we'll get more. But I especially want to thank Senator Coons, and we'll turn to you next. Senator Coons?

Senator COONS. Thank you, Senator Hatch, and I want to thank the Chairman and the Ranking Member for calling this hearing to examine trade secret theft, its importance in the American economy, and whether the Defend Trade Secrets Act might be a part of the solution. And I want to especially thank Senator Hatch for his terrific leadership on intellectual property over so many Congresses and the work that he and his staff have done. He has already referenced the very wide range of support for this measure in the Senate, the 15 current Co-Sponsors, and among the whole stakeholder community. I'll also mention the identical House version introduced by Representatives Collins and Nadler has 93 Co-Sponsors.

I think the biggest reason for this broad groundswell of support is because the bill provides a commonsense and focused tool to fight a large and growing problem. American businesses, are, as has been mentioned before, losing hundreds of billions of dollars annually to trade secret theft and misappropriation. Federal law enforcement, however, only has the resources to bring a handful of Federal criminal cases, just 15 for the whole country last year.

Civil enforcement is left to a patchwork of sometimes inconsistent State laws, so I view this as an opportunity to create a uniform standard that will allow all parties to use the same law combined with access to Federal courts and injunctive relief, appropriately narrowly tailored, to address this growing threat to American competitiveness.

Senator Hatch and I've also worked on an open legislative drafting process through which we've taken into account many criticism and legitimate concerns and made modifications, and I am committed to continuing to do so, although I think the wide range of supporters for the bill already indicates we are pretty close to having a finished product.

I would like to ask consent, if I might, to include in the record three additional documents. A letter of support from 20 preeminent trade secret practitioners, led by Mark Krotowski of Morgan Lewis and Mark Halligan of Fisher Broyles; as well as an article from Corporate Counsel by Mr. Krotowski and Greta Burkholder; and a statement for the record by Mr. Krotowski.

Senator HATCH. Without objection, they will be entered into the record.

[The information appears as a submission for the record.]

Senator COONS. Thank you, Senator.

If I might, Ms. Cochran, just an opening question for you, and thank you for the example of Kevlar and the detailed example of how trade secret theft has significantly impacted DuPont. Am I correct that DuPont finds itself on both sides of trade secret disputes? And how do you think this bill appropriately balances the rights and the concerns of both plaintiffs and defendants in trade secret litigation?

Ms. COCHRAN. That is a great point, Senator. We do find ourselves on both sides of the table, which is why we have been very careful in the review on this. We have been sued for alleged trade secret theft, and so we view it with the eye of both what would happen, you know, as both a defendant and as a plaintiff. So, we feel comfortable both on the employee mobility issue for that reason, because we have also found ourselves hiring from, you know, top talent that happens to be in competitor areas as well, and the same thing on the seizure side when it comes to being a plaintiff or a defendant.

Senator COONS. Well, thank you. Mr. Beall, as we all continue to focus on your 50 kilometers of fiber optic cable, one of the innovative components of this legislation is that it allows for a victim of misappropriation to go to court and get an ex parte order, a tailored, focused order providing for the seizure of misappropriated information. And there has been some concern raised about whether that has been appropriately tailored.

Do you have a real-life example you might share with us that is illustrative about where this remedy could have prevented the loss of Corning's trade secrets and then how that impacts your manufacturing and your ability to keep jobs in the United States?

Mr. BEALL. Yes, I do. Thank you, Senator. We have a situation where there was an individual who had taken a fair amount of information, proprietary and trade secret information, upon leaving the employ of Corning, and it became apparent that that individual

had taken the information. We had a limited amount of time to act. We reached out to the FBI, and their resources were constrained, as you might imagine. And, again, with the limited amount of time, we sought a temporary restraining order in the local State court, which was granted, but ultimately the individual fled the country, and the trade secrets left with the individual.

Now, had we had the ex parte seizure in this particular circumstance and the FBI was unable to assist because of—because of constraints—and I don't want to say the FBI hasn't been helpful. They have been helpful, incredibly helpful in many circumstances for us. But in this particular instance, they didn't have the resources available. In this instance, we would have at least had the option to seek the ex parte seizure remedy and obtained our information back prior to the individual leaving the country with the stolen trade secret information.

Senator COONS. Well, thank you.

Senator Hatch, I will have further questions in another round, but I am grateful for those opening two answers. Thank you very much for your work.

Senator HATCH. Senator Flake, we will call on you.

Senator FLAKE. Thank you, and I want to thank the Chair and Ranking Minority Member for having this hearing as well. And I appreciate the work that has been done, and I appreciated working with Senators Coons and Hatch particularly on this. I particularly want to thank them for working with me on the provisions regarding ex parte seizure to make sure that they are narrowly tailored and that they contain the relevant and necessary due process protections and can't be abused. I will not say any more about the need for this legislation and the impact of this on the economy. To make sure that it does, the fact that you say it is 50 kilometers rather than 31.069 miles of cable there I think indicates that you export a lot of it, and so that's important for our economy nationally, and Corning, I might add, has a good facility in Arizona where you manufacture some telecom cable. So, I appreciate the work that has been done.

Mr. Pooley, can you shed some light? I know there's been some concern expressed by some that just as with patents there might be some kind of troll problem if legislation like this is enacted. Has there been any example at the State level with these State laws of trolling that we—that we should be concerned with? And is that likely to ramp up if we have some Federal remedies here?

Mr. POOLEY. Thank you, Senator. Indeed, no, we have never experienced a trade secret troll problem, and for the reasons that I described a little bit earlier, it's simply not possible because trade secret law is so different than patent law in that way. It is certainly possible from time to time that individual plaintiffs in a trade secret case may bring a weak case, but since the enactment of the Uniform Trade Secrets Act, there has been fee shifting available as a remedy. And we have seen nothing that looks like a general problem of people who own trade secrets going off and filing lawsuits against many others. First of all, they can't do it. And, second of all, the remedies are sufficient to disincentivize that kind of behavior.

Senator FLAKE. Ms. Sandeen, do you want to shed some light on that? Is that a concern that you have?

Professor SANDEEN. Well, Senator, thank you. First of all, in the article that Jim is referring to, Mr. Pooley is referring to, that I wrote with a co-author, we did characterize our concerns about abusive trade secret litigation as a “trade secret troll problem.” And one thing to understand is basically the meaning of that term, since it was first coined in the patent context, has kind of morphed to mean in broader terms abusive IP litigation, and that’s really our concern. And I mention it in my written statement. Small businesses are being sued for all manner of IP infractions, which are not necessarily strong claims, and then they have to defend them, and often it disrupts their business, and often it puts them out of business.

So, it’s not a surprise to me that there are not a lot of people in that camp opposing this bill because they have gone out of business, a lot of them. And I know Jim. Jim and I practiced law in California for many years together, and I’m sure he has represented defendants who were victimized by very weak intellectual property claims, very weak trade secret claims. And so, that’s what we are referring to when we are talking about trade secret trolls.

Senator FLAKE. As I mentioned, Ms. Sandeen, we took great care, we believed, to make sure that the ex parte seizure provisions are narrowly tailored and due process provisions are there. Do you have concerns still about the language here, that it is too broad? Or is it tailored enough?

Professor SANDEEN. You know, I recently wrote a book on international trade secret protection, and this remedy comes from the U.K. It’s called an “Anton Piller order.” And even the judge who created that order in that particular case in the U.K. has since said that it was—it has been overused. It was a very unique situation.

So, I do continue to have concerns, and I think the existing preliminary injunctive relief power that the Federal courts have and the State courts have is sufficient without this very extraordinary remedy.

Senator FLAKE. Thank you, Mr. Chairman.

Senator HATCH. All right. Senator Whitehouse.

Senator WHITEHOUSE. My time is short and my questions are many, so what I think I will do is ask them and ask people to get back to me for the record, because some of them are going to be somewhat complex.

My first question is; bearing in mind that the subjects of these orders are, by definition, recalcitrants who will not obey a lawful injunction, what degree of force may be used in the execution of the seizure order? I don’t know if any of you have been present at the scene of a search warrant execution, but it is a highly disruptive and occasionally violent process. May doors be broken in? May cabinets be forced open? Are employees sequestered the way they are in a search warrant application? And presumable it’s done without notice in order to preserve the element of surprise. So, the element—the extent of the force and surprise that would be used in the execution, I’d be interested in, and also by whom? Would the court marshals be sent out to do this? Would private actors be authorized to do this? So, that would be my first question.

The second is once something is seized, I get this if you are looking at an object or a sample that you can grab and take back and now it is out of the control of the individual. It's a little bit different when you are dealing with electronic information. If you have to seize an entire company's computer systems, for instance, in order to be able to control the space in which the sought information exists, then somebody has to have the task of sorting through all of that seized information in order to isolate the information that is subject to the order. Who does that sorting? And what are the privacy concerns for whoever else's information might be swept up in that broader search? And how do they protect themselves? Who becomes the person who sorts through all this and decides where the boundaries of the sought information are?

Third question. What happens if you now go to the cloud? Now, you are executing this seizure order, search warrant, whatever it is, in a third party's very complex data environment. What are the constraints there? And, again, how do you deal with the problem of overseizure now that you are dealing with cloud and potentially much larger amounts and a real difficulty of identifying whose personal information might be there? So, that would be question three.

Question four is how realistic is it that any seizure would be deemed wrongful or excessive after a court order had been obtained for it? Is that really a meaningful constraint on this process? A court order is usually an absolute defense to any concern that the act involved was unlawful. You are executing the court order. And if the execution of the order was unduly either violent or broad on the part of the marshals or whoever else was executing it, then who is at fault? Because, you know, there are separate parties, the party who came in, the company that wants it executed, and then whoever did whatever the actual seizure was.

Fifth, both witnesses Beall—Beall and Pooley have in their fact patterns that they have used described the intention to flee overseas and outside the jurisdiction of the United States, which is obviously a very legitimate concern. I have been the Anti-Piracy Caucus Chair with Senator Hatch, so I am deeply concerned about this, but I don't want to create something that becomes a menace to Americans in the spirit of accomplishing that. If what we're really concerned about is the intention for people or for the data to flee overseas, shouldn't we focus this on that problem rather than on people who are going to stay in the country, who are going to be always amenable to various judicial orders, and so forth?

And, finally, in my experience, employee agreements that involve confidentiality, nondisclosure, and noncompete can often end up being pretty hard fought. There end up being very strong feelings on both sides. If this becomes as hardball tactic in a battle between a company and an employee who has now moved on to become a competitor or to do something else and they are arguing about, well, they shouldn't have taken this list or whatever, should we exempt cases that involve that kind of standard employee civil dispute from the application of this particular mechanism?

And I am over my time already, so I will leave it with that. But I hope I've conveyed my sense that as much and as deeply as every person here cares about protecting our intellectual property, I have called cyber intellectual property theft the biggest wrongful theft of

the transfer of value in the history of humankind. But launching this kind of potentially violent, surprise, Government-sanctioned action into people's homes and businesses and potentially also into data, which it gets very hard to know where the limitations are, I think is something that deserves a good deal more caution than I have heard in this hearing so far.

Thank you, Chairman.

Senator HATCH. Thank you, Senator. We will try and get those questions from the Senator put together, and if you could answer those, we would really appreciate it.

Senator HATCH. Okay. We will go to Senator Tillis.

Senator TILLIS. Thank you, Senator Hatch.

Actually, I want to start with Mr. Beall. Actually, Mr. Beall, I want to thank Corning for a great presence in North Carolina, a great employer. I know a lot of the discussion has focused on the domestic trade secret protection, but can you talk a little bit about the differences and the challenges between domestic and foreign trade secret protection?

Mr. BEALL. Sure. Some of the challenges that we incur overseas are that it's very difficult for us to be able to obtain discovery over what has actually occurred within the facilities outside of the United States. So, typical—typical legal systems outside of the U.S. don't have an open discovery system, so it is difficult, in fact, impossible at times, to request information around what exactly is happening in the facility and obtaining that information. That's a frustration for us, because the opposite is not true, right? I mean, a foreign company can come to the United States and say, "Hey, I think you stole my trade secret. I want to see what you are doing inside your facility," and based on the discovery laws, we've got to provide some information.

So, we're playing a little bit with our hands behind our back in that regard, and that's why I think it is important as part of the activities in the bill that we have here to show that, hey, we are the gold standard, and we are putting ourselves out as the gold standard, and part of that is filling in this hole, if you will, where there's a no civil remedy today under Federal law, and filling that gap tells and sends a message to our trading partners, "Hey, here's the way it should be done, this is the way it's done in the United States, and we would like to see it done overseas." It's very important to us because we do operate overseas, and we feel like we're at a bit of a disadvantage there.

Senator TILLIS. For Corning, how would you set the ratio in terms of the long-term threat assessment between domestic trade secret theft and foreign trade secret theft? Where is most of your concern?

Mr. BEALL. That's a good question. It is probably 60/40 foreign to U.S.

Senator TILLIS. Would you expect that to grow over time.

Mr. BEALL. I think it will probably grow over time. I mean, trade secret is a problem around the world. Trade secret theft is a problem around the world, and oftentimes—it's a difficult question for me because oftentimes there is a U.S. component and there is a foreign component. And it's not just one country; it is many countries. So, it's a global problem for us, not any specific country per se.

Senator TILLIS. Okay. And in my remaining time, Ms. Cochran, in your opening comments you talked about the DTSA being a gold standard. Ms. Sandeen, in your opening comments you mentioned that it creates more problems than it solves. And, Mr. Pooley, I think you were generally supportive. So, in the time remaining, can you give me in about 45 seconds—we'll treat this like a debate. We will go right down the line, starting with Ms. Cochran and then ending with Mr. Pooley—why you think it's the gold standard and why you differ with maybe the comments made by Ms. Sandeen and vice versa?

Ms. COCHRAN. I'm going to summarize, Senator, with the points that we have made. One, it's offering the Federal civil remedy. It is the United States taking the leadership in a very important issue, and hopefully other countries will follow. And then, finally, because time is of the essence in cases like this, to be able to take a step forward quickly to secure and prevent further dissemination of the information.

Senator TILLIS. Ms. Sandeen.

Professor SANDEEN. Thank you, Senator. The main reason is, as I mentioned, there is no Federal jurisprudence currently for civil trade secret. It will have to be developed by the Federal courts. The Federal courts are not being directed by the U.S. Congress in this bill to base their opinions on the UTSA, including the comments. That means that the Federal courts can choose between all manner of existing law from all manner of cases, first restatement, third restatement of unfair competition, et cetera. I think that will lead to less uniformity in the law of trade secrecy, not more.

A better result might be to actually, you know, if this bill goes forward, is adopt a Federal Uniform Trade Secrets Act with all the commentary included, not just selected commentary.

Senator TILLIS. Mr. Pooley.

Mr. POOLEY. Thank you, Senator. All businesses, small and large, need this legislation to go forward because the nature of the threat has changed. This is a gold standard because it has been so carefully thought through to address both the need and the problems on the other side. I can say I have been present at execution of a search warrant in a trade secret case. These are not drug busts. When people get this kind of order delivered on them, they comply. And if it has been prepared properly, then we will get exactly what the law was intended to provide, which is preservation of that secret so it does not move and it does not get destroyed.

Senator TILLIS. Thank you. Thank you, Mr. Chair.

Senator HATCH. Thank you, Senator Tillis. Senator Perdue, and this will be the end of the first round.

Senator PERDUE. Thank you, Senator Hatch, and I appreciate the forbearance of the witnesses. I just have a couple quick questions.

In my business career, you know, running a multinational, I have fought this most of my career, and I understand the sensitivities and the direction that the courts need to take relative to instruction here. I am a Co-Sponsor of this bill. I want to further this debate. But I have a question today specifically. I think we have covered the topic today very well, but on the cyber threat, we've been doing a lot of work this Congress on cybersecurity in several areas, and a big part of the misappropriation of trade secrets today

in my experience has been the growing cybersecurity infringement on this and the international nature of the threat. We talked about that a little bit, but I would like to get each of your perspectives on this. I think some of you have talked about it. I'd like to get a summary of this.

I'd love you to talk about the extraterritoriality and how we can address this through this legislation, and what else do we need to consider as we talk about the cyber issues in addition to what the professor has talked about may be a shortcoming in the current legislation. Ms. Cochran.

Ms. COCHRAN. Thank you, Senator. I don't want to disappoint, but I think our thought was that this is going to be an important piece of legislation for us, regardless of whether or not it's South Korea or it's South Carolina, where is the origin of the trade secret theft. So, the cases that we have been, you know, studying, that we have experienced in the last several years, that have been the basis for why we support this bill have not directly derived out of the cyber espionage aspect of it. So, for us, it is both the domestic and international facets.

Senator PERDUE. Thank you.

Mr. BEALL. I would agree with Ms. Cochran. We certainly see attempts at network penetration in our company. It's something that we deal with on a weekly basis, not a yearly basis. It occurs quite—quite prevalently. But our main concern here is in circumstances—and there're really two ways when we find out there is trade secret theft that has gone on.

One I have already mentioned, which is when we know about a bad actor, he has quickly left the facility, and we have a limited period of time to access his whereabouts and obtain the information back.

The second situation is in scenarios where we have suppliers who make parts of our apparatus for our critical businesses and our critical manufacturing, and those suppliers will call us, and we have a robust program in place where we educate the suppliers and say, "Hey, if you see anything that looks like our stuff, please give us a call." And we often see the trade secret misappropriation coming through that angle where our suppliers will come to us and say, "Somebody just gave us an order. It looks like it is Corning's drawings. What should we do about it?" And so, we have really encouraged that kind of dialogue, and it has been very fruitful for us because then we can—could really address the problem head on.

And another reason why I think this particular bill is helpful for us is it gives cross-jurisdictional discovery because our suppliers are all over the country.

Senator PERDUE. On that point—sorry to interrupt, and I want to get to the other two witnesses real quickly, but do you have any problems in communicating with competitors relative to that issue there in terms of what their experiences are and so forth? Are there any antitrust laws you run into in terms of discovery with a common provider providing similar equipment to a competitor that may be one of your—may be one your designs?

Mr. BEALL. Not too much, because our designs are so unique and customized, and this is part of the trade secret issue we have been talking about today, that it is very clear when somebody sees our

design that it's ours. I mean, they might wipe off the Corning name on the design drawings, but ultimately there's a lot of telltale signatures that had to have been developed and were developed by Corning, we know who developed them, and so it's very easy for us in those instances to tell that this was—this was certainly something that came from Corning, was somehow misappropriated. And then it is up to us to try to figure out—put the pieces back together to figure out where the misappropriation occurred and try to correct that.

Senator PERDUE. Professor.

Professor SANDEEN. Thank you, Senator. I am very concerned about cyber espionage. I don't think this bill addresses that, however, and——

Senator PERDUE. No, it does not.

Professor SANDEEN. The main reason is, I think, we should address the bad act of cyber espionage directly rather than requiring the predicate fact being proven of the trade secrecy, because really what's going on is businesses whose systems are broken in care about a broader set of business information being taken or tampered with than the limited set of trade secrets that exist. And so, I wouldn't use this legislation to solve the cyber espionage problem.

Mr. POOLEY. Senator, if I might just add very quickly to that, I am glad you brought up extraterritoriality because it is one of the major reasons why we need to have Federal courts looking at these issues. Much more of the theft that happens these days, whether it's cybersecurity, cyber espionage, or whether it's done by actors locally who then might leave, the fact is there is an international component to it. State court judges, in my experience over the years, have a hard time dealing with this. Federal judges deal with international issues. The jurisdiction of courts here for the consequences of acts done in another place, they've seen that many times. They understand what comity is and isn't. And so, we can get much more predictable and effective relief in Federal court. Thank you.

Senator PERDUE. Thank you all. Thank you, Mr. Chairman.

Senator HATCH. Well, thank you, Senator Perdue. Let me just ask a couple of questions here in the end. Let me ask you this, Mr. Pooley. Professor Sandeen noted in her oral statement——

Senator TILLIS. Mr. Chair, I see a couple people out there struggling to hear. I do not think they can hear very well.

Senator HATCH. Yes, something is wrong with this mic. I will have to get a little closer.

Professor Sandeen noted in her oral statement that the seizure provision is unprecedented in U.S. law. But isn't the provision in the bill modeled on the provision contained in the Lanham Act? And as you know, the Lanham Act has been used by the Federal courts for almost 70 years. Am I wrong on that?

Mr. POOLEY. Thank you, Senator. No, you are exactly right. The provisions of the DTSA relating to seizure were patterned directly on the Lanham Act and then taken from there and constrained as a result of the discussions with various stakeholders to make sure that applying these remedies in a trade secret case would not cause undue harm and would not involve third parties in the seizure.

One of the most important things about the seizure provisions that keeps it contained is that it applies only to the trade secret misappropriator himself. Going into the cloud is not an issue. He has to be in possession of the secret. When that happens and the secret can be adequately described, then the court can act. These are—this makes it both similar to the Lanham Act on which it is based and much narrower in the sense that it is designed specifically for a trade secret situation.

Senator HATCH. Okay. Now, you have also had a chance to review—or have you had a chance to review Professor Sandeen's recent blog post regarding your article on trade secrets. Would you care to respond to that.

Mr. POOLEY. Well, only in this sense, Senator. I would say that my experience in actually representing dozens and dozens of startups over the years presents a very different picture to me and what I've observed in terms of the overall threat and concerns. Startups have an equal interest in the robust protection of their trade secrets with larger companies and sometimes even more.

One of the other things I disagree respectfully with the professor about is that somehow there is an idea in her writing and in this article that through this law we will be encouraging people to use trade secret protections, businesses to use it, and take them away from the patent system, which has a policy of disclosure. The patent system is not based on a public policy of disclosure. Disclosure is a price. The Supreme Court in *Eldred v. Ashcroft* told us this. It is a price exacted from the applicant—patent applicant in order to justify the quasi-monopoly that the applicant is given.

The objective of the patent law is to encourage innovation and the progress of the useful arts, and as the Supreme Court told us in *Kewanee* back in 1974, that is exactly the purpose of the trade secret laws as well. They get there through a different route. But if we didn't have secrecy, we wouldn't have the dissemination of information that is made possible through collaborations and licensing. It is absolutely necessary to make that happen. Thank you.

Senator HATCH. Okay. I appreciate that clarification. Ms. Cochran and Mr. Beall, how do you respond to arguments that the proposed legislation will limit the diffusion of information and knowledge? Go ahead. Ms. Cochran, we will go with you first and then Mr. Beall.

Ms. COCHRAN. We don't believe that that is an issue, Senator. We utilize both patents which publish and trade secrets, and some of the trade secret information that we keep is not even available under patent law because it doesn't meet patent law requirements. So, it's just another mechanism for us, and we disseminate a lot of information through the patent system that just so happens to publish as well.

Senator HATCH. Do you agree with that, Mr. Beall.

Mr. BEALL. I do agree with that, Senator. We at Corning take a look at protections both under the patent law as well as under trade secret protection. And I mean, the types of things that are critical—in fact, some of Corning's greatest inventions have been process engineering, dropping the cost of a particular product sale. And we could be talking about things so much as turning a certain dial or the particular angle that glass flows from one part of our

process to another. And these, you know, these are the types of things that are absolutely critical to how we operate, things we've learned over years. If there's a certain breakdown in the process, we know exactly how to fix it immediately. And these are—you know, as Ms. Cochran mentioned, these are things that are not necessarily amenable to patent protection, but certainly critical for trade secret protection.

Senator HATCH. We will go into the second round, and I have to leave, but we will turn to my colleague/Co-Sponsor Senator Coons, and then Senator Tillis has offered to help here and continue the discussion.

Senator COONS. Great. Thank you very much, Senator Hatch. I just have a few questions. I wanted to touch on two or three things to round out some of the previous exchanges. And as he is leaving, I want to thank Senator Hatch again for his leadership on working so hard on this bill.

Professor Sandeen, if I might just follow-up on the question Senator Hatch just had about information diffusion, you just posted something on a blog entitled "Patently O" that summarizes your opposition to the bill as being rooted in your seeing IP issues through the lens of information diffusion. And if I understand correctly, that's summarized best perhaps by saying that rather than seeing strong protections, you favor disclosure, quote, "because society benefits when trade secrets leak out."

Is it really your view that the loss of trade secrets by a U.S. company is a good thing? Help me understand how this advantages American innovation and manufacturing.

Professor SANDEEN. Thank you, Senator. I didn't make up that language. It came from the U.S. Supreme Court case in *Kewanee* that described trade secret protection as being like a sieve. And the point that the Court made in that case and the whole reason why States' trade secret law was not preempted was because it was weak. And what the U.S. Supreme Court said, and I think rightly, is that when trade secrets are weak, it then forces companies like DuPont and Corning to make an important decision, which is; do we protect things by patent law or do we protect them by trade secret?

I acknowledge that some things cannot be protected by patent because they have already been invented, for instance, or because they wouldn't fall within patentable subject matter. But the point is that the stronger you make trade secret, the greater the choice companies will make to protect things as trade secrets rather than patents. When that happens, the disclosure of inventions that occurs when patents are published will end. And I happen to believe strongly that intellectual property policy needs to be balanced so you give companies the incentive that Mr. Pooley talked about, but not a de facto monopoly forever, because ultimately society benefits when companies can learn from public knowledge and develop competing businesses which actually provide competing products that might be better and at lesser cost.

So, it's a balance, and I think we have to be careful about that balance.

Senator COONS. Well, if I might, Ms. Sandeen, Mr. Pooley, in that abstract commitment to a balance between the diffusion of in-

formation and the free market of ideas and information wanting to sort of seek its best owner and a legal system where we are also trying to protect American invention, innovation, competitiveness, and manufacturing, how do you view the appropriate balance between trade secret and IP?

Mr. POOLEY. Thank you, Senator. There are people who believe that information should be free, generally, and I think there is more and more of them. But that is definitely not what the Supreme Court said in *Kewanee*. It is a brilliant decision, actually, in many ways because it speaks precisely to this balance. How can we have a system that, on the one hand, demands disclosure as the price for this quasi-monopoly and, on the other hand, allows secrets to be maintained? And the Court explained it very, very well, and it's the difference between whether information can leak and, therefore, the trade secret protections are relatively weaker or whether they should leak, which is the position, I understand, of a few economists and law professors. But I do not hold that. And the Supreme Court in *Kewanee* made it the choice of those who develop valuable information to choose one path or the other as best suits them to get the information out to the marketplace for the benefit of the public. Sometimes that is through a patent, but very, very often, and increasingly these days, it is through secrecy.

Senator COONS. Well, I am very concerned about American manufacturing and maintaining our competitiveness, and private sector investment in R&D related to manufacturing is the overwhelming majority of R&D in this country. And we've heard two compelling examples of the manufacturing of world-class products that would leave our shores tomorrow if the information embodied in the trade secrets developed over decades in the manufacture of Kevlar and fiber optic cable were truly free.

Let me ask one last question, if I might, given the limitations of time. Mr. Pooley, I was concerned last year when the professors raised an argument that our bill could be used to impair employee mobility, and I think some other Members today have expressed concerns that perhaps this could be used to harass employees who are seeking to leave an employer. That's the last thing that Senator Hatch or I wanted to do, is to impair employee mobility, particularly in high-performing engineering fields, and so we included specific language in the bill this year that protects an employee's right to move from company to company. And you have certainly litigated many cases on both sides of that question. Do you think we have gotten it right?

Mr. POOLEY. Thank you, Senator. Yes, you have. The language that's used in the DTSA is the same as the language in the Uniform Trade Secrets Act. So, if we have an employee mobility problem by the enforcement of trade secret laws in this act, well, we already have it in 47 of the 50 States in the U.S. All of those States allow injunctions against threatened misappropriation. And I think the language that you have added to the bill this time provides an additional and very significant level of comfort that Federal judges in particular are not going to get themselves involved in trying to do anything other than to protect the integrity of the information that might be moving from one place to another. It's not in their province, and certainly they've been directed through the language

that you have so wisely chosen here not to let this spill over into side disputes about noncompete covenants and the like. We will have the same standard apply here that has been applied through the Uniform Act along with, as I say, the additional level of comfort, and I think that will make sure we do not have these problems.

Senator COONS. Well, thank you very much, Mr. Pooley, Professor Sandeen, Mr. Beall, and Ms. Cochran. Thank you for your testimony today, and thank you for the second round of questions.

Senator TILLIS [presiding]. Thank you, Senator Coons. I was actually going to go to an Agriculture Committee hearing, and I stepped out, but I decided to come back because there was just something else I wanted to talk about.

I was—early in my career, I was in product management and later research and development role manager in the high-tech sector back in the '80s. What we would do, if we were going to move forward with a major R&D initiative, is we would have to come together, determine really whether the goal was achievable, how much it was going to cost, and what length of time would we potentially have a competitive advantage to justify whether or not we ever make that investment. If we don't get this right, it will have a chilling effect on America continuing to be the leading innovator in the world.

Earlier this week, the President gave a speech where he started out saying "American ingenuity," corrected himself and said "human ingenuity." I think that's nonsense. I think that we need to continue to recognize that America is the greatest innovator, the greatest and most innovative Nation that has ever existed. And part of the reason why we do that is we provide certainty to businesses to be able to make the kinds of investments that give us that disruptive capability, technological advantage, whether it's high-tech, pharmaceuticals, agriculture, no matter what. When we start having a discussion about the distribution or diffusion of knowledge, I read that as knowledge redistribution like wealth redistribution. It's not a good thing to do.

And a lot of people will say, well, this is a Senator talking about protecting these big businesses that just abuse their competitive advantage. First, I think that's nonsense. I am more concerned with the guys that just came out of college, and gals, who are putting their mortgage behind an innovative idea and shortening the horizon for the length of time that they can benefit from the huge personal risk that they have taken. That's what we have to work on in this bill.

I am also concerned with the fact that you've got a 60/40 mix today, 60 percent being foreign. That's going to grow. And I think our future trade agreements need to make it very clear that these nations that want free trade with the United States better level the playing field in terms of what we can do to protect our intellectual property.

So, that was less of a question, more of a statement. I would be happy to have you all react to it. But I think that is very important for us to be grounded in how this sort of policy—and I understand Ms. Sandeen's concerns, and I think we should continue to work to address some of them. But foundational to this legislation is pro-

protecting the intellectual property of the sum total of businesses that happen to be in the greatest and most innovative Nation that's ever existed. And I am going to do everything that I can in this Committee and as a Senator to make sure that we get to that end.

And Ms. Cochran, I would be happy to have you all make closing statements, and we will carry the Committee to its closure.

Ms. COCHRAN. Thank you, Senator. I think your points are well taken. Those are exactly the sentiments that DuPont has had. We also recognize and it should be noted that we invest a lot to find out if someone has stolen our trade secrets, which is not a free—

Senator TILLIS. And at the expense of investing in more innovation.

Ms. COCHRAN. That is exactly right. We would rather put it into the R&D. Thank you.

Senator TILLIS. Mr. Beall.

Mr. BEALL. I would also agree with your statements and appreciate those, Senator. My job at Corning is to protect intellectual property. That's the lifeblood of our company. And anything that we can have, any new tools to help achieve that goal are absolutely welcome, and that's why we support this bill.

We spend an inordinate amount of money on research and development, and as you said, we do it because we want to advance the technology. But we don't do it because we want somebody else to take a free ride on the work and the money we have spent to accomplish and produce the kind of products we have.

Senator TILLIS. Yes. Ms. Sandeen, I don't want you to take me dismissing some of what I think are your very valid comments. I think that there are forums where we clearly see the diffusion of information and knowledge as a plus. Open source is a classic example of that. But I think there are other instances where the nature of the product and the nature of the technology lends itself to one to where you really want to encourage the protection of the key innovators and make sure that that's the bedrock of our process. I just wanted to make sure you didn't think everything you said I disagreed with, just a few points.

Professor SANDEEN. Well, Senator, I do not disagree with what you just said. My concern is that not every company in the United States is like DuPont and Corning or the other Sponsors of this bill, which have—know what a trade secret is, know how to identify it, know how to engage in reasonable efforts to maintain secrecy. There are a lot of companies out there that, frankly, do not know or even think they have a trade secret until they go to an attorney like Mr. Pooley who tells them they might have a trade secret, and then they file litigation.

My concern is when that litigation—and most of it's filed against employees, former employees—is brought against former employees and they had no notice or little notice on what the trade secrets were. We have a situation now that those employees can be thrown into Federal prison when they didn't even know what a trade secret was.

And so, one of the things we might consider in the legislation is beefing up and being more specific about what steps employers, companies should take before they can bring a Federal cause of ac-

tion. That might eliminate some of these weak cases from being made into a Federal case. Thank you.

Senator TILLIS. Thank you. Mr. Pooley.

Mr. POOLEY. Senator, first of all, I'd like to thank you for your remarks with which I wholeheartedly agree. Back when I started in this field in the 1970s, the only thing that a company really needed to do to protect its competitive edge was guard the photocopier and watch who went in and out the front door. And I think we can all see how times have changed. And these trade secrets are—it's just a term that we apply to exactly what you are talking about, the kind of information that gives us our competitive edge as a Nation.

We owe it to the people who produced that information to give them the most effective tools that we can to make sure that the integrity of that information is protected so that it can return benefits to the public at large and to those who created it in the first place. This legislation just gives them a choice to go to Federal court where they can get that kind of protection. Thank you, Senator.

Senator TILLIS. I want to thank all the witnesses for being here. It's been very informative. I think it is instructive to a bill that I have Co-Sponsored and I look forward to working with Senator Coons and Senator Hatch on.

We will leave the record open for a week so that other Members may submit questions. We would appreciate your indulgence on that and any other information you would like to provide. This hearing is adjourned. Thank you.

[Whereupon, at 11:52 a.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

**Prepared Statement by Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Hearing on “Protecting Trade Secrets: the Impact of Trade Secret Theft on American
Competitiveness and Potential Solutions to Remedy This Harm.”
December 2, 2015**

The United States is the world’s leader in innovation, creating cutting-edge technologies and products that improve our daily lives. This occurs in good measure because of our robust system of intellectual property protection and enforcement.

Trade secrets are a lesser known, but increasingly important form of intellectual property.

Trade secrets allow for the legal protection of commercially valuable, proprietary information. Some famous and oft-cited examples of trade secrets include the formula for Coca-Cola or the recipe for Kentucky Fried Chicken.

In fact, a broad range of valuable information may be protected as a trade secret, including complex financial and technical information and computer algorithms.

These trade secrets hold immense value to American companies. The U.S. Chamber of Commerce recently released a report stating that “publicly traded U.S. companies own an estimated \$5 trillion worth of trade secrets.”

Trade secrets encompass an expanding portion of firms’ intellectual property portfolios, particularly in knowledge-centric areas of the economy such as technology and manufacturing.

However, the theft of trade secrets of American companies is increasing, and this hurts the U.S. economy and costs American jobs. Globalization, the emergence of the digital economy, and the increasing frequency with which trade secret thieves utilize technology and cyber capabilities, has made it more difficult for trade secret owners and law enforcement to guard against theft and to fight back.

Last year, the Federal Bureau of Investigation’s Assistant Director of the Counterintelligence Division, Randall Coleman, testified before the Committee that “economic espionage and theft of trade secrets are increasingly linked to the insider threat and the growing trend of cyber-enable trade secret theft.”

In February 2013, the White House released a report detailing that “[e]merging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating.”

Then-Attorney General Eric Holder underscored these findings when he stated that, “There are only two categories of companies affected by trade-secret theft: those that know they’ve been compromised and those that don’t know yet.” The result is that, according to a recent report of the Commission on the Theft of American Intellectual Property, annual losses owing to trade secret theft are likely comparable to the current annual level of U.S. exports to Asia – over \$300

billion. The report further estimates that trade secret theft is responsible for the loss of 2.1 million American jobs.

Unlike other areas of intellectual property, the protection of trade secrets in the United States has mainly been a matter of state law, with forty-seven states having enacted some variation of the Uniform Trade Secrets Act.

While differing state trade secret laws share many features, state legislatures often made changes as they enacted the UTSA. This has led some to argue that the existing patchwork of state laws imposes difficult procedural hurdles in the many cases where a trade secret is taken across state lines. Federal law, through the Economic Espionage Act of 1996 (EEA), allows federal law enforcement authorities to criminally prosecute trade secret thieves, but it doesn't give trade secret owners a private right of action in federal court.

As companies increasingly utilize trade secrets and as trade secret theft has soared, the FBI reports that their caseload for economic espionage and trade secret theft cases increased more than 60% from 2009 to 2013. In fact, some commentators point out that in the face of what the FBI has described as an "immense threat," the Bureau's Counterintelligence Division's Economic Espionage Unit, which is tasked with investigating offenses under the EEA, does not have the resources and necessary bandwidth to bring prosecution of all trade secret cases.

I've heard from a broad coalition of stakeholders - large and small - representing job creating businesses in innovative sectors of the American economy, about the need for a federal law to protect their valuable trade secrets.

In my own state of Iowa, we've seen first-hand how some of our most innovative agricultural companies, like DuPont Pioneer, have become targets of trade secret thieves who seek to profit from the hard work and research of others. In one recent case, foreign nationals were indicted for engaging in a scheme to steal proprietary test seeds from Iowa fields to benefit a foreign agricultural company.

So, I look forward to learning more about this important issue and potential legislative solutions.

**Statement of Senator Patrick Leahy (D-Vt.),
Ranking Member, Senate Judiciary Committee,
Hearing on “Protecting Trade Secrets: the Impact of Trade Secret Theft on American
Competitiveness and Potential Solutions to Remedy This Harm”
December 2, 2015**

Today’s hearing focuses on a topic that is essential to our Nation’s economy and our status as the leading source of innovation around the world.

In Vermont, trade secrets protect the specialized knowledge of woodworkers and artisans that have been crafting heirloom products for generations. They protect the secret recipes for Vermont craft brews and closely-guarded customer lists for our top tourist services. They protect cutting-edge technologies that Vermont businesses are developing in plastics, complex manufacturing, software, and green technology. Trade secrets are relied on by countless businesses to help keep their products and services unique.

Today we will hear about the importance of trade secrets from two companies that have used proprietary information to build global brands and create tens of thousands of jobs across America and around the world. Yet trade secrets are especially important to small businesses, which often lack the resources to seek patent protection for their inventions. The features that make trade secret protections so useful also make them vulnerable, since disclosure by a rogue employee or by a cyber-attack can end their confidential status in an instant.

In the United States, trade secret law is the one form of intellectual property protection that currently lacks a federal civil remedy. I have heard from businesses, practitioners, and law enforcement experts that creating such a remedy will improve the law by promoting uniformity and reducing the procedural hurdles that companies now face when stolen information is taken across state lines. Carefully written legislation will fill this gap in the law, and provide businesses in Vermont and across the country with an improved tool to protect their intellectual property.

It will also ensure that our Federal law serves as a meaningful example internationally. During my travels to China and other countries I have emphasized the need for strong global protection of trade secrets. There is much more to be done to address the problem of trade secret theft internationally, but adopting a uniform Federal policy at home is one important step.

Good, thoughtful work is being done in this Committee to craft such legislation. One priority for me has been ensuring that any seizure remedy to protect trade secrets is narrowly-tailored—for example, so that actions to protect confidential information on a computer server do not unintentionally impact other content on the server that is unrelated to the theft. I thank Senators Coons and Hatch for working with me and with technology companies to address this concern. I look forward to the Committee’s continued consideration of the bill.

In 2012, we passed two pieces of legislation that helped improve our trade secret laws, including the Theft of Trade Secrets Clarification Act, which I introduced to close a troubling loophole in the law that allowed an employee who had stolen trade secrets to go free because the stolen

secret was not part of a product sold in interstate commerce. I am glad that the Committee is continuing its bipartisan work in this vital area. I look forward to working with Chairman Grassley, Senators Hatch and Coons, and with all members of this Committee on this important issue for American businesses.

#####

Hearing on

**Protecting Trade Secrets:
the Impact of Trade Secret Theft on American
Competitiveness and Potential Solutions
to Remedy This Harm**

United States Senate Committee on the Judiciary

December 2, 2015

**Written Statement of Thomas R. Beall
Vice President and Chief Intellectual Property Counsel
Corning Incorporated**

I. Introduction

Good morning Chairman Grassley, Ranking Member Leahy, and Members of the Committee. My name is Tom Beall. I am Vice President and Chief Intellectual Property Counsel to Corning Incorporated. Thank you for holding this hearing. I appreciate the opportunity to testify today about the importance of trade secret protection.

Background on Corning

For context, let me give you a little background on Corning Incorporated. We have been in business as an American manufacturer for over 160 years and take great pride in our heritage as one of America's oldest and most innovative companies. We are on pace to be issued over 400 patents in the U.S. this year, and over 1,200 globally, making us one of the top patent awardees in the materials sciences category. We operate in 26 states, and have manufacturing in 11 of those states, including, a state of the art automobile emissions control facility in Erwin, New York, the world's most advanced optical fiber manufacturing plants in Wilmington and Concord, North Carolina, life science products facilities in California and Utah, and telecommunications products facilities in Arizona and Texas.

Corning's strategy for success is based on two key foundations. First, we invent and innovate with tenacity, consistently investing 8-10 percent of our sales in research, development & engineering (RD&E). Second, we manufacture efficiently. Invention is only valuable if you can successfully commercialize the product. So once we introduce a new product, we relentlessly drive down our cost of manufacturing through process engineering. Today, we are the world's lowest-cost manufacturer for 80 percent of the products we make.

Simply put, invention, innovation, and low-cost manufacturing through process engineering are the keys to success in American manufacturing.

Because of our commitment to RD&E, we have been fortunate to develop a number of life-changing technologies. In the 19th century, we invented the process to manufacture the glass envelope for Thomas Edison's light bulb. Subsequently, we invented the ceramic core of the catalytic converter that has removed 4 billion tons of harmful emissions from the atmosphere, optical fiber that enables the Internet, and LCD glass providing the foundation for display technologies in a wide range of consumer electronics. And when you touch your mobile phone, you are likely touching Corning® Gorilla® Glass, now found on 4.5 billion mobile devices worldwide. Inventions like these have earned Corning the National Medal of Technology and Innovation four times.

In order to protect those life-changing discoveries and provide the incentive to continue this innovation legacy, Corning relies on strong intellectual property protection, most importantly in the form of patents and trade secrets.

I am honored to testify before this Committee, which over the last two decades has passed numerous measures fundamental to the health of American innovation. For Corning your

dedication to patent protection has been particularly important. We applaud your work over the course of multiple Congresses to find common ground on the Leahy-Smith America Invents Act, and we appreciate your current efforts to make progress against patent trolls through the PATENT Act.

Today I am here to discuss trade secret protection and its importance to companies like Corning. Primarily I want to discuss the Defend Trade Secrets Act. Later I will discuss other steps the federal government can take to encourage global trade secret protection.

II. Trade Secrets Are Vital to a Company's Competitiveness

The know-how a company has developed and protects as a trade secret is often its key ingredient for success. A company that does not protect its know-how—or cannot protect it—cannot afford to continue innovating because its competitors will gain the same knowledge without having invested similarly in research and development.

Trade secrets are therefore among a company's most valuable assets. Trade secrets include a wide variety of confidential, commercially-valuable information, including proprietary technologies, formulas and codes, unique designs, industrial techniques, and customer lists. For high-tech manufacturers like Corning, they include manufacturing processes that give us a competitive edge in the global marketplace. And every innovative company, from large to small, relies on trade secrets in some fashion to set it apart.

As with other forms of intellectual property, trade secrets are often developed at significant cost. But, unlike other forms of intellectual property, the competitive advantage trade secrets provide depends on the information remaining confidential. Ensuring robust protection for trade secrets is therefore vital—it allows companies to maintain their edge, keeps workers on the job, and creates an environment that is conducive to continued innovation and creation of the next generation of ideas, processes, and products.

Unfortunately, trade secrets are increasingly the targets of theft and misappropriation. The threat may come from outside a company or from within—rival companies, foreign governments, and company insiders who recognize the value of our confidential information may take our trade secrets and sell them for their own profit, or use them to replicate our innovations at a fraction of the cost.

A 2014 analysis by CREATE.org and PwC estimates the value of U.S. trade secret loss at 1% to 3% of GDP annually, equating to \$160 billion to \$480 billion a year in a \$16 trillion economy.¹ Trade secret theft affects every segment of the U.S. economy, and the threat is growing: The 2013 U.S. Intellectual Property Enforcement Coordinator Report stated that the

¹ CREATE.org, PwC, *Economic Impact of Trade Secret Theft*, February 2014, available at <https://create.org/resource/economic-impact-of-trade-secret-theft/>.

FBI has experienced a 39 percent increase in new trade secret theft cases since 2009.² The 2013 Report of the Commission on the Theft of American Intellectual Property provides specific examples of trade secret theft against U.S. companies in chemical, aerospace, financial services, software, and other industries.³ The Commission, co-chaired by Dennis Blair and Jon Huntsman, found that “American companies of all sizes are victimized” by trade secret theft, which “is undermining both the means and the incentive for entrepreneurs to innovate.”⁴

III. Trade Secret Law Should Keep Pace with the Threat

Currently, the legal tools available to protect trade secrets in the United States include the federal criminal statute - the Economic Espionage Act (“EEA”) - and civil remedies available under various state laws. The EEA criminalizes the misappropriation of trade secrets for the benefit of a foreign government or for economic gain. It is an essential statute, but it is not a panacea. First, federal investigators and prosecutors have limited resources and are unable to bring charges in all cases of trade secret theft. Second, although the EEA punishes the wrongdoer, it provides no private cause of action for the victim to seek compensation for the theft.

At the state level, most states have enacted laws modeled on the Uniform Trade Secrets Act. These state law protections are important, but are less efficient and effective as the nature of our economy – and trade secret misappropriation – becomes more interstate and international.

Many of today’s innovative companies, both large and small, operate across state and international borders and have their trade secrets threatened by competitors around the world; they maintain company data digitally, trade around the globe, and may have employees in multiple states and countries. For these companies, the existing patchwork of state laws is inadequate for several reasons. First, trade secret theft often requires immediate action in order to preserve the value of the stolen property, particularly when a stolen trade secret is taken across state lines, or when the misappropriator seeks to leave the country. In many states, courts lack sufficient tools to act quickly to prevent dissemination of a stolen trade secret across state lines. Second, state courts lack procedures equivalent to federal court to seamlessly conduct cross-jurisdictional discovery. Because trade secret misappropriation often involves actors in multiple states, litigating in state court can be highly inefficient. Third, variation in state laws creates challenges for companies seeking an efficient, unified compliance plan, and results in the additional unnecessary cost of navigating different state laws.

² U.S. Intellectual Property Enforcement Coordinator, Joint Strategic Plan on Intellectual Property Enforcement, at 43 (2013), *available at* <https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipeec-joint-strategic-plan.pdf>.

³ The National Bureau on Asian Research, The Report of the Commission on the Theft of American Intellectual Property, at 39–45 (May 2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

⁴ *Id.* at 1.

IV. Importance of a Federal Civil Remedy for Trade Secret Misappropriation

Once a trade secret has been divulged, irreparable harm may be suffered because the value of the secret may be lost forever. In light of this reality, a consistent, unified body of trade secret law is necessary to fill the gap left by the EEA and state laws. Owners of other forms of intellectual property—patents, copyrights, and trademarks—can protect that property by enforcing their rights in federal court with a civil cause of action. We believe there should be corollary for trade secret protection.

In the two decades since Congress made it a federal crime to steal trade secrets, the nature of misappropriation has continued to evolve, and our laws protecting trade secrets should as well. Corning is proud to support the Defend Trade Secrets Act and encourages the Committee to move it forward with all appropriate speed.

The Defend Trade Secrets Act (S.1890/H.R. 3326) will create a uniform standard for the protection of trade secrets nationwide, improving the efficiency and predictability of litigation and allowing companies to create one set of best practices to protect their intellectual property in every jurisdiction. With a federal cause of action available, parties can streamline multi-state discovery and service of process, resulting in faster and less costly litigation. The legislation will also provide a mechanism for obtaining expedited relief when a company's trade secret is threatened with imminent destruction or dissemination. In extraordinary cases, this includes ex parte seizure of the stolen trade secret when necessary to preserve the value of the property. Of course, any legislation must be balanced, and the Defend Trade Secrets Act also contains safeguards to prevent abuse, including damages in the event of a wrongful seizure.

The Defend Trade Secrets Act enjoys support from large and small companies in industries as diverse as software, biotech, pharmaceutical, manufacturing, medical devices, semiconductors, agriculture, automotive, and apparel.

We thank Chairman Grassley and Ranking Member Leahy for their leadership on trade secret issues and intellectual property more generally. We thank Senators Hatch, Coons, and Flake for introducing this important legislation, and the Committee members who have co-sponsored the Defend Trade Secrets Act: Senators Durbin, Tillis, Blumenthal, Sessions, Klobuchar, and Perdue.⁵ Your consensus-oriented approach to this legislation has helped to attract support from all industry sectors, and we look forward to continuing to work together on this issue that is so important to the American economy.

V. Other Recommendations

⁵ We also thank Senators Ayotte, Baldwin, Blunt, Crapo, Kirk, and Risch for their cosponsorship of S.1890. In the House, H.R. 3326 was introduced July 29, 2015 concurrently and with language identical to S.1890 by Representatives Doug Collins, Nadler, Holding, Jeffries, Chabot, Conyers, Lamar Smith, DelBene, Richmond, Marino, Trent Franks, Deutch, Hanna, Reed, Guthrie and Farenthold. H.R. 3326 currently has a total of 90 cosponsors. We thank all the supporters of the bill.

We recommend three other actions by the federal government aimed at promoting trade secret protection internationally.

First, we believe every future international trade agreement to which the United States is a party should require all signatories to enact and enforce effective criminal and civil trade secret protections. Corning was one of many companies urging the adoption of such language in the Trans-Pacific Partnership, and we were pleased to see it included. (In fact, passage of the Defend Trade Secrets Act will help American trade negotiators secure such commitments in the future by providing a U.S. example of the civil-law component to complement the EEA as an example of the criminal-law component.)

Second, we urge the federal government to encourage other nations to adopt meaningful discovery practices in order to achieve equity in the access to sensitive company information through litigation. Most foreign countries lack the kind of open discovery process that is available in the United States. As a result, foreign companies suspected of misappropriation can simply refuse to respond to inquiries from their U.S. competitors, even when the U.S. company specifically describes the information believed to be stolen. The opaque nature of most foreign litigation systems thus becomes a shield for misappropriators, in contrast to the transparency of the U.S. system. We urge Congress and the Administration to work to achieve greater reciprocity from our major trading partners regarding the availability of sensitive company information in trade secret litigation.

Third, we recommend that the United States initiate an on-going dialogue on trade secret misappropriation with other nations equally committed to intellectual property protection. Such a dialogue would assist in developing effective international trade secret protection.

VI. Conclusion

Twenty years ago this Committee became a leader in the protection of trade secrets with the enactment of the Economic Espionage Act. We appreciate today the opportunity to discuss the need for federal civil protections. We urge you to enact the same legal protections for trade secrets that other forms of intellectual property have long enjoyed. A federal civil remedy for trade secret misappropriation will help safeguard valuable company information that serves as the foundation for American innovation. In addition, we recommend standard trade secret protection as mandatory in all international trade agreements, efforts to achieve greater reciprocity from our major trading partners regarding the availability of sensitive company information in trade secret litigation, and an on-going dialogue with other nations regarding trade secret misappropriation.

Thank you for the opportunity to appear before you today. We appreciate your leadership and look forward to working with you on trade secret protection and other important issues facing our nation.

Hearing on

**“Protecting Trade Secrets: the Impact of Trade Secret Theft on American
Competitiveness and Potential Solutions to Remedy This Harm”**

United States Senate Committee on the Judiciary

December 2, 2015

Written Statement of Karen Cochran

Associate General Counsel and Chief Intellectual Property Counsel

E. I. du Pont de Nemours and Company

Testimony of Karen Cochran
Associate General Counsel and Chief Intellectual Property Counsel
E. I. du Pont de Nemours and Company

December 2, 2015

Good morning Chairman Grassley, Ranking Member Leahy, and Members of the Committee. My name is Karen Cochran, Associate General Counsel and Chief Intellectual Property Counsel for E. I. du Pont de Nemours and Company (DuPont). Thank you for the opportunity to testify today on an issue of importance not only for my company—but for the American economy.

I want to express my support and appreciation for the leadership of Senators Hatch and Coons and their bi-partisan legislation, the Defend Trade Secrets Act, S. 1890. I also want to thank the Committee for your interest in trade secret protection.

I am here today on behalf of DuPont in support of S. 1890. DuPont has extensive experience in establishing, maintaining, and defending our trade secrets. It is our position that S. 1890 will provide an improved mechanism to protect trade secrets.

DuPont's History as an Innovator

Throughout our history, DuPont's research locations have been the birthplace of a diverse array of innovations found in homes, farms, and businesses across the United States and around the world. DuPont's long line of innovation includes well-known technologies and products from Kevlar® and Tyvek® to seed and crop protection. These products reached the market with ingenuity, many years of dedication, and with the support of intellectual property protection.

As an innovator, DuPont™ depends on intellectual property protection—including trade secrets. Realizing the full potential of our innovation often includes knowledge-building that can span decades. This work generates a range of intellectual property from patents to trade secrets.

DuPont recently defended the trade secrets for one of our well-known products, Kevlar®. This experience brought about our realization of the importance of S. 1890 and updating trade secret protection and remedies. In sum, I will share the highlights of our trade secret enforcement experience, the need for assured, direct access to a federal court for these cases, and generally why time is of the essence in trade secret theft.

DuPont's Experience with Trade Secret Theft and Litigation

The technology behind DuPont™ Kevlar® is a high-strength fiber used in a range of applications from protective body armor to fiber-optic cables. DuPont invested over fifty (50)

years of research and development to master this technology. Our product quality and manufacturing expertise have been unparalleled.

DuPont safeguards and maintains much of its valuable Kevlar® know-how as trade secrets. It was in 2006, however, that DuPont suspected that it had been a victim of trade secret theft. What we initially thought to be the misconduct of one ex-employee, turned out to be a sophisticated, large-scale trade secret theft of one of the most recognized and ground-breaking products in history. The federal criminal investigation led to indictments of Kolon Industries, Inc. under the Economic Espionage Act. The civil matter DuPont filed against Kolon would not be resolved until 2015.

As stated in the court record, Kolon ‘undertook various efforts to learn DuPont’s trade secrets...[and] find out how DuPont...operated...to produce a high quality...fiber at a profitable and price-competitive production level.’ To accomplish their goal, they recruited long-standing, former DuPont employees who had access to Kevlar® trade secrets throughout their employment with the company.

Fortunately, our case allowed us to access federal court. Even there, we experienced difficulty in determining the depth of the trade secret theft. We also experienced excessive delays. Court-compelled discovery indicated that Kolon had destroyed evidence. DuPont pursued these allegations with the assistance of a forensic expert, and the Court found Kolon to have deleted or destroyed considerable volumes of relevant evidence. After multiple motions to

compel, hearings and investigation to piece together what remained, this evidence destruction severely hampered DuPont's ability to prove its case.

What DuPont Learned in Trade Secret Litigation

Our nine-year effort to defend our Kevlar® trade secrets exemplifies the importance of S. 1890 and its modernization of trade secret law. We urge the committee to consider what we learned from trade secret litigation: (1) the need for assured, direct access to federal court; and (2) the need to reduce the risk of further trade secret dissemination or the destruction of evidence.

First, the federal court's experience with litigating complex technologies for other intellectual property disputes is a valuable tool in addressing comparable complexities in trade secret cases. Existing state law enforcement is inadequate to address the interstate and international nature of trade secret theft. A federal civil remedy would eliminate jurisdictional complications and provide the full spectrum of legal options available to owners of other forms of intellectual property. Our ability to be in federal court was a significant help in advancing the Kolon case.

Second, paper copies and locked cabinets are no longer the standard medium of storage and dissemination of information. Information is now in portable, electronic form. It can be hidden and rapidly shared, or as in the case with Kolon, quickly deleted. The seizure provisions enable a trade secret owner under limited, controlled conditions, to proactively contain a theft

before it progresses and the trade secret is lost. A seizure mechanism may have prevented Kolon's comprehensive destruction of evidence and eliminated or reduced the need for a lengthy, expensive litigation.

Conclusion

In conclusion, I urge the Committee to consider moving forward legislation, providing a federal process of certainty in allowing companies to protect their trade secrets in federal court. S. 1890, the Defend Trade Secrets Act, would represent a gold standard for national trade secret laws globally. Again, thank you again for the opportunity to testify today. I will be pleased to answer questions you may have or supply additional information for the record.

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

Introduction

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

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

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

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

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

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

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

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

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

Background of Trade Secret Law

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

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

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

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

Meanwhile, a school of thought had developed among commentators that trade secret law should be abolished altogether because it was inconsistent with, and therefore preempted by, federal patent law. This argument was famously rejected by the U.S. Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974). Two important public interests, the Court explained, were served by trade secret law: the "maintenance of standards of commercial ethics and the encouragement of invention." Without guaranteed secrecy, businesses would be left to expensive self-help security measures that would disadvantage smaller competitors and discourage dissemination of information through sharing. And as a practical matter, there was no conflict between the two systems because they operate so differently: patent law is strong, providing an exclusive right "against the world;" while trade secret rights are "weaker," because they do not protect against reverse engineering or independent development.

The Uniform Trade Secrets Act Has Failed to Produce Needed Uniformity

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

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

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

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

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

Existing Federal Laws Cannot Solve the Problem

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

³ For a comprehensive collection of state variations, see Sid Leach, *Anything but Uniform: A State-By-State Comparison of the Key Differences in the Uniform Trade Secrets Act* (2015) available at <http://www.swlaw.com/assets/pdf/news/2015/10/23/How%20Uniform%20Is%20the%20Uniform%20Trade%20Secrets%20Act%20-%20by%20Sid%20Leach%20-%20AIPLA%20paper.pdf>

⁴ See R. Mark Halligan, *Revisited 2015: Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 14 J MARSHALL REV. INTELL. PROP. L. 476, 494 (2015).

⁵ See 28 U.S.C. §1367; *United Mine Workers of America v. Gibbs*, 383 U.S. 715, 725 (1966); *Tech Enterprises, Inc. v. Wiest*, 428 F.Supp.2d 896, 902 (W.D. Wis. 2006) (dismissing trade secret claim because it did not share a "common nucleus of operative facts" with a trademark claim).

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

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

In other words, the time-critical nature of interstate and international misappropriation of valuable digitized data requires an immediate and sophisticated response mechanism, and neither state law nor the EEA criminal framework provides a satisfactory solution. Federal courts, however, can provide the necessary resource. First, under the DTSA federal courts would operate under a single, national standard for trade secret misappropriation and a transparent set of procedural rules, offering predictability and ease of use. Second, federal courts provide nationwide service of process and a unified approach to discovery, enabling quick action by trade secret owners even when confronted with actors in multiple jurisdictions. Third, as a result of their extensive experience with complex cross-border litigation involving intellectual property, federal courts would be able to resolve jurisdictional issues quickly and applications for injunctions or seizures fairly. Fourth, their generally more predictable discovery procedures will serve the legitimate needs of trade secret plaintiffs, who typically must develop most of the facts to prove their case through defendants and third parties.

The Defend Trade Secrets Act and the Law Professors' Opposition

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

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

⁷ 18 U.S. C. §§ 1831-1839.

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

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

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

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

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

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

9

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

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

The DTSA Will Create More Uniformity, Not “Undermine” It

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

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

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

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

¹¹ The EEA, at 18 U.S.C. § 1839(3), describes the scope of “trade secret” as “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.” The shorter definition of UTSA § 1(4) is “information, including a formula, pattern, compilation, program device, method, technique, or process”

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

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

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

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

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

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

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

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

The DTSA Ensures Free Mobility Of Labor

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

¹² Fed.R.Civ.Pro. 26.

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

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

Conclusion

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

EXHIBIT 1

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

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

By James Pooley¹

INTRODUCTION

Trade secret theft has been a federal crime since 1996, covered by the Economic Espionage Act (“EEA”).² But civil misappropriation claims remain limited to state court filings under common law or local variants of the Uniform Trade Secrets Act (“UTSA”). Calls for federal jurisdiction have grown with the increasing importance of information as a business asset and with the emergence of technology that makes theft of these assets almost infinitely easier. Recent examples involving international actors have galvanized the business community to request a straightforward solution: amend the EEA to provide a federal option for private claims.

Several bills were introduced in the 113th Congress to accomplish this, and to authorize provisional remedies for seizure of relevant property to prevent secret technology from being transferred out of the jurisdiction. The 2014 legislation was not acted on before Congress adjourned. A revised version is pending now, the Defend Trade Secrets Act of 2015 (“DTSA”), reflected in identical House (H.R.3326)³ and Senate (S.1890)⁴ bills.

¹ Mr. Pooley is a member of the California bar. He recently served as Deputy Director General of the World Intellectual Property Organization, an agency of the United Nations, where he was responsible for managing the international patent system. This service followed 37 years as a trial attorney handling hundreds of trade secret and patent disputes, many of them involving interstate and international actors. He has taught trade secret law and litigation as an adjunct professor at the University of California, Berkeley and at Santa Clara University. He is the author of the treatise “*Trade Secrets*,” first published by Law Journal Press in 1997 and continuously updated since then. He is also a co-author of the *Patent Case Management Judicial Guide* (Federal Judicial Center 2009, 2015). His most recent business book is *Secrets: Managing Information Assets in the Age of Cyberespionage* (Verus Press 2015). Mr. Pooley currently serves as Chairman of the Board of the National Inventors Hall of Fame, and is a past president of the American Intellectual Property Law Association. This paper was presented at the 2015 Annual Conference of the George Mason University School of Law Center for the Protection of Intellectual Property. The author wishes to thank his fellow presenters and the audience for their useful feedback. He also wishes to thank Mark Schultz for helpful comments and Jaci Arthur for her research support.

² 18 U.S.C. §§ 1831-1839.

³ <https://www.congress.gov/bill/114th-congress/house-bill/3326>

⁴ <https://www.congress.gov/bill/114th-congress/senate-bill/1890>

The current draft legislation has received broad support from a variety of industries,⁵ and also enjoys unusually bipartisan political sponsorship.⁶ However, a group of thirty-one law professors submitted opposition to the predecessor bills in the form of an “open letter” dated August 26, 2014.⁷ Among other objections, they complained that the seizure provisions created inappropriate risks to third parties, that injunctions were not sufficiently limited, and that increasing available remedies for misappropriation would lead to decreased employee mobility.

Anticipating a renewed effort in the 114th Congress, several professors, including three of those who had signed the open letter, published journal articles that expanded on their concerns.⁸ In the most recent of these, a new argument was offered: that federalizing civil trade secret law would unleash a dangerous new class of litigants called “trade secret trolls,” who, like their patent counterparts, would terrorize the community of legitimate innovators.

On July 29, 2015, the current legislation was introduced simultaneously in the House and Senate.⁹ Among other modifications, the new version tightened the seizure requirements, limited certain injunctive relief, and constrained judicial orders that would block an employee from accepting a new job. On August 3, the two authors of the “Trolls” article issued another open letter of their own, arguing that the changes were not enough and that the DTSA suffered from the same drawbacks as the previous proposals, leading to their prediction that it would “spawn a new intellectual property predator.”¹⁰ On November 17th, those authors were joined by 29 others in another open letter, contending that the legislation

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

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

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

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

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

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

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

In this article I offer a different perspective, informed not only by scholarship and public service but also by a professional lifetime of experience handling trade secret litigation and trials. As I will explain in more detail below, federalizing civil trade secret law would fill a critical gap in effective enforcement of private rights against cross-border misappropriation that has become too stealthy and quick to be dealt with predictably in state courts. The bills would accomplish this by effecting only very modest changes, relying heavily on existing laws and rules. The seizure provisions in particular are so narrowly drawn that only the most clearly aggrieved plaintiffs would risk invoking the procedure. Having no pre-emptive effect, the federal law would leave in place all relevant state laws and policies, including those relating to mobility of labor. Finally, I will argue that the specter of a new species of “trade secret troll” is so completely untethered to the realities of trade secret rights and disputes that it can safely be ignored.

BACKGROUND: THE DEVELOPMENT OF U.S. TRADE SECRET LAW

Unlike other types of intellectual property that have always been defined by statute, the origins of trade secret protection lie in the common law, catalyzed by nineteenth century industrialization that created a need to transfer and share secrets in business (which is why we refer to them as “trade” secrets). The law’s principles emerged from the results and reasoning of individual cases enforcing promises of confidentiality. Although many of the early cases emphasized the center of the inquiry as a confidential relationship that the law should respect, courts also recognized that the beneficiary enjoyed a property right in the expectation of secrecy.¹² But the courts’ logical emphasis on protecting a confidential relationship led the original framers of the Restatement to categorize trade secrets within the law of torts. The 1939 Restatement (First) of Torts §§ 757-59 thus was the first step in “harmonizing” state common law. However, forty years later when the Second Restatement was published, trade secrets were not covered at all. The reporters explained that in the intervening years the fields of unfair competition and trade regulation had encroached to such an extent that

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

¹² See, for example, *Peabody v. Norfolk*, 98 Mass. 452, 458 (Mass. 1868): If one “invents or discovers, and keeps secret, a process of manufacture, . . . he has a property in it, which a court of chancery will protect against one who in violation of contract and breach of confidence undertakes to apply it to his own use, or to disclose it to third persons.” Whether or not trade secrets may be counted as “property” – some of the academic opponents of the DTSA think it should not – has long been debated, but since secret information can be transferred and taxed like other property, the question seems to be moot. See JAMES H. POOLEY, *TRADE SECRETS* §1.02[8] (Law Journal Press, updated 2014).

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

This explanation was published about five years after the most important development in trade secret law of the twentieth century: the opinion of the U.S. Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*,¹⁴ in which petitioners claimed that state trade secret law should be pre-empted as conflicting with federal patent law, because the latter requires disclosure and the former protects against it. Finding no pre-emption, the Court explained that trade secret law was grounded on important public interests: “[t]he maintenance of standards of commercial ethics and the encouragement of invention.”¹⁵ Without guaranteed secrecy, businesses would be left to expensive self-help security measures that would disadvantage smaller competitors and discourage dissemination of information through sharing.¹⁶ And as a practical matter, there is no conflict between the two systems because they operate so differently: patent law is strong, providing an exclusive right “against the world;” while trade secret rights are “far weaker,” because they do not protect against reverse engineering or independent development.¹⁷

It was against this backdrop that the National Conference of Commissioners on Uniform State Laws in 1979 issued the first of two versions of the Uniform Trade Secrets Act.¹⁸ The need for the UTSA arose, according to the Commissioners, because development of the law among the states had been “uneven,” and therefore the standards and remedies established by common law were uncertain.¹⁹ Of course, the lack of treatment by the Restatement (Second) reinforced the need for an alternative path toward uniformity.

¹³ RESTATEMENT (SECOND) OF TORTS 1-2 (1979) Div. 9, Introductory Note: “the influence of Tort law has continued to decrease, so that it is now largely of historical interest, and the law of Unfair Competition and Trade Regulation is no more dependent upon Tort law than it is on many other general fields of the law and upon broad statutory developments, particularly at the federal level.”

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

¹⁵ *Id.* at 481. On the social interest in ethics, the court also noted that there is an “inevitable cost to the basic decency of society when one firm steals from another.” 416 U.S. at 487.

¹⁶ *Id.* at 485-86 (“The holder of a trade secret would not likely share his secret with a manufacturer who cannot be placed under binding legal obligation to pay a license fee or to protect the secret. The result would be to hoard rather than disseminate knowledge.”). See also 416 U.S. at 493: “Trade secret law promotes the sharing of knowledge, and the efficient operation of industry”

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

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

¹⁹ *Ibid.*

The UTSA tried to codify the fundamental principles of the existing common law of trade secrets, “preserving its essential distinction from patent law.”²⁰ But the common law had moved on since 1939, and the drafters of the UTSA effectively changed the Restatement rules in some significant ways. These shifts included broadening the scope of protection for information where its value was “actual or potential.” Section 757 of the Restatement had required that secrets be “in continuous use” in a business. Now, “ephemeral” data (such as private bids) and “negative” secrets (such as the results of failed experiments) would be protectable. On the other hand, under the Restatement (First) the trade secret owner’s self-help measures had been only a factor for consideration; under the UTSA those “reasonable efforts” became part of the required proof to establish a protectable secret.

What could constitute a misappropriation was also changed. Under the original Restatement mere acquisition of a secret, even if improper, was not actionable absent proof of use or further disclosure; while the UTSA addressed acquisition where the actor had reason to know that it had been accomplished by improper means.²¹ In the same vein, the Restatement of Torts had provided “immunity” for third parties who received secret information in good faith; whereas the UTSA adopted a rule that liability could be imposed following notice, subject to limited remedies based on a showing of innocent reliance by the user.²²

But as its name suggests, a primary objective of the UTSA was uniformity. On that score, the results have been disappointing. First, there are the two official versions, one issued in 1979 and the other in 1985 (mainly enhancing remedies), with a number of states having adopted the first before the second became available.²³ And quite a few states have enacted a customized version of the official one.²⁴ The notes to the Uniform Act acknowledge this by listing some of the individual states’ variations as annotations, adding a disclaimer that notes are not provided for states that “depart from the official text in such a manner that the various instances of substituted, omitted, and added matter cannot be clearly

²⁰ *Ibid.*

²¹ UTSA §1(2). See also RESTATEMENT (THIRD) OF UNFAIR COMPETITION §40, cmt. b (1995): “The prior Restatement of this topic imposed liability only for the wrongful use or disclosure of another’s trade secret. Improper acquisition of a trade secret was not independently actionable.”

²² UTSA §2(b). See comments.

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

²⁴ See Sid Leach, *Anything but Uniform: A State-By-State Comparison of the Key Differences in the Uniform Trade Secrets Act* (2015) available at <http://www.swlaw.com/assets/pdf/news/2015/10/23/How%20Uniform%20is%20the%20Uniform%20Trade%20Secrets%20Act%20-%20by%20Sid%20Leach%20-%20AIPLA%20paper.pdf>

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

Academics and practitioners have noted this lack of uniformity of the UTSA.²⁶ A few examples will help illustrate the scope of the problem. California dropped the language requiring that a trade secret be not “readily ascertainable,” with the result that the defendant is required to specially plead that circumstance as an affirmative defense.²⁷ Illinois also eliminated the “readily ascertainable” language, and it prohibits royalty injunction orders, sets a different limitations period and allows permanent injunctions.²⁸ Idaho requires that computer programs carry a “copyright or other proprietary or confidential marking” to qualify for protection.²⁹ Georgia limits protection of customer lists to physical embodiments, in effect allowing employees to appropriate such information in (human) memory.³⁰ South Carolina’s version of the UTSA requires a court hearing an injunction request to consider “average rate of business growth” in determining a head start period, and prescribes very particular rules for discovery of trade secret information, even for local discovery in aid of an action pending in another jurisdiction.³¹

In 1995 the Restatement (Third) of Unfair Competition was released, including a new treatment of the law of trade secrets at §§39-45. Although the new Restatement does an excellent job of summarizing and explaining the principles in a fashion broadly consistent with the UTSA, it has not yet achieved the level of acceptance that one might have hoped for. In fact, in states where the UTSA has not been adopted, courts still refer to the 1939 Restatement of Torts, sometimes applying its (now minority) position on, for example, the need to show “continuous use” of secret information.³²

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

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

²⁷ See James H. Pooley, *The Uniform Trade Secrets Act: California Civil Code §426, 1 SANTA CLARA H.T. L. J.* 193, 197-98 (1985).

²⁸ 765 ILCS §1065 (1988).

²⁹ Idaho Code §48-801(4)(c).

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

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

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

In 1996, in recognition of substantial lacunae in existing federal criminal remedies and with a particular focus on the challenge of foreign state-sponsored theft of trade secrets, the EEA was passed by Congress and signed into law.³³ The process of legislative consideration was swift and bumpy, with some last-minute amendments.³⁴ In the years since its enactment, the EEA has had a mixed record of success. In the view of one veteran prosecutor, the average of about eight prosecutions per year is a “languid pace” that probably has done little to create a deterrent effect.³⁵ In part this may be due to a reluctance of victims to bring cases to the prosecutor, either because of a loss of control or Fifth Amendment effects on civil claims,³⁶ or it may be due to a lack of resources or interest within the various offices of the U.S. Attorneys, who have discretion whether to accept qualifying cases.³⁷

PROPOSED LEGISLATION TO ADD A CIVIL CLAIM TO EEA

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

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

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

³⁴ *Id.* at 187.

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

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

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

³⁸ See, for example, Pace, note 26 *supra* (arguing that variation in state laws applying to easily portable secrets made it difficult for larger companies to predict the outcome of disputes, and that the lack of a unifying federal statute raised questions about whether the U.S. was in full compliance with its obligations under international treaties).

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

⁴⁰ See, e.g., Lao, note 26 *supra*.

⁴¹ See Almeling, note 26 *supra*.

well as the procedural advantages for trade secret owners, including national service of process.⁴² Most commentators favoring a federal law have argued that it should explicitly preempt state law, in order to achieve the maximum benefits of uniformity. However, even a supplemental procedure – a choice of federal forum – would likely provide most of the expected advantages, without having to overcome opponents’ arguments that states provide a useful “laboratory” for experimentation and that preemption might endanger important state policies.⁴³

Congressional efforts to provide a national civil claim for trade secret theft began in earnest in 2011, with the introduction of a proposed amendment to other legislation.⁴⁴ The amendment would have added a private civil remedy to the EEA, together with an ex parte seizure provision patterned on language from the Lanham Act. That effort failed to secure a vote on the amendment. The following year Senator Coons, along with Sens. Kohl and Whitehouse, introduced S.3389, the Protecting American Trade Secrets and Innovation Act, a revised and somewhat more comprehensive version of the 2011 proposal, using language from the EEA and UTSA to define the subject and remedies, and again including a provision for ex parte seizures on very specific showings. The bill did not progress.

In the 113th Congress, several bills sought to create a private right of action under the EEA. The Defend Trade Secrets Act (S.2267) (2014 DTSA), introduced by Sens. Coons and Hatch, was substantially similar to S.3389 from the previous Congress, although it proposed a limitations period of five years rather than three. Earlier, S.1770 had been introduced by Sen. Flake as the Future of American Innovation and Research Act, with language and provisions similar to the Coons-Hatch proposal, but maintaining a three-year limitations period and adding a section covering anti-suit injunctions. In the House, Rep. George Holding led a bipartisan group in submitting H.R.5233, the Trade Secrets Protection Act of 2014 (TSPA), again with a structure similar to S.2267 but providing more detailed constraints on the seizure process. Finally, Rep. Zoe Lofgren introduced H.R. 2466, the Private Right of Action Against Theft of Trade Secrets Act, a two-

⁴² R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656, 667-68 (2008). Mr. Halligan has recently updated his comprehensive treatment of the subject in R. Mark Halligan, *Revisited 2015: Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 14 J. MARSHALL REV. INTELL. PROP. L. 476 (2015).

⁴³ See Seaman, note 8 supra, at 365-67. The fear of federal trade secret law displacing any state’s rules on the separate question of noncompete covenants is overdone, even under a preemptive regime. However, the current bills are explicitly non-preemptive and so the concern is even more abstract.

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

paragraph amendment to the EEA that would have added a civil cause of action, but without the ex parte seizure provisions. The TSPA was favorably reported out of committee, but no other action was taken, and all four bills expired at the end of the 113th Congress.

LAW PROFESSORS' OPPOSITION

While industry expressed virtually unanimous support for the 2014 DTSA and the TSPA, and both received unusually bipartisan backing, opposition to the bills arrived in the form of a letter signed by thirty-one law professors engaged in “intellectual property law, trade secret law, innovation policy and/or information law.”⁴⁵ The letter argued that there was no apparent need for the legislation, because “effective and uniform state law already exists,” current procedures for interstate and foreign process were adequate, and access to federal courts for state law claims was available under diversity jurisdiction. It claimed that the bills would not solve any perceived problems, because they would leave in place potentially determinative “ancillary state law” issues and because they failed to address the challenge of establishing jurisdiction over foreign actors. And it complained that enactment of the legislation would cause serious harm, by imposing a dangerous process for ex parte seizures, ignoring the right to reverse engineer, and raising the prospect of indefinite injunctions. Requiring definition of secrets early in litigation to address jurisdiction issues, it added, could increase the risk of improper disclosure. Finally, it suggested that the new laws could be used “as an additional weapon to prevent public and regulatory access to information, collaboration amongst businesses, and mobility of labor.” Congress, the letter concluded, should redirect its attention away from trade secret misappropriation and instead focus on legislation to combat “cyber-espionage and foreign espionage.”

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

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

⁴⁵ See *2014 Professors’ Letter*, note 7 *supra*.

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

Although a non-preemptive federal statute could lead to related issues of state law being resolved in some cases, federal courts have demonstrated in other areas of concurrent jurisdiction that they are quite capable of resolving those issues. They have also proven capable of using protective orders to prevent loss of secrecy in the courtroom. In addition, it is safe to assume that, because of their generally more extensive experience with international litigation, federal judges are well equipped to efficiently handle difficult questions of personal jurisdiction over foreign defendants.

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

It is on their last cluster of arguments that I find myself in strongest disagreement with the professors’ 2014 letter. The idea that collaboration among businesses would somehow be diminished because litigants could sue in federal court makes no sense. Indeed, it is the very existence of judicial remedies for misappropriation that makes business collaboration possible. As the Supreme Court explained in *Kewanee*: “The holder of a trade secret would not likely share his secret with a manufacturer who cannot be placed under binding legal obligation to pay a license fee or to protect the secret. The result [of preempting trade secret law] would be to hoard rather than disseminate knowledge.”⁴⁷

Similarly, the proposition that adding a federal civil cause of action for misappropriation would reduce public or regulatory access to critical information is a non sequitur. The legislation would affect only a private interest in information, and the Freedom of Information Act and other statutes that form the federal edifice of health and safety regulation would not be changed at all.

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

⁴⁶ *Id.* at 3

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

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

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

Third, the professors claim that the DTSA "likely will increase the length and cost of trade secret litigation," with consequential damage to "small businesses and startups." As with many of their other points of opposition, this one rests on overstatement and speculation. Although the law would only apply to trade secrets that are "related to a product or service used in, or intended for use in, interstate or foreign commerce," there is nothing in our experience with similar

⁴⁸ The letter relies on a brief essay which itself appears to have drawn from the professors' earlier correspondence. John Tanski, *The Defend Trade Secrets Act Is Strong Medicine. Is It Too Strong?*, Corporate Counsel (October 30, 2015), available at <http://www.corpcounsel.com/id=1202741205249/The-Defend-Trade-Secrets-Act-Is-Strong-Medicine-Is-It-Too-Strong?slreturn=20151009142017>. The author incorrectly asserts that the DTSA would allow a court to "shut down the defendant's business for up to a week." His fears of "trade secret trolling" are based on the claim that trade secret law covers so much information that "it is easy for unscrupulous plaintiffs to manufacture trade secret claims and use them as strategic weapons." But he fails to acknowledge that this broad scope of the law has not led to any epidemic of false claims in state courts, much less explain why nuisance suits or the imagined "trolls" would be more likely to emerge under the scrutiny of federal judges.

⁴⁹ The letter claims, without citation of evidence or authority, that in states that recognize the concept of inevitable disclosure, "the typical remedy is to enjoin the departing employee from commencing employment until the subject trade secret information is no longer a trade secret." See *2015 Professors' Letter*, note 11 *supra*, at 4-5. My own review of the case law reveals instead that "the outcome usually will not be an outright ban on employment, but a more limited injunction that permits the employee to go to work but forbids participation in some particular product line or area of the business." See Pooley, *Trade Secrets*, note 12 *supra*, at §7.02[2]. Indeed, orders not to take a job are "exceptional," and usually occur only when some form of noncompetition agreement is already in place, or there is clear evidence of fraud or bad faith. *Ibid.*

federal laws that would suggest this requirement could not easily and quickly be met with uncontroverted proof, much less that it would “both delay the case and result in increased costs” of litigation. And although the letter cites survey evidence demonstrating the substantial cost of trade secret litigation, that applies equally in state court proceedings where discovery can be as extensive and produce as many collateral disputes.⁵⁰

Finally, the letter returns to the argument made in 2014, that existing state law is “coherent,” “robust and uniform,” so that U.S. businesses already enjoy “a high level of predictability.” As I have already pointed out, this dismissive rhetoric hardly obscures the reality of a patchwork of differing standards and rules – in some ways more divergent than before enactment of the UTSA – that necessarily create friction and inefficiency for companies with interstate operations. Indeed, one might suppose that is why the DTSA enjoys such broad support in the business community. The professors also submit, without offering analysis or examples, that whatever uniformity now exists will be undermined by the EEA’s supposedly “broader” definition of a trade secret.⁵¹ Finally, they point out the obvious: by failing to make the federal law preemptive, the trade secret holder will have a choice of forum, which they characterize as “forum shopping.”

I turn now to the law review articles that followed issuance of the 2014 professors’ letter. The first of these, by Zoe Argento of Roger Williams University Law School, is entitled *Killing the Golden Goose: the Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation*.⁵² It treats the issue of cyber-espionage comprehensively and clearly, but that strength highlights the main problem with its logical structure. In her attack on the legislation, Professor Argento begins by assuming that the only problem to be solved is cyber-espionage. From there she proceeds to critique the legislation mainly on the basis that it would not solve that problem. And while it is undoubtedly true that giving private parties the right to sue in federal court is unlikely to put much of a dent in the international hacking scourge, that is certainly not the only problem that the bills confront. Instead, their main objective is to make it more practical for trade secret owners, in an age where their rights

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

⁵¹ In fact, the EEA and the UTSA merely use different exemplary terms to express precisely the same idea: that the potential scope of trade secret protection is almost infinite. The EEA includes “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes.” 18 U.S.C. §1839(3) But every one of those categories also qualifies under the UTSA definition, which applies to “information, including a formula, pattern, compilation, program, device, method, technique, or process.” UTSA §1(4).

⁵² See Argento, note 8 supra.

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

While I disagree with some of the other propositions advanced in the Argento article, in particular her treatment of the “property” theory,⁵³ it is helpful to point out a few illuminating statements. First she acknowledges that the North Carolina and Alabama trade secret statutes “vary significantly” from the UTSA.⁵⁴ She also agrees that significant advantages come with access to federal courts, noting that actors in a case involving cyber theft are “more likely to reside in a different state or even a different country,” and that discovery is much more of a challenge in state court, where the proponent has to petition the courts of both relevant states.⁵⁵

The second major article to appear in opposition to the proposed legislation is by Christopher Seaman of Washington and Lee University School of Law, titled *The Case Against Federalizing Trade Secrecy*.⁵⁶ This is a prodigious and scholarly work, comprising 77 pages and 492 footnotes. But it is worth the read. Professor Seaman leaves no reasonable issue untouched in his review of the law that provides context for the bills, and his analysis is generally fair and often insightful. However, in line with the professors’ letters, he overstates the extent of trade secret law harmonization that has been achieved by the UTSA and as a result minimizes the benefit of a unifying federal influence.⁵⁷ And while one of his key theses is that federalization risks abandoning the advantage of the states as

⁵³ *Id.* at 182-86, where the author equates the policy objective of encouraging innovation with a “property theory” (in contrast to a “tort theory” focusing on ethical behavior) that is supposedly inimical to the free movement of labor because it grants “exclusive rights” to the trade secret holder. I believe that the dispute between the “property” and “confidence” schools of thought is of historical interest only, and that modern law recognizes both interests. See note 11 *supra* and accompanying text. I also am concerned with Professor Argento’s choice of vague and undefined terms in relation to trade secret law, such as “over-protection,” “over-broad” and “strong” protection. In my experience, this kind of value-laden terminology is too frequently used in place of rigorous analysis of the competing interests that are almost always present in this area of the law.

⁵⁴ *Id.* at 178 n. 23. See also p. 208 n. 204: “States vary on what constitutes misappropriation, the definition of a trade secret, the length of injunctions, exemplary damages, attorney fees, and the statute of limitations.”

⁵⁵ *Id.* at 210.

⁵⁶ See Seaman, note 8 *supra*.

⁵⁷ For example, he says that “most jurisdictions follow the UTSA’s substance on the main points and depart only on less frequently encountered issues, such as the availability and amount of exemplary (punitive) damages.” *Id.* at 354. He is probably correct that “most” of the 47 jurisdictions follow the substance of the UTSA, but that leaves quite a few whose variations can matter quite a bit depending on circumstance. For example, the attorney appearing in a California case and unaware of its special requirement to plead ready ascertainability is likely to neglect that procedural detail and as a result waive the substantive claim. See note 25 *supra* and accompanying text. Similarly, when Professor Seaman points out that “only” eight states provide different limitations periods, he is making a value judgment that companies dealing with these differences may not share. *Id.* at 355

“laboratories” for experimentation with differing policies,⁵⁸ he gives little weight to the fact that the bills are expressly non-preemptive, leaving the states free to test policy choices as they wish.

Also in line with the first professors’ letter, Professor Seaman laments what he sees as an inverse relationship between the “strength” of trade secret law and the amount of useful information that is made available to the public. In fact, he hypothesizes a “bell curve” in which “weak” protection of secrets will (as *Kewanee* recognized) lead to less disclosure, but in which “too much trade secret protection” will have the same result.⁵⁹ There are multiple problems with this construct, not the least of which is the elusive abstraction of “strength” of the law and how to measure it. That failing shows up clearly when one tries to apply the notion to the pending bills. Just what is “too strong” in this context?⁶⁰ The way he uses the phrase, the substantive (scope of rights) is conflated with the procedural (choice of court where rights will be enforced). If one considers the shift in trade secret law from the 1939 Restatement of Torts to the modern rule of the UTSA, there was undoubtedly some “strengthening” taking place. But by any rational comparison, the modest procedural changes inherent in the DTSA amount to more of a tweak than a departure.

Along the same lines, Professor Seaman argues that “federalizing trade secrecy would create more robust rights against extraterritorial conduct compared to patent law.”⁶¹ The observation seems intuitively correct, but why is that a problem? Patents are a strictly territorial government-granted franchise, while trade secrets are established by a private relationship of confidence, the violation of which is commonly addressed wherever the parties are located, the bad behavior occurs, or its effects are felt.⁶²

⁵⁸ *Id.* at 365.

⁵⁹ *Id.* at 385.

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

⁶¹ *Id.* at 380.

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

Like Professor Argento, Professor Seaman acknowledges that there could be benefits accruing to trade secret owners from having access to a federal forum. Specifically, he agrees that there is “some force” to the claimed advantages of nationwide service of process, broader jurisdictional reach over foreign defendants, more liberal discovery rules, and greater experience of federal judges in handling “complex IP and commercial disputes.”⁶³ But he argues that these benefits can be achieved without amending the EEA, by litigants asserting their rights to federal diversity and supplemental jurisdiction.⁶⁴ Of course, as already noted, complete diversity is often not present in trade secret disputes; and supplemental jurisdiction requires a common set of “central facts,” which also is frequently absent.⁶⁵ Indeed, the weakness of his argument is underscored by his proposed alternative to the bills: Congress should remove the complete diversity requirement just for trade secret cases.⁶⁶

The most unusual of the three articles is *Here Come the Trade Secret Trolls*, by David Levine of Elon University School of Law and Sharon Sandeen of Hamline University School of Law.⁶⁷ It relies heavily on the Argento⁶⁸ and Seaman articles but does not supply any new evidence or fresh analysis.⁶⁹ Instead, its main contribution is to repeat in various ways a strikingly implausible prediction: that the pending legislation would “allow trade secret trolls to roam free in a confused and unsettled environment, threatening or initiating lawsuits for the sole purpose of exacting settlement payments, just like existing patent trolls.”⁷⁰

⁶³ See Seaman, note 8 supra, at 368.

⁶⁴ *Id.* at 369.

⁶⁵ See 28 U.S.C. §1367; *United Mine Workers of America v. Gibbs*, 383 U.S. 715, 725 (1966); *Tech Enterprises, Inc. v. Wiest*, 428 F.Supp.2d 896, 902 (W.D. Wis. 2006) (dismissing trade secret claim because it did not share a “common nucleus of operative facts” with a trademark claim).

⁶⁶ See Seaman, note 8 supra, at 386.

⁶⁷ See *Trolls*, note 8 supra.

⁶⁸ Like Argento, the authors of *Trolls* begin their attack on the bills by assuming incorrectly that the only issue being addressed is cyberhacking. For this assumption they rely on a press release from Sen. Coons’ office. *Id.* at 233-34. But even that selected document does not demonstrate such a narrow focus: “In today’s electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor.” In other words, the core problem arises from changes in technology and the globalization of business. The authors’ straw man attack then becomes an argument (at 238-43) that we need more data on cyberhacking before considering legislation.

⁶⁹ Indeed, many of its propositions are notable for the lack of any evidence or analysis. For example, the authors dismiss concerns over variations in state versions of the UTSA as “some minor but insignificant differences,” without addressing why the variations should not matter. *Id.* at 243. And they trivialize the advantages of a federal choice of forum by simply asserting, without citation of any reference, that existing laws addressing interstate discovery “are not onerous” and that trade secret lawsuits involving foreign defendants are “rare.” *Id.* at 251.

⁷⁰ *Id.* at 252.

“Patent troll” is a pejorative term deriving from the child’s story about a troll who surprised unsuspecting passers-by to demand payment for crossing a bridge. It is most often applied to companies whose only business consists of buying up and asserting patent rights. The metaphor works in that context because patents are an easily alienable right issued by the government, are effective “against the world,” and can be infringed regardless of fault. Trade secrets, in stark contrast, are private rights that can be asserted only against a thief or one who has breached a confidence. Although frivolous trade secret lawsuits have occasionally been filed, existing law has sufficient sanctions to deal with those instances, and the bills contain precisely the same penalties. As I will explain in more detail below, there never has been such a thing as a “trade secret troll,” and there is no reason to believe that the pending legislation will cause this imagined beast to materialize.

THE 2015 BILLS

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

The provisions covering *ex parte* seizure of property are extensive and tightly drawn. An application must be accompanied by a sworn affidavit from which it “clearly” appears “from specific facts” that injunctive orders under FRCP Rule 65 would be insufficient because the defendant would evade them, that the seizure is necessary to prevent immediate and irreparable injury to the trade secret holder, and that the harm from refusing the order would exceed the harm to the defendant or any third party from issuing it. The application must also demonstrate likelihood of prevailing on the elements of the misappropriation claim, describe with particularity the material to be seized, prove the danger that the material will be moved or lost, and certify that there has been no publicity of the requested seizure.⁷¹

Seizure orders cannot be issued in summary form, but are required to contain findings of fact and conclusions of law, and must be drawn as narrowly as possible to achieve their purpose while minimizing interruption of any directly related business and preventing interruption of the defendant’s unrelated operations. The plaintiff must post a bond to secure liability for a seizure that turns out not to have been justified, but the amount of the bond will not limit damages that can be claimed for wrongful seizure. The order (which must be served by federal marshals) can remain in effect only seven days before a hearing

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

is held, at which the plaintiff must show facts justifying continuation of the order and at which the court may modify the normal discovery timeframes.⁷² (Because the legislation is silent on the issue, presumably the court in parallel with the seizure process may entertain proceedings for more common forms of injunctive orders under Rule 65.)

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

Regarding the more prosaic aspects of trade secret remedies, the bills follow closely the language of the Uniform Trade Secrets Act, allowing for injunctions against “actual or threatened” misappropriation, but adding a limitation that any order may “not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation.”⁷³ This provision was apparently intended to address concerns about employee mobility and the “inevitable disclosure doctrine,” a subject that was raised in the professors’ letters and is discussed in more detail below. Familiar language from the UTSA defines injunctions requiring affirmative actions and in exceptional circumstances imposing a reasonable royalty for no longer than use of the trade secret could have been prohibited.⁷⁴

Damages are to be calculated as provided under the UTSA, consisting of the plaintiff’s actual loss, together with any unjust enrichment not otherwise accounted for. Willful and malicious misappropriation can trigger an award of treble damages, plus attorney’s fees. Consistent with the UTSA, attorney’s fees may also be awarded to a defendant if a claim of misappropriation is found to have been prosecuted in bad faith.⁷⁵

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

⁷² *Id.* at §2(b)(2)(B-D).

⁷³ *Id.* at §2(b)(3)(A)(i).

⁷⁴ *Id.* at §2(b)(3)(A)(iii).

⁷⁵ *Id.* at §2(b)(3)(B-D).

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

criminal behavior, the bills add a definition of “misappropriation” to §1839 that tracks the language of the UTSA, but that also specifies that “improper means” may not include “reverse engineering or independent derivation,” another concern that was highlighted by the 2014 professors’ letter.⁷⁷

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

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

THE PROPOSED LEGISLATION MEETS A REAL NEED

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

Now return to the present and you will readily understand why this scene only three decades distant seems so impossibly quaint. With the arrival of ubiquitous digital devices with massive storage and robust wireless communications, the risk

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

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

⁷⁸ *Id.* at §2(f).

⁷⁹ *Id.* at §3(b).

⁸⁰ *Id.* at §4.

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

profile of holding trade secrets has been profoundly and irretrievably altered. Never have information assets been so vulnerable to loss.

And never have they been so valuable. As reported by Ocean Tomo, the share of public company value represented by intangible information leapt from 17% in 1975 to 68% in 1995 to 84% today.⁸² This means that industry in the span of a single generation has experienced a shift of historic proportions in the kind of property it uses to create value.

In another important shift, the way that companies choose to protect their investment in their innovations has moved away from a concentration on patenting and towards trade secrets. This was first reported in 2000 by researchers at Carnegie-Mellon,⁸³ and was confirmed by a 2012 report from the National Science Foundation and the Census Bureau. They found that, among “R&D-intensive” firms – who collectively account for two thirds of U.S. R&D investment – secrecy was deemed important at more than twice the level of patents.⁸⁴

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

In short, the risk of trade secret misappropriation is now digital and global, and the remedies to address it have to be a match for the risk. Viewed in that light, the current situation faced by U.S. industry is sadly inadequate. State laws are far from uniform, placing a burden on companies with regional or national operations.⁸⁵ This is not an abstract problem. A trade secret owner who learns of

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

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

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

⁸⁵ Identification of secrets in litigation is one example of a procedural issue unique to some states that can affect the progress of a misappropriation case. In California, no discovery by the

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

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

Suppose the trade secrets case is pending in state court in Illinois and discovery establishes that a critical witness with potentially smoking-gun evidence resides in California. The first step required is the filing of a motion in Illinois state court requesting the Illinois court to issue a discovery petition authorizing the out-of-state deposition. After obtaining the Illinois court order, a special action must then be filed in California to obtain a court order from the California court under the doctrine of comity among states to authorize the valid issuance of the subpoena in California to the California resident. The whole process can take months with briefings both in the Illinois courts and the California courts.⁸⁶

It is no answer to suggest, as have Professors Levine and Sandeen, that federal prosecutors stand at the ready to take such cases to federal court under the current EEA criminal provisions.⁸⁷ The reality is starkly different, as described by former EEA prosecutor Peter Toren, who has analyzed the relatively “languid pace” of filings (eight per year on average) under the statute.⁸⁸ As Mr. Toren points out, EEA investigations and prosecutions are “resource intensive and complex,” often requiring technical expertise that prosecutors do not possess, and as a result they are inclined to exercise their discretion to refuse the case in favor of handling other matters. This “reluctance to prosecute EEA cases is reinforced” by internal guidelines that disfavor prosecution when the victim has a civil remedy, as most do.

In short, the time-critical nature of interstate and international misappropriation of valuable digitized data requires an immediate and sophisticated response mechanism, and neither state law nor the EEA criminal framework provides a

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

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

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

⁸⁸ See Toren, note 35 *supra*.

satisfactory solution. Federal courts, however, can provide the necessary resource. First, they will be operating under a single, national standard for trade secret misappropriation and a transparent set of procedural rules, offering a much-needed level of predictability and ease of use. Second, they provide nationwide service of process and a unified approach to discovery, enabling quick action by trade secret owners even when confronted with actors in multiple jurisdictions.⁸⁹ Third, as a result of their extensive experience with complex cross-border litigation involving intellectual property, they will be able to resolve ex parte matters fairly and jurisdictional issues quickly and efficiently. Fourth, their generally more predictable and uniform discovery procedures will serve the legitimate needs of trade secret plaintiffs, who typically must develop most of the facts to prove their case through defendants and third parties.⁹⁰

Having reliable access to federal courts in trade secret cases requires that the EEA be amended. It is not sufficient to say that plaintiffs can get there through diversity jurisdiction, since complete diversity is required, and many trade secret cases will not qualify due to the involvement of one or more local defendants. And supplemental jurisdiction is not the answer either, since not all cases present the opportunity to plead a claim based on federal law, and in any event the decision to exercise supplemental jurisdiction depends on finding a common core of facts.⁹¹

THE SEIZURE REMEDY IS NARROWLY DRAWN TO A SPECIFIC NEED

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

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

⁹⁰ See *Greenberg v. Croydon Plastics Co., Inc.*, 378 F.Supp. 806, 814 (E.D. Pa. 1974): "Plaintiffs in trade secret cases, who must prove by a fair preponderance of the evidence disclosure to third parties and use of the trade secret by the third parties, are confronted with an extraordinarily difficult task. Misappropriation and misuse can rarely be proved by convincing direct evidence. In most cases plaintiffs must construct a web of perhaps ambiguous circumstantial evidence from which the trier of fact may draw inferences which convince him that it is more probable than not that what plaintiffs allege happened did in fact take place. Against this often delicate construct of circumstantial evidence there frequently must be balanced defendants and defendants' witnesses who directly deny everything."

⁹¹ See note 64 supra and accompanying text.

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

But allowing an ex parte seizure is categorically unacceptable to the authors of the *Trolls* article, who suggest instead that the victimized business should use its rights under existing law to “search company premises, requiring the return of company property, or engage in timely exit interviews.”⁹³ Such self-help measures can work well in an environment where the departing employee is cooperative, but in a more hostile situation they are utterly impractical. The same is true for the authors’ proposed solution that “larger and more sophisticated companies” can place a “legal hold” on their records in anticipation of litigation.⁹⁴ But the most unfathomable of the authors’ arguments on this point is that destruction of records is actually “beneficial to the trade secret owner to the extent it eliminates the threat of wrongful disclosure or use of the information”⁹⁵ This sort of reasoning not only trivializes a serious wrong but also invites a new, and dangerous, perspective on spoliation of evidence.

While our court system must provide a realistic ex parte remedy to prevent prospective catastrophic loss of information assets, we also should insist that the remedy be drawn narrowly, to permit intervention only to the extent required, with appropriate disincentives against abuse. The bills appear to strike that balance well. In the first place they demand compelling proof of a real risk of disappearance or destruction of the trade secrets. From the sworn affidavit it must “clearly appear” that a restraining order under Rule 65(b) – for example, an order preventing destruction or removal from the jurisdiction – would be ineffective because “specific facts” demonstrate that the defendant “would evade, avoid, or otherwise not comply with such an order.” The plaintiff’s abstract fear – for example, based on the defendant’s access to the information and its easily transportable character – will not be enough.⁹⁶ Instead, judges will have to see clear evidence of relevant behavior, such as excessive downloading followed by reformatting of the company laptop, revenge-tainted threats, missing files, attempted improper access to data, and the like, which when considered in context convinces the court that the secrets are in immediate peril.

⁹² Cf. *First Technology Safety Systems, Inc. v. Depinet*, 11 F.3d 641, 652 (6th Cir. 1993) (reversing a district court seizure order where facts were insufficiently specific to justify ex parte relief).

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

⁹⁴ *Ibid.*

⁹⁵ *Ibid.*

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

This statutory framework is not new; it has been used in the field of counterfeit goods.⁹⁷ The Lanham Act provisions for ex parte seizure are nearly identical to those in the bills, allowing the remedy only where it “clearly appears from specific facts” that another kind of order would not suffice.⁹⁸ The parallels continue with requirements for specific findings supporting a balance of harm in favor of the proponent due to an imminent danger of irreparable harm, and that the court hold the seized material and prevent publicity of the proceedings.⁹⁹

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

When considering the possibility of abuse by the applicant, one has to recognize not only the difficulty of making the case but also the penalties for not getting it right. The plaintiff must post a bond, but the bond will not limit the amount that the defendant and others affected by the order may claim for damages. Moreover, federal judges are not known for suffering fools gladly, and they have substantial powers to sanction inappropriate behavior under Rule 11.¹⁰¹ What plaintiff – or plaintiff’s counsel – would take that sort of open-ended risk for a few days of inconvenience meted out to a former employee or competitor? And if the claim is truly and obviously meritless, why would a defendant “capitulate,” rather than just file an opposition?

The authors of the *Trolls* article argue that in spite of all the restrictions the potential for abuse remains, because a trade secret owner could exact a settlement payment by sending out letters threatening an ex parte seizure application.¹⁰² But

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

⁹⁸ 15 U.S.C. §1116(d)(4)(B).

⁹⁹ 15 U.S.C. §1116(d)(5)-(7).

¹⁰⁰ It is therefore difficult to comprehend how the authors of the 2015 professors’ letter could assert that “an alleged misappropriator will be unable to immediately and meaningfully challenge the plaintiff’s assertions” in an ex parte application. See *2015 Professors’ Letter*, note 11 *supra*, at 3. There is no reason that the defendant could not mount such a challenge the same day or the next.

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

¹⁰² See *Trolls*, note 8 *supra*, at 255 (before the court could act on an application, “adjudication may happen in the marketplace, where the recipient of a trade secret troll’s letter (which would

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

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

The professors' letter of August 2014 claimed that the previous draft legislation would "limit mobility of labor,"¹⁰³ but did not explain exactly why this was so. In the articles published since then, the contours of the argument began to emerge. Professor Argento built her position on the assumption that "trade secret rights are intended to serve the public interest, not trade secret holders specifically."¹⁰⁴ This was a novel reinterpretation of the rationale laid down by the Supreme Court in *Kewanee*, which recognized the twin policy objectives of enforcing commercial morality and encouraging innovation. Naturally the public benefits indirectly from ethics in business and from the innovative work of industry. But the immediate beneficiary of trade secret law is the one holding the secret, because without the law's support the holder (in particular a small business) would be harmed by expensive and inefficient self-help measures deployed to keep information secret.¹⁰⁵ From her public interest-centered position, Argento argued that departing employees can serve society through a "cross-pollination effect" resulting from "seepage of useful information that benefits the public."¹⁰⁶

The Seaman article developed the point further by invoking the so-called "inevitable disclosure doctrine," a subject that gained prominence (or notoriety, depending on your point of view) following a court ruling that prohibited an executive from taking the same job with a direct competitor, because the circumstances indicated a threat of disclosure or use of the secrets he knew.¹⁰⁷ Using "inevitable disclosure" as an example, Seaman argued that federalizing trade secret law could endanger free movement of labor by removing the states' ability to serve as "laboratories" for competing policy positions.¹⁰⁸ He forecast the result that "firms that engage in innovation protected by trade secrecy would no

threaten a seizure action) will have to decide if it has the capacity and resources to challenge the claim in court. If it does not . . . the practical impact could be a settlement payment and, potentially, the end of the business. Innovation may be lost, jobs may be terminated, and lives may be devastated based upon an unproven allegation or a seizure remedy improperly issued.").

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

¹⁰⁴ See Argento, note 8 *supra*, at 202.

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

¹⁰⁶ See Argento, note 8 *supra*, at 188.

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

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

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

The 2015 professors’ letter goes further, arguing that the new version of the DTSA “implicitly recognize(s)” the doctrine, which it claims can “prevent individuals from being able to feed their families.”¹¹⁰ The specific language in the bills begins with a provision taken directly from the UTSA, which as already noted authorizes injunctions to prevent “actual or threatened misappropriation.”¹¹¹ The DTSA adds this proviso: “provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation.” The plain meaning reflects an intent that courts be able to set reasonable conditions on employment, in order to avoid circumstances that would threaten the integrity of secret information. But for the professors, the proviso triggers a focus on the assumed evil of the abstract “doctrine,” an assumption that is unjustified.

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

¹⁰⁹ *Id.* at 367. Professor Seaman’s fears are not grounded in fact. First, the bills are not preemptive, leaving state legislatures and courts free to experiment on any issues that they deem important. And so although there is no evidence of any company actually choosing to locate its R&D facilities based on local acceptance or rejection of inevitable disclosure, nothing in the bills would foreclose that hypothetical possibility.

¹¹⁰ See 2015 Professors’ Letter, note 11 *supra*, at 5. The professors support their concern with citation to a paper arguing “that lesser constraints on employee mobility may increase economic growth and innovation.” Quoting On Amir and Orly Lobel, *Driving Performance: A Growth Theory of Noncompete Law*, 16 STAN. TECH. L. REV. 833, 837-38 (2013). The authors of the paper describe an online survey experiment suggesting that employees perform less well when they know they will be prohibited from doing the same task later, or will be paid less to do it. Apart from the question of how much can be extrapolated from the observation that people are more productive when they know they are free to do what they like afterwards, the paper begs the very important question of how much of that value should be set off against the loss of valuable rights when employees decide to leave with otherwise protectable secrets.

¹¹¹ See UTSA, note 18 *supra*, at §2.

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

THE CONCEPT OF "TROLLS" CANNOT APPLY TO TRADE SECRETS

The term "trade secret troll" is an oxymoron. As in the fairy tale where he controls access to an important bridge, the troll has to have something to "catch" the unsuspecting pedestrian. Patents fill the bill, but trade secrets cannot. Just imagine the "trade secret troll" jumping up to file a lawsuit against a passer-by. The troll has to allege that the person participated in either a theft or a breach of confidence. There is no such thing as a no-fault trade secret claim.¹¹⁵ Anyone that might try to bundle them to build a business – for example, by sending out threat letters to an entire industry – is doomed to immediate failure.

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

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

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

¹¹⁵ The so-called "innocent misappropriator" who receives information unaware that it is someone else's trade secret will face liability only prospectively from the time of receiving notice. Restatement (Third) of Unfair Competition, §40, cmt d; 14 U.L.A. 433 §§2(b), 3(a). See also note 21 *supra* and accompanying text.

This is a reflection of the profound differences between patents and secrets. Patents are territorial rights granted by a government with the effect of excluding all others from making or selling the described invention. Liability is strictly imposed. Trade secret rights, in contrast, are not a government grant but derive from a private relationship in which information is shared in confidence. The law intervenes only when that specific confidence has been breached, or an unauthorized actor has gained access by “improper means,” which the UTSA defines through the examples of “theft, bribery, misrepresentation . . . or espionage.”¹¹⁶ Apart from that protection against misappropriation, the trade secret holder has no rights at all. Anyone else may hold the same information through independent discovery or reverse engineering of a publicly available product. This is why the Supreme Court called trade secrets “weak” in relation to patents.¹¹⁷

The pending bills would not alter these fundamental facts nor would they reduce any of the sanctions that have typically been applied to discourage frivolous claims.¹¹⁸ Apart from providing a very circumscribed and risky opportunity to request ex parte seizure as described above, the only difference would be to give trade secret holders the option of going directly to federal courts with their claims. What is it about that relatively modest change to the law that would provoke the appearance of a kind of litigant that we have never seen before in any of the states where trade secret laws have been enforced for over a century? One would assume that the proponents of such a scenario would have to come armed with real evidence combined with very persuasive logical analysis. Instead, we have been offered only opinion (“the capabilities of trade secret trolls remain to be seen, but the risk is very real”)¹¹⁹ and apocalyptic speculation (“trade secret trolls [will] roam free in a confused and unsettled environment, threatening or initiating

¹¹⁶ 14 U.L.A. 433 §1(1). Another important distinction from patents, not specifically relevant to this point, is that the trade secrets rights flow with the information across borders, and are nominally enforceable wherever jurisdiction over the breach has been established. I say “nominally” because the enforcement of trade secret rights in other countries, although strongly influenced by Article 39 of the TRIPS Agreement, is quite variable. See generally Douglas C. Lippoldt & Mark F. Schultz, *Uncovering Trade Secrets – An Empirical Assessment of Economic Implications of Protection for Undisclosed Data* (OECD 2014), available at http://www.oecd-ilibrary.org/trade/uncovering-trade-secrets-an-empirical-assessment-of-economic-implications-of-protection-for-undisclosed-data_5jxz15w3j3s6-en?crawler=true.

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

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

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

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

CONCLUSION

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

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

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

¹²⁰ *Id.* at 252.

Statement of Professor Sharon K. Sandeen, December 2, 2015

STATEMENT OF PROFESSOR SHARON K. SANDEEN¹

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

ON

“Protecting Trade Secrets: the Impact of Trade Secret Theft on
American Competitiveness and Potential Solutions to Remedy This Harm.”

December 2, 2015

I. INTRODUCTION

Thank you Chairman Grassley, Ranking Member Leahy and the other members of the Senate Judiciary Committee.

I am honored to be here today. I am a professor of law at Hamline University School of Law (subject to the acquiescence by the ABA, soon to be Mitchell Hamline School of Law). I am also the author of numerous books and articles on the topic of United States and international trade secret law, including the first trade secret law textbook for law school use. I am also a former civil litigator, having worked in that capacity for 15 years before becoming a law professor. In fact, it was my experiences as a litigator that drew me to focus my scholarship on trade secret law and information policy.

For the record, I am against the misappropriation of legitimate trade secrets and fully support the existing set of state laws and the existing federal criminal statute that are designed to protect such secrets. I also agree that the problem of cyberespionage is serious and is an appropriate issue for Congress to address. However, the Defend Trade Secrets Act does not directly address the problem of cyberespionage and I believe its costs are greater than its marginal and debatable benefits.

¹ Prepared by Sharon K. Sandeen, Professor of Law, Hamline University School of Law, St. Paul, Minnesota and David S. Levine, Associate Professor of Law, Elon University School of Law, Greensboro, North Carolina. David S. Levine is an Affiliate Scholar at Stanford Law School’s Center for Internet and Society and a Visiting Research Collaborator at Princeton’s Center for Information Technology Policy. He has written several articles on trade secrecy and information access, and was a civil litigator in intellectual property and other related fields for seven years before entering academia.

Statement of Professor Sharon K. Sandeen, December 2, 2015

You [have heard/ will hear] from multiple presenters about the problems of trade secret misappropriation and cyberespionage from the perspective of large, multi-national corporations that have been victimized by the wrongful acquisition of their trade secrets.

I will speak from a perspective that has not been adequately represented in discussions about the D.T.S.A., that of numerous start-up companies, entrepreneurs, mobile employees, and small and medium-sized businesses that are sued for trade secret misappropriation and forced to defend themselves, often when there are no legitimate trade secrets or little or no evidence of misappropriation.

I am happy that over 40 law professors from across the country have joined me and my co-authors in expressing their concerns in two letters written in opposition to the proposed legislation.²

II. The Vast Majority of Trade Secret Cases Are Brought Against Former Employees, Not Spies

Although much of the commentary that surrounds the D.T.S.A. concerns the problem of cyberespionage, the vast majority of trade secret claims in this country are not against alleged spies but involve former employees or other business associates.³

This is where the potential for abuse arises. Usually in these cases, the alleged misappropriation does not involve the wrongful acquisition of trade secrets, but rather an alleged breach of a duty of confidentiality.⁴ In other words, in most trade secret cases the defendant was voluntarily given access to the alleged trade secret by his or her own employer or business associate, sometimes under circumstances giving rise to a duty of confidentiality, sometimes not.

The companies that support the D.T.S.A. are very sophisticated, have ample legal resources, and have detailed policies and procedures in place to identify and protect their trade secrets. However, not all trade secret plaintiffs fall into that camp.

Often, businesses do not even know that they might have trade secrets until a former employee leaves to go to work for a competitor or to start a competitive business. When the

² 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 Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2015" (S. 1890, H.R. 3326) (Nov. 7, 2015), available at <https://cyberlaw.stanford.edu/blog/2015/11/new-professors-letter-opposing-defend-trade-secrets-act-2015>.

³ David Almeling, et. al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZAGA L.R. 57, 59-60 (2010); David Almeling, et. al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZAGA L.R. 291, 303 (2009).

⁴ See UNIF. TRADE SECRETS ACT § 1(2) (UNIF. LAW COMM'N 1985), definition of "misappropriation."

Statement of Professor Sharon K. Sandeen, December 2, 2015

former employer hires an attorney, the former employee finds out – after the fact – that she may be involved in trade secret misappropriation.

Where legitimate trade secrets exist and there is evidence of misappropriation, I have no problem with litigation brought against former employees. However, I am against the misassertion of trade secret rights, including for the purpose of disrupting a competitor or to punish a former employee who has a great new idea and some entrepreneurial initiative. This is what my co-author, David Levine, and I refer to as the “Trade Secret Troll” problem, which is akin to, but (as we explain in our article) not identical to, the patent troll problem.⁵

Misunderstandings about the true scope of trade secret rights and the limited types of behaviors that constitute misappropriation help explain why many trade secret cases are unsuccessful. The lack of success is not because the existing trade secret law in the United States is inadequate, but because the putative trade secret owner either did not have legitimate trade secrets or cannot prove that they were misappropriated.

III. There Are Important Reasons Why Trade Secrets Rights Are Limited

When considering whether the D.T.S.A. actually addresses cyberespionage, it is important to understand that trade secret law does not protect all business information. It does not even protect all secret business information. It only protects a subset of secret business information which can meet trade secrecy’s stringent legal requirements.⁶

Trade secret doctrine has long recognized that information that is known by both the general public, or within a particular industry, cannot be a trade secret. Trade secret law also does not protect the general skill and knowledge that employees learn on the job, often including highly specialized knowledge and skills.

Unfortunately, many trade secret plaintiffs do not understand these limits. They also do not understand that it is not “wrong” for companies to engage in legitimate competitive intelligence, reverse engineering, and independent development. These are some of the ways that businesses stay competitive and are able to offer consumers better products and lower prices.

⁵ See David S. Levine and Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 Wash. & Lee L. Rev. Online 230 (2014), fn. 1 and related text.

⁶ See UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM’N 1985), defining a “trade secret” as information that is: (1) secret; (2) has independent economic value; and (3) is the subject of reasonable efforts to maintain its secrecy.

Statement of Professor Sharon K. Sandeen, December 2, 2015

There are important reasons for the limitations on the scope of trade secret protection. First, there is the strong public policy, repeated in numerous Supreme Court cases,⁷ that the law cannot (and should not) protect information that is in the public domain.

Additionally, there is a longstanding policy that inventors should seek patent protection rather than keeping their inventions as trade secrets. As the U.S. Supreme Court stated, trade secret protection must be limited because otherwise it interferes with the patent policy of disclosure of information upon which others can ultimately build.⁸

The D.T.S.A., when coupled with recent changes to patent law as a result of the America Invents Act, threatens to disrupt this longstanding policy.⁹ Enabling companies to threaten federal trade secret litigation - particularly with respect to formulas and processes that can be used while still being kept hidden - will undermine the disclosure purposes of both U.S. patent law and state trade secret laws. The net result will be a reduction in access to and diffusion of information and knowledge in this country,¹⁰ possibly less innovation, and certainly more litigation.

In other words, the public interest will be harmed.

IV. Trade Secret Litigation Is Expensive and Will Be Even More Expensive Under the Defend Trade Secrets Act

There are a number of reasons why the D.T.S.A. will increase litigation costs, costs that small businesses that are wrongfully accused of trade secret misappropriation can ill-afford.¹¹

First, as there is no federal civil trade secret jurisprudence, numerous issues that have long been resolved at the state level are sure to be highly litigated at the federal level. As the

⁷ See e.g. *Sears, Roebuck & Co. v. Stiffel Co.*, 376 U.S. 225 (1964); *Compco Corp. v. Day-Brite Lighting, Inc.*, 376 U.S. 234 (1964); *Bonito Boats Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141 (1989).

⁸ *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974).

⁹ The case of *Metalizing Eng'g Co. v. Kenyon Bearing & Auto Parts Co.*, 153 F. 2d 516 (2d Cir 1946), established the principle (now known as the Metalizing Doctrine) that an inventor cannot make commercial use of an invention, even in secret, and later seek to patent the invention after the expiration of the applicable grace period. While there is little legislative history surrounding the AIA to support the assertion that Congress intended to statutorily overrule the Metalizing Doctrine, some proponents of the AIA have urged such an interpretation. Those that do also have an interest in stronger trade secret protection that, because of the issues of federal preemption discussed in *Kewanee*, can only be accomplished through the adoption of federal trade secret legislation.

¹⁰ For general discussion about the impact of trade secret law on access to information, see David S. Levine, *Secrecy and Unaccountability: Trade Secrets in our Public Infrastructure*, 59 FLA. L. REV. 135 (2007) (explaining how the aims of secrecy sometimes conflict with "the methods and purpose of transparent and accountable democratic governance").

¹¹ Sharon K. Sandeen, *The DTSA: The Litigator's Full-Employment Act*, 72 Wash. & Lee L. Rev. Online (forthcoming 2015).

Statement of Professor Sharon K. Sandeen, December 2, 2015

federal courts develop their jurisprudence, they will have multiple sources of existing state law to borrow from,¹² but with no direction from Congress on which to choose.

I favor the Uniform Trade Secret Act which has been adopted in 47 of 50 states, but federal judges may go a different direction, thereby leading to less uniformity in trade secret doctrine, not more. I am particularly concerned that many of the well-established principles of trade secret law that are discussed in the comments to the UTSA are not included in the proposed legislation.

I am also concerned about how the federal courts might address the so-called inevitable disclosure doctrine and other employment-related issues that often arise in trade secret cases, such as the enforceability of noncompete agreements. As a native of northern California, I have witnessed first-hand how California benefited from the mobility and entrepreneurial spirit of its workforce. Many argue that Silicon Valley would not be so successful were it not for the long-standing policy of California that holds noncompete agreements unenforceable except in very limited circumstances.¹³

Having employees learn on the job and then believe that they can build a better business is the American Way and is what keeps many employees engaged and striving for a better life. Unfortunately, today, start-up companies can easily find themselves as defendants in all manner of alleged IP infractions. For example:

- They pick a name for their business, only to receive a cease-and-desist letter alleging trademark infringement;
- They purchase a printer for use in their business and they get sued for patent infringement;
- They download software to fix the printer, and they are accused of copyright infringement;
- They use information they learned on the job, arguably general skill and knowledge, and they get sued for trade secret misappropriation.

These are the real-world consequences for U.S. businesses of ever-expanding IP rights and remedies. Although, in theory, weak or illegitimate claims will be exposed during the course of litigation, many small businesses, start-ups, and mobile employees cannot afford to litigate. Instead, they are forced to simply capitulate.

¹² This includes: (1) the Restatement (First) of Torts provisions governing trade secrecy; (2) the Uniform Trade Secrets Act; (3) the Restatement (Third) of Unfair Competition provisions governing trade secrecy; and (4) the trade secret jurisprudence of fifty states.

¹³ See, i.e., AnnaLee Saxenian, *Regional Advantage: Culture and Competition in Silicon Valley and Route 128* (Cambridge, MA: Harvard University Press 1994).

Statement of Professor Sharon K. Sandeen, December 2, 2015

The D.T.S.A.'s jurisdictional clause will be highly litigated for the simple reason that trade secrets are not used openly or in ways that their connection to interstate commerce can be seen and easily tested. Since the existence of trade secrets and their use in interstate commerce is a Constitutional requirement, one can expect numerous motions and debates on the issue of federal court jurisdiction, including a lot of early and costly discovery.

The proposed civil seizure provision will also be highly litigated, particularly since it is a tool that plaintiffs can use to shut down a competitor's business. Although this concern was addressed somewhat compared to the legislation introduced last session, what remains is a highly complex and troublesome remedy that is fraught with potential abuse.¹⁴ It is particularly troublesome when one considers that many plaintiffs in trade secret cases do not have strong claims but the ex parte nature of the remedy means that there will be no one to point out such weaknesses.

V. There Are Better and More Direct Ways to Address the Cyberespionage Problem

I believe that the Defend Trade Secrets Act is well-intentioned. I share the sponsors' concerns about cyberespionage and the misappropriation of legitimate trade secrets by foreign operatives. However, I think there are better ways to address those problems.

For one, if the intent of the law is to stop the wrongful acts of cyberespionage and other forms of spying, why would we want to make the existence of a legitimate trade secret a predicate fact? Isn't the real concern the bad acts that lead to the improper acquisition of confidential business information, regardless of whether that information qualifies as a trade secret?

We already have a federal law on the books with both criminal penalties and a civil cause of action that addresses the wrongful acquisition of information stored in a computer, known as the Computer Fraud and Abuse Act.¹⁵ Why not amend that law to more directly address the bad acts of cyberespionage while at the same time solving the problem that the current law poses with respect to everyday Internet usage? This would differentiate the egregious cases of intentional espionage from cases that involve ill-informed former employees and Internet users.¹⁶

There are also better and more direct ways to address some of the procedural problems that the proponents of the D.T.S.A. use to justify the legislation. For instance, Congress could exercise its powers under the Full Faith and Credit Clause of the Constitution and direct state

¹⁴ Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 Wash. & Lee L. Rev. Online (forthcoming 2015).

¹⁵ 18 U.S.C. §1030.

¹⁶ For more discussion of proposed alternatives, see *Here Come the Trade Secret Trolls*, *supra* note 5. See also, Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 Va. L. Rev. 317, 385-90 (2015).

Statement of Professor Sharon K. Sandeen, December 2, 2015

courts to more readily recognize and enforce orders and judgments entered by other courts in trade secret cases.¹⁷ There may also be ways for Congress to make interstate discovery easier, helping all state court litigants and not just trade secret litigants.

In conclusion, the D.T.S.A.'s proponents have not made the case for the federal expansion of trade secret law, particularly in light of the fact that we already have a robust set of state laws and many trade secret cases are already filed in federal courts based upon diversity jurisdiction.

If anything is clear, it is that more laws are not necessarily better, particularly when a proposed law is largely duplicative of existing state laws and when the proposed law will increase the costs of litigation and has the potential for significant abuse.

Because disrupting established trade secret principles and the legitimate business operations of start-up companies, small and medium sized enterprises, and mobile employees is the most likely outcome of the D.T.S.A., it should be rejected.

Thank you for your time and attention. I would be happy to answer any questions.

oOo

¹⁷ For an example of this strategy with respect to protection orders issued in domestic violence cases, see 18 U.S.C. §2265.

United States Senate Committee on the Judiciary
Hearing on
“Protecting Trade Secrets: The Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy this Harm”

Questions for the Record for Thomas R. Beall, Corning Incorporated

Questions from Senator Whitehouse:

1. In executing a civil seizure order under the Defend Trade Secrets Act (“DTSA”), what degree of force would law enforcement agents be entitled to use? Would law enforcement agents executing the seizure be permitted to knock down doors? Open locked cabinets by force? Should they be authorized to restrain the defendant or sequester staff and employees during the search of a business?

Answer: As a threshold matter, we believe that the DTSA’s stringent requirements for obtaining a seizure order ensure that seizure will be used rarely and in narrow circumstances. To justify a seizure order, the applicant must provide very specific information about not only the misappropriation itself but also the necessity and equity of the seizure. When seizure is ordered, it must be carried out by a law enforcement officer. As a company, while we do not set the policies or standards for law enforcement officials, we respect the fact that they must protect public safety even as they enforce the law. We do not believe that inappropriate force will be a significant issue in enforcing a seizure order under the DTSA because we are unaware of issues regarding inappropriate force in the context of copyright or trademark protection - areas of intellectual property in which a similar order is authorized.

2. Who should be responsible for sorting through the data and electronic devices seized pursuant to a DTSA civil seizure order? Should courts permit the plaintiff who initiated the suit to search through the seized devices to locate stolen trade secret information? Isn’t this role best performed by a disinterested third party appointed by the court?

Answer: We believe that the DTSA provides an important safeguard by restricting access to seized material until all parties have had an opportunity to be heard in court. We are confident that a court will then tailor the review of the seized material based on the specific facts, similar to the manner in which a court would restrict discovery involving confidential information. In some instances, this may involve a third-party appointed by the court.

3. Testimony offered at the hearing indicated that a civil seizure order issued pursuant to the DTSA could not be used to seize data in the cloud because the DTSA requires that the defendant be in possession of the misappropriated trade secret. Do you agree with this assessment? Isn’t a civil plaintiff likely to argue that a defendant possesses the data the defendant stores in the cloud? Doesn’t the dictionary definition of “possession,” which includes ownership or control, support this argument?

Answer: A seizure order issued pursuant to the DTSA should not be used to seize either data in the cloud or a computer server on which the data resides. The DTSA now includes a number of safeguards which were negotiated with cloud service companies to protect against such an occurrence. These safeguards were included in the version of the legislation reported last year by the House Judiciary Committee, and were included again in S. 1890 and its companion bill, H.R. 3326, when the two bills were introduced with identical language this year. Regarding protection of third parties, three of the safeguards are particularly important: *First*, a seizure can only be ordered against the party that used “improper means” to misappropriate the trade secret. “Improper means” includes theft or bribery, but not mere knowledge that the secret was improperly obtained. A cloud service company, therefore, would not be subject to a seizure order by virtue of its customer storing a stolen trade secret on the company’s server because the cloud company would not have used improper means to misappropriate the information.

Second, a seizure order can only issue if a temporary restraining order (TRO) would be inadequate to prevent the propagation or dissemination of the trade secret because the party would “evade, avoid, or otherwise not comply with such an order.” We believe this safeguard is significant because, in the case of a legitimate and responsible third party service provider, a court presumably would consider a TRO adequate to prevent propagation or dissemination.

Third, a seizure cannot be ordered against a person unless the applicant can show that the person would “destroy, move, hide, or otherwise make such matter inaccessible to the court” if the person had advance knowledge of the order. This further protects third parties, including cloud providers, but allows an order to issue when necessary to prevent a person attempting to abscond with the secret.

4. Are the protections in the DTSA against overseizure a meaningful constraint? Is a court that has found sufficient evidence to grant a civil seizure order likely to later rule that the seizure was wrongful or excessive? If law enforcement agents executing a civil seizure order overseize or act wrongfully would the plaintiff be liable for their actions?

Answer: Yes, we believe the protections are very meaningful. As a starting point, a seizure order issued under the DTSA must be the “narrowest seizure of property necessary” to achieve the purpose of the section and must minimize any interruption of the business operations of third parties. And this concern for minimizing the interruption of business operations extends even to the person accused of misappropriating the trade secret - indicating, in our view, a real effort in the legislation to treat all parties fairly.

Moreover, a person suffering damage by reason of a wrongful or excessive seizure can bring an action against the applicant for damages for lost profits, cost of materials, loss of good will, punitive damages in instances where the seizure was sought in bad faith, and attorney fees. We believe this high price for abuse will discourage seizure applications except where they are truly justified. For Corning, such disincentives are important because, while the seizure remedy is a

critical component of the legislation, we do not want it to be abused against us or any other responsible party.

5. Should civil seizure under the DTSA be limited to those instances where a defendant is likely to flee the United States? Should more be done to carve out routine employer-employee disputes from the civil seizure provisions of the DTSA?

Answer: The seizure provision allows trade secret owners, in extreme circumstances, to recover stolen secret information before it is sold to a competitor or otherwise disseminated. In such situations, time is of the essence. Once the secret is disclosed, it by definition loses its value. Sometimes the thief is looking to flee the country; other times, the thief may be attempting to sell it from the United States. In either case, the ability to act quickly and prevent disclosure is critical. Because the seizure remedy of the DTSA would be available only within narrow circumstances and contains numerous safeguards, we do not believe it would be used in routine employer-employee disputes.

United States Senate Committee on the Judiciary
Hearing on
“Protecting Trade Secrets: The Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy this Harm”

Questions for the Record for Thomas R. Beall, Corning Incorporated

Questions from Senator Klobuchar:

1. The Defend Trade Secrets Act allows a party to seek an ex parte order to seize misappropriated trade secrets. Some have expressed concerns that some companies may try to abuse this provision to gain a competitive advantage against their competitors.

- What provisions in the bill protect against this type of the abuse?
- How effective will these provisions be in preventing attempts to misuse this seizure provision?

Answer: The legislation contains a number of safeguards to prevent abuse. First, in order to obtain a seizure order, the applicant must demonstrate:

- a) that seizure is necessary to prevent the propagation or dissemination of the trade secret;
- b) a Rule 65(b) temporary restraining order would be inadequate because the defendant would evade, avoid or otherwise not comply with it;
- c) immediate and irreparable injury will occur if the seizure is not ordered;
- d) the harm to the applicant of not issuing a seizure order outweighs the harm to the defendant of issuing it;
- e) the likelihood of demonstrating the information is a trade secret and the defendant used improper means to obtain it; and
- f) the defendant would destroy, move, or hide the matter if it had notice from the applicant.

As a threshold matter, we think it will be a significant burden for a trade secret owner to meet all of these requirements. For example, it would be difficult to persuade a court that a person will evade a federal court order or destroy evidence without showing very specific information leading to that conclusion.

Second, in the exceptional case where the trade secret owner is able to meet this burden and justify seizure, the court’s order must be the “narrowest seizure or property necessary” to prevent dissemination of the secret. And then the defendant can move at any time to modify or dissolve the order, with a hearing on the matter not later than seven days after the order issues.

Moreover, a person suffering damage by reason of a wrongful or excessive seizure can bring an action against the applicant for damages for lost profits, cost of materials, loss of good will, punitive damages in instances where the seizure was sought in bad faith, and attorney fees.

We think these safeguards against abuse of the seizure provision will be very effective. The bill sets a high bar for getting ex-parte seizure in the first place, then allows the defendant to be heard quickly in court, and provides significant punishment for abuse.

2. The focus of most of this hearing is on remedying the harm suffered by companies who are victims of trade secret disclosures.

- Do you see this legislation as providing benefits to companies even before they lose trade secrets, based on increased certainty that if something goes wrong they can recover?
- What are those benefits?

Answer: Yes, we do see this legislation as providing benefits to companies even before they lose trade secrets. For companies like Corning, having effective, predictable, and enforceable trade secret laws provide the confidence we need to continue to invest in research and development, develop new products, improve our manufacturing processes, and keep related jobs in the United States.

Moreover, the DTSA will help us internationally. Currently, the United States encourages other nations to adopt both civil and criminal trade secret protections, even though it has no national civil trade secret statute itself. We think the DTSA will give the United States a shining example of an effective civil trade secret law, which will be helpful in persuading other countries to create meaningful trade secret protections of their own.

United States Senate Committee on the Judiciary

December 2, 2015

**“Protecting Trade Secrets: The Impact of Trade Secret Theft on American Competitiveness
and Potential Solutions to Remedy this Harm”**

Questions for the Record for Karen Cochran

Associate General Counsel and Chief Intellectual Property Counsel

E.I. du Pont de Nemours and Company

Questions from Senator Whitehouse

1. In executing a civil seizure order under the Defend Trade Secrets Act (“DTSA”), what degree of force would law enforcement agents be entitled to use? Would law enforcement agents executing the seizure be permitted to knock down doors? Open locked cabinets by force? Should they be authorized to restrain the defendant or sequester staff and employees during the search of a business?

Answer: We see no reason why an execution of a seizure order under the DTSA would require force. As with other statutes enabling private parties to file an application for a seizure, the DTSA orders are carried out by experienced law enforcement officers and cooperation from the subject is routine. In addition, the specificity required by an application under the DTSA ensures that in the rare case of a seizure, an order will be narrowly tailored.

2. Who should be responsible for sorting through the data and electronic devices seized pursuant to a DTSA civil seizure order? Should courts permit the plaintiff who initiated the suit to search through the seized devices to locate stolen trade secret information? Isn’t this role best performed by a disinterested third party appointed by the court?

Answer: The DTSA restricts a seizure applicant's ability to view seized material either during or after the seizure. The provisions prohibit copying seized materials. The courts and law enforcement must protect and secure the material from physical and electronic access while it is in the custody of the court. The right approach for reviewing the seized material will vary based on the facts of each case; in some circumstances, this may mean the appointment of a third party or in camera review by the court. Ultimately, we are confident that courts will effectively manage evidence in their custody as they routinely do in cases involving protective orders and other business-sensitive materials.

3. Testimony offered at the hearing indicated that a civil seizure order issued pursuant to the DTSA could not be used to seize data in the cloud because the DTSA requires that the defendant be in possession of the misappropriated trade secret. Do you agree with this assessment? Isn't a civil plaintiff likely to argue that a defendant possesses the data the defendant stores in the cloud? Doesn't the dictionary definition of "possession," which includes ownership or control, support this argument?

4. Are the protections in the DTSA against over-seizure a meaningful constraint? Is a court that has found sufficient evidence to grant a civil seizure order likely to later rule that the seizure was wrongful or excessive? If law enforcement agents executing a civil seizure order over-seize or act wrongfully would the plaintiff be liable for their actions?

Answer for 3 and 4: The DTSA has been drafted with the input of technology companies, cloud service providers, and companies in all industries to address concerns about whether the bill's original language would have permitted seizures of third-party servers. In its present form, we are satisfied that the DTSA does not permit seizures of servers themselves or of data hosted on third-party servers in the cloud.

We are also satisfied the DTSA will neither permit nor lead to over-seizures. First, the DTSA contains a damages provision giving anyone harmed by an excessive or abusive seizure a cause of action with recoverable damages that include lost profits, loss of goodwill, and loss of materials.

Punitive damages and recovery of attorney's fees are available to victims of abusive, bad faith tactics.

Second, the provision's comprehensive requirements and multiple mandatory showings under oath serve to restrict the availability of an order significantly and limit the possibility of reckless or abusive seizures. For example, a person applying for a seizure order must swear under penalty of perjury in written submissions to a federal district court judge to the truth of specific and detailed facts and circumstances. The sworn facts and circumstances first of all must demonstrate to the court's satisfaction that (i) a legitimate trade secret has been misappropriated by a specific person through improper means, (ii) the alleged thief would evade or ignore a traditional restraining order, and in addition, (iii) the thief would move or destroy the trade secret if given notice of the application. The DTSA includes several other mandatory showings, but at a minimum, without these threshold showings, the district court may not issue a seizure order.

The seizure provisions in the DTSA speak not only to potential victims of trade secret theft, but to any parties tempted to use seizure improperly. For that reason, we scrutinized the seizure provisions from two important perspectives—that of a legitimate victim of trade secret theft, and that of a company being victimized by an abusive party. We concluded that the provisions' very strict, rigorous prerequisites and judicial safeguards ensure that civil seizures will likely occur only in rare and entirely justified circumstances. As a result, we are confident that the DTSA is drafted in a way that minimizes that risk by eliminating incentives for abuse; it would be a risky and simply ineffective way for a competitor to attempt to gain an advantage.

5. Should civil seizure under the DTSA be limited to those instances where a defendant is likely to flee the United States? Should more be done to carve out routine employer-employee disputes from the civil seizure provisions of the DTSA?

Answer: Trade secret theft is a serious threat to DuPont and other innovative companies regardless of whether it comes from an employee seeking to take our know-how to a competitor, or a foreign entity seeking to sell our intellectual property to the highest bidder. In both situations, the seizure provision facilitates the immediate action necessary to prevent the value of

our trade secrets from being destroyed. Because the DTSA is focused on intentional misappropriation, seizures may only issue when a court finds that the secret will be imminently moved, hidden, or destroyed if notice is given, and that the subject would not comply with a court order. The legislation is therefore drafted in a way that will not capture ordinary employment matters. But it will provide a critical tool for trade secret owners who face the possibility of losing the value of years of hard work and innovation.

Questions from Senator Klobuchar

1. The Defend Trade Secrets Act allows a party to seek an ex parte order to seize misappropriated trade secrets. Some have expressed concerns that some companies may try to abuse this provision to gain a competitive advantage against their competitors.

- **What provisions in the bill protect against this type of the abuse?**
- **How effective will these provisions be in preventing attempts to misuse this seizure provision?**

Answer: Increasingly, today's trade secret information is created, stored and transferred in portable, electronic forms. Time is of the essence once a trade secret theft has been discovered. To reduce the risk of further trade secret dissemination or the destruction of evidence, a victim of trade secret theft needs assured, direct access to a federal court and the court's power to impose temporary orders that preserve the status quo in special circumstances. In a very small set of circumstances where a traditional *ex parte* temporary restraining order will not suffice, trade secret victims need proactive capabilities to stop or contain a theft in progress. DuPont is satisfied that the civil seizure provisions in the DTSA give victims the tools needed for such extraordinary, rare circumstances.

One would be ill-advised to abuse the DTSA for competitive advantage. For one, it contains a damages provision that provides a cause of action to anyone harmed by an excessive or abusive seizure. The recoverable damages include lost profits, loss of goodwill, and loss of materials.

Punitive damages and recovery of attorney's fees are available to victims of abusive, bad faith tactics.

Second, the provisions' comprehensive requirements and multiple mandatory showings under oath serve to restrict the availability of an order significantly and limit the possibility of reckless or abusive seizures. For example, a person applying for a seizure order must swear under penalty of perjury in written submissions to a federal district court judge to the truth of specific and detailed facts and circumstances. The sworn facts and circumstances must demonstrate to the court's satisfaction that (i) a legitimate trade secret has been misappropriated by a specific person through improper means, (ii) the alleged thief would evade or ignore a traditional restraining order, and in addition, (iii) the thief would move or destroy the trade secret if given notice of the application. These very rigorous pre-requisite showings are just some of several mandatory showings required for judicial findings; but at a minimum, without sufficient evidence to support these mandatory threshold findings, a district court may not issue a seizure order.

The seizure provisions in the DTSA speak not only to potential victims of trade secret theft, but to any parties tempted to use seizure improperly. We scrutinized the seizure provisions from two important perspectives—that of a legitimate victim of local and international trade secret theft, and that of a company being victimized by an abusive party or competitor. We conclude that the provisions' very strict, rigorous prerequisites, judicial safeguards, and damages provision ensure that civil seizures will likely occur only in rare and entirely justified circumstances. As a result, we are confident that the DTSA is drafted in a way that minimizes any risk of abuse by eliminating its very incentives. An abusive applicant's misconduct in seeking a competitive advantage would in all likelihood require perjury, false or deceptive testimony, bad faith, sanction-worthy legal representation, misrepresentations to a federal court, and probable awards of expansive damages, punitive damages, and legal expenses.

2. The focus of most of this hearing is on remedying the harm suffered by companies who are victims of trade secret disclosures.

- **Do you see this legislation as providing benefits to companies even before they lose trade secrets, based on increased certainty that if something goes wrong they can recover?**
- **What are those benefits?**

Answer: Successful innovation requires collaboration and information-sharing among colleagues, co-workers, and in many instances, other companies. More and more, collaborators are interacting from great distances through electronic and digital means. Although some critics argue that stronger trade secret laws promote secrecy, the opposite is true. When we have confidence that our proprietary and trade secret information, which today can be captured *in toto* and carried on portable media in digital form, is protected by reliable and readily available laws and judicial procedures, we can more efficiently and effectively share information both within our company and with partners worldwide. DuPont is proud to invest heavily in research and development to create the next generation of innovative processes, materials, and products. Effective and reliable trade secrets protection allows us to continue this investment with confidence.

With the existing patchwork of state trade secrets laws and jurisdictional hurdles, our abilities to share and collaborate are hampered, both domestically and internationally. At home, the uniformity provided by the DTSA would streamline our compliance efforts and make interstate and global collaboration less risky and more efficient. And for companies like DuPont that do business globally, the DTSA would also provide a model for the rest of the world and enhance our ability to protect our investments in foreign jurisdictions. The DTSA will do more than provide a remedy for victims of misappropriation; it will have an immediate, positive impact on all American companies that create jobs and invest in research and development in the United States.

James Pooley Responses to Senator Grassley Questions for the Record

“Protecting Trade Secrets: the Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm”

**U.S. Senate Committee on the Judiciary
December 2, 2015**

1. The DTSA amends the Economic Espionage Act to create a federal civil remedy for the misappropriation of trade secrets. The DTSA provides that an applicant for relief may file, on *ex parte* basis, for the seizure of property from the party accused of stealing a trade secret if necessary to prevent the propagation or dissemination of the trade secret.

When legislative solutions that would have created a civil right of action for trade secret theft have been proposed in previous Congresses, there has been concern that the *ex parte* seizure provision may have been overbroad. Does S. 1890 adequately address those concerns? If so, how?

ANSWER: S.1890 does adequately address the concerns that were raised about proposals for *ex parte* seizure. We should keep in mind that the process is not new. State laws under the Uniform Trade Secrets Act provide that “affirmative acts to protect a trade secret may be compelled by court order,” and *ex parte* orders have occasionally been granted, both in state and federal courts, where specific facts clearly show that the defendant would not obey a preventive order and that giving advance notice would likely lead to the destruction of the secret. S.1890 makes this authority explicit, but responds to concerns raised with predecessor bills by strictly limiting seizure to property that is “necessary to prevent propagation or dissemination of the trade secret” and that is in the possession of the wrongful actor. It also requires that seizures be carried out by law enforcement, and that property be held by the court pending a hearing, which must be held within seven days. As a further curb against abuse, court orders must be directed to the “narrowest seizure of property necessary” and must minimize interruption of legitimate business. Damages for wrongful

seizure will not be limited to the amount of the required bond. In my opinion and based on my experience, the process of S.1890 is more circumscribed than would be available by proceeding under existing state and federal injunction provisions.

2. Some opponents of a federal civil cause of action have claimed that it could harm small businesses and start-ups and impede employee mobility. In your experience as a practitioner who has represented clients of all sizes in trade secrets cases, and as a researcher on the subject, are these concerns legitimate?

ANSWER: I firmly believe that providing a federal forum for civil trade secret claims will not harm small businesses or start-ups, nor will it impede employee mobility. In fact, in my experience it could prove a significant advantage for defendants in most cases. This is because unlike state courts where pre-trial issues are often handled for all cases in a single motions department, federal judges have the case from beginning to end and so are more likely to focus at an early time on dismissal of meritless claims. For the defendant in a trade secret case, this can translate into greater predictability and lower cost. And because small businesses and start-ups rely more on secrecy to protect their competitive advantage, having a choice of federal forum will give them more options for enforcing their rights as plaintiffs. As for employee mobility, the applicable language of S.1890 (permitting injunctions against "actual or threatened misappropriation") is identical to the Uniform Trade Secrets Act. But S.1890 goes further, adding a proviso to ensure that no order can interfere with anyone accepting a new job under conditions that avoid actual or threatened misappropriation.

**James Pooley Responses to Senator Whitehouse Questions for
the Record
“Protecting Trade Secrets: the Impact of Trade Secret Theft on
American Competitiveness and Potential Solutions to Remedy
This Harm”
U.S. Senate Committee on the Judiciary
December 2, 2015**

1. In executing a civil seizure order under the Defend Trade Secrets Act (“DTSA”), what degree of force would law enforcement agents be entitled to use? Would law enforcement agents executing the seizure be permitted to knock down doors? Open locked cabinets by force? Should they be authorized to restrain the defendant or sequester staff and employees during the search of a business?

ANSWER: In my experience with execution of search warrants in criminal trade secret cases, the party in possession of the specific matter to be seized (e.g., a storage drive or computer) readily complies with law enforcement officials’ requests for access to the identified information. The person accused of trade secret theft typically is not a violent criminal and does not otherwise have any criminal record, and thus force is not needed. In addition, although the court issuing the seizure order cannot be expected to anticipate all issues that might arise in its execution, the DTSA requires that the court “direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties” or of the defendant’s operations “that are unrelated to the trade secret that has allegedly been misappropriated.”

2. Who should be responsible for sorting through the data and electronic devices seized pursuant to a DTSA civil seizure order? Should courts permit the plaintiff who initiated the suit to search through the seized devices to locate stolen trade secret information? Isn’t this role best performed by a disinterested third party appointed by the court?

ANSWER: Because of the DTSA's strict requirements that the application identify "with reasonable particularity the matter to be seized and where it is located," the court will normally be in a position to require from the applicant any information that could help determine the specific location or description of the trade secret information within some electronic storage device, whether by the use of file names, key words or other search methodology. The DTSA requires that the search be carried out by government officials and that the court protect "the seized property from disclosure by restricting the access of the applicant, including during the seizure" In addition, the DTSA requires that any seized property be taken in by the court and protected from "physical and electronic access during the seizure and while in the custody of the court." Therefore, it would not be proper under the DTSA to allow the applicant to "search through the seized devices to locate stolen trade secret information." The DTSA does allow for the applicant to petition the court for access to the seized trade secrets, which the court may permit once both parties have been given the opportunity to be heard.

3. Testimony offered at the hearing indicated that a civil seizure order issued pursuant to the DTSA could not be used to seize data in the cloud because the DTSA requires that the defendant be in possession of the misappropriated trade secret. Do you agree with this assessment? Isn't a civil plaintiff likely to argue that a defendant possesses the data the defendant stores in the cloud? Doesn't the dictionary definition of "possession," which includes ownership or control, support this argument?

ANSWER: The DTSA contains several provisions – additions since last year's Senate bill – that protect against this result. I understand that the requirement that "the person against whom seizure would be ordered" (a) has misappropriated the trade secret and (b) has possession of it, combined with the additional requirement that the person is likely to destroy it or flee, addressed the concerns of cloud providers to ensure that seizures would not extend to information located on third party servers and would not apply to legitimate businesses generally. The DTSA's approach is consistent with the normal

understanding of the term “possession” as actual, rather than constructive.

In the cloud context, a traditional Rule 65 order issued to the provider would be adequate to secure the trade secret held by the third party provider. Therefore, no seizure application could meet the threshold condition that a Rule 65 order “would be inadequate” because the person would “evade, avoid or otherwise not comply.”

4. Are the protections in the DTSA against overseizure a meaningful constraint? Is a court that has found sufficient evidence to grant a civil seizure order likely to later rule that the seizure was wrongful or excessive? If law enforcement agents executing a civil seizure order overseize or act wrongfully would the plaintiff be liable for their actions?

ANSWER: If the asserted facts on which the seizure order is based turn out to be wrong, it is the applicant that is responsible, not the court, and the court will not hesitate to hold such applicants accountable. It is important to place this in context: all ex parte requests are extraordinary, and most courts will err on the side of denying them. In my many years’ experience dealing with judges – in both federal and state courts – on ex parte applications, they all react with a natural reticence and skepticism, knowing that they must rely on the applicant to establish a compelling reason to allow this very unusual form of relief. Frequently they will closely question counsel about the nature and quality of the evidence. If they later discover that they have been misled in any way, they likely will impose substantial sanctions, and certainly will entertain proceedings to enforce the right of the wrongfully accused to be made whole. Regarding the liability of the plaintiff for actions of law enforcement in going beyond the bounds of the order or of other legal restrictions on their conduct, I do not claim any special expertise on that question.

5. Should civil seizure under the DTSA be limited to those instances where a defendant is likely to flee the United States?

Should more be done to carve out routine employer-employee disputes from the civil seizure provisions of the DTSA?

ANSWER: No, I believe it is not practical to do more than has already been done by the authors of the DTSA to ensure that it meets its objectives while protecting against abuse. Studies show that the vast majority of trade secret loss continues to occur through insiders, mainly employees. When an applicant is able to make the specific, fact-based showing required by the DTSA – that is, that the defendant has in his possession a misappropriated trade secret that is in immediate danger of being completely destroyed or taken from the jurisdiction and that he is likely to ignore a preventive order – the situation is not in any respect “routine,” but is fraught with the likelihood of irreparable damage. And although proof of intent to flee the United States represents a heightened degree of this risk, it is by no means the only risk that the seizure provision is designed to mitigate. For example, if a trade secret becomes known beyond the circle of those who are authorized, it could lose its entire value. Electronic transmission out of the jurisdiction is one way such a loss could be realized, and seizure before the transmission happens could prevent the loss.

**James Pooley Responses to Senator Klobuchar Questions for
the Record**

**“Protecting Trade Secrets: the Impact of Trade Secret Theft on
American Competitiveness and Potential Solutions to Remedy
This Harm”**

**U.S. Senate Committee on the Judiciary
December 2, 2015**

1. The Defend Trade Secrets Act allows a party to seek an ex parte order to seize misappropriated trade secrets. Some have expressed concerns that some companies may try to abuse this provision to gain a competitive advantage against their competitors.

- What provisions in the bill protect against this type of the abuse?
- How effective will these provisions be in preventing attempts to misuse this seizure provision?

ANSWER: A number of the DTSA seizure provisions combine to make this remedy extremely unlikely to be abused. First, the threshold requirements are very high. Only property “necessary to prevent the propagation or dissemination of the trade secret” may be seized, and the application must particularly identify that property and its location. Seizure may be carried out only against the person who misappropriated and possesses the secret. The sworn application must establish “clearly” from “specific facts” that a preventive order under Rule 65 would be inadequate because the person would likely not comply with it but would hide or destroy the secret; that there is a risk of immediate and irreparable injury that outweighs the harm to the person and substantially outweighs harm to third parties; and that the plaintiff is likely to succeed in proving misappropriation of a valid trade secret. The court must order only the “narrowest seizure” necessary, conducted in a way that minimizes any disruption of legitimate business operations and prevents the applicant from getting access to the secret until both parties have been heard. A full hearing must be held within seven days, when the plaintiff must be ready to demonstrate that the need for seizure still exists, and in the meantime anyone can apply to modify or suspend the order. And as difficult as it is to obtain a seizure order, the DTSA imposes serious consequences if

the applicant gets it wrong. In addition to court-ordered sanctions under Rule 11, the victim of a wrongful seizure is granted a claim for damages that is not limited by the amount of the required bond. Based on my experience dealing with preliminary remedies in state and federal court, and in counseling clients about the risks, I believe that these provisions will provide an effective deterrent against abusive seizure applications.

2. The focus of most of this hearing is on remedying the harm suffered by companies who are victims of trade secret disclosures.
- Do you see this legislation as providing benefits to companies even before they lose trade secrets, based on increased certainty that if something goes wrong they can recover?
 - What are those benefits?

ANSWER: The ideal remedy for trade secret misappropriation is always to prevent it, since a secret once released cannot be recalled, and no one can ever be sure that damages will adequately compensate for a lost business advantage. Experienced lawyers know that the highest priority for business owners is preventive relief. The DTSA responds to this need by providing the same judicial authority as exists under current state law: actual or threatened misappropriation may be enjoined. And it adds a special provision for ex parte seizure to cover those unusual cases in which it can be established that the misappropriator will not obey an injunction but is likely to flee the jurisdiction or destroy the secret. As I have indicated in my previous answer, a seizure order is very difficult to obtain, and properly so. But in those special cases that qualify, the DTSA will provide a very valuable benefit to the trade secret owner.



December 22, 2015

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

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

Dear Chairman Grassley and Ranking Member Leahy:

This letter is submitted by the undersigned, Professor Sharon K. Sandeen, to respond to the questions Senator Sheldon Whitehouse posed during the December 2, 2015 hearing, “Protecting Trade Secrets: the Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm” and to expand upon the letter in opposition to the Defend Trade Secret Act of 2015 (the DTSA) that was signed by myself and 41 other law professors.¹

Two points must be stressed at the outset. First, it appears that the focus of most Senators’ concerns was on the ability of large U.S. companies to remain competitive with foreign companies, the fear being that without a federal civil trade secret law foreign companies will come to possess U.S.-generated trade secrets and use them to compete against U.S. companies. While I share this concern, Congress should also be concerned about the interests of U.S.-based individuals and companies (including entrepreneurs and small and medium-sized enterprises

¹ See Professors’ Letter in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326), dated November 17, 2015, available at: <https://cyberlaw.stanford.edu/files/blogs/2015%20Professors%20Letter%20in%20Opposition%20to%20DTSA%20FINAL.pdf>.

(SMEs)) that wish to build competitive businesses within the U.S. but are often hindered in doing so by the over-assertion of intellectual property (IP) rights, including trade secret rights. Trade secrets laws should not be made so strong that they can be used to quell legitimate competition.

Second, trade secret rights should not be made so strong that they tie-up the free flow of information because (like limited incentives) information and knowledge are essential components of innovation, invention and creativity.² Rather, the focus should be on finding the optimal balance between protecting truly “secret” information and allowing other information (including the general skill and knowledge that workers learn on the job, which are not protectable as trade secrets under existing law) to flow freely. I think this balance has largely been achieved under existing state laws due to the “sieve-like” nature of U.S. trade secret rights. I am concerned that this balance will be significantly altered by the DTSA, leading to more litigation³ and less innovation, competition and labor mobility.

Question 1: In executing a civil seizure order under the Defend Trade Secrets Act (“DTSA”), what degree of force would law enforcement agents be entitled to use? Would law enforcement agents executing the seizure be permitted to knock down doors? Open locked cabinets by force? Should they be authorized to restrain the defendant or sequester staff and employees during the search of a business?

Response: As currently written, the DTSA provides little guidance to law enforcement on how the *ex parte* civil seizure order (hereinafter “seizure order” or “seizure remedy”) will be executed and whether and to what extent force may be used during its execution. It is clear, however, that the basis for a seizure order is not the same as it is for a criminal search and seizure order and, thus, a civil seizure order should not be executed in a similar manner. The target of a civil seizure order is not being accused of a crime but, instead, is being sued for a civil wrong for which a variety of remedies are available.

Although the seizure order proposed in the DTSA is often favorably compared to the seizure order that exists under federal trademark law,⁴ the “property” to be seized is markedly different, as is the required egregiousness of the underlying behavior.⁵ Whereas the similar

² Alan Hyde, *WORKING IN SILICON VALLEY: ECONOMIC AND LEGAL ANALYSIS OF A HIGH-VELOCITY LABOR MARKET* (2003) and Alan Hyde, *The Wealth of Shared Information: Silicon Valley's High-Velocity Labor Market, Endogenous Growth, and the Law of Trade Secrets*, available at <http://andromeda.rutgers.edu/~hyde/WEALTH.htm>; see also, Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. Rev. 575, 585-92 (1999) (describing the value of knowledge spillovers in the development and growth of Silicon Valley).

³ See Sharon K. Sandeen, *The DTSA: The Litigator's Full-Employment Act*, 72 Wash. & Lee L. Rev. Online 308 (2015).

⁴ 15 U.S.C. § 1116(d).

⁵ For a more in depth analysis of the civil seizure remedy, see Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 Wash. & Lee L. Rev. Online 284 (2015).

provisions of trademark law focus on trademark counterfeiters, no attempt is made in the seizure provisions of the DTSA to differentiate between egregious and minor instances of trade secret misappropriation. Moreover, in the trademark context, physical goods are seized which clearly bear infringing trademarks. Once seized, these goods can be stored much like they would be maintained by a wholesaler until such time as they are either released to the defendant for resale because they are not, in fact, counterfeit goods, or destroyed if they are counterfeit goods.

The execution of a seizure order in a trade secret case will not be so precise and orderly because the putative trade secrets will not be as easy to identify as goods bearing trademarks. Rather, execution of a seizure order in a trade secret case is likely to require law enforcement personnel, unaccompanied by any representative of the applicant,⁶ to sift through reams of physical and digital records to find the proverbial “needle in a haystack.” Unless the alleged trade secrets can be easily identified and segregated from other information and data, the seizure of non-trade secret information and trade secrets that are owned by the defendant is likely to occur in the process.⁷

The seizure provision of the DTSA requires that service of any order “shall be made by a Federal Law enforcement officer, or may be made by a State or local law enforcement officer, who upon making service, shall carry out the seizure under the order to be executed.”⁸ Without further specification, this undoubtedly means that a team of uniformed officers will descend upon the target individual’s home or business and effectively shut down business operations while the physical premises and electronic equipment can be searched. The draft legislation does not specify what will happen in the case of a recalcitrant defendant that refuses to grant access to the premises or computer systems.

In contrast to the DTSA, the original “Anton Piller Order” that I referred to in my testimony was limited with respect to how it could be executed. As Lord Denning explained in the case of *Anton Piller KG v. Manufacturing Processes Limited*:

But the Order sought in this case is not a search warrant. It does not authorise the Plaintiffs' Solicitors or anyone else to enter the Defendant's premises against his will. It does not authorise the breaking down of any doors, nor the slipping in by a back door, nor getting in by an open door or window. It only authorises entry and

⁶ S. 1890. The Defend Trade Secrets Act of 2015 (hereinafter DTSA), §2(a) (“(b)(2)(B)(iii)(I)”).

⁷ See Goldman, *supra* note 5, at 290 (noting that trade secret information is often commingled with other, non-confidential information); see also David Post, *A Misguided Attempt to “Defend Trade Secrets,”* Washington Post, <https://www.washingtonpost.com/news/voikh-conspiracy/wp/2015/12/02/and-we-need-stronger-protection-for-trade-secrets-because> (Dec. 2, 2015) (explaining that “the distinction between information that is protected and information that is not protected” under trade secrets law “is usually in dispute and quite difficult to discern”).

⁸ DTSA § 2(a), (“(b)(2)(E)”).

inspection by the permission of the Defendants. The Plaintiff must get the Defendant's permission.⁹

Senator Whitehouse's question and the foregoing quote raise the very important issue whether seizure orders should be executed like criminal search and seizure orders. Since it is contended by the proponents of the DTSA that seizure orders will be difficult to obtain, it is also worth considering whether the limited benefits of such a remedy are worth the potential for errors and abuse.

Question 2: Who should be responsible for sorting through the data and electronic devices seized pursuant to a DTSA civil seizure order? Should courts permit the plaintiff who initiated the suit to search through the seized devices to locate stolen trade secret information? Isn't this role best performed by a disinterested third party appointed by the court?

Response: As currently written, the DTSA requires that any materials seized "shall be taken into custody of the court,"¹⁰ but it does not specify whether or when seized property, including electronic equipment and digital data, will be evaluated and sorted to determine what portion of it constitutes the plaintiff's legitimate trade secrets. To the contrary, it requires that the seized materials be secured from "physical and electronic access during the seizure."¹¹ This means that no one has the right to access the seized property until the seizure order is lifted or some process for review is mandated by the court. Even if the seizure order is ultimately lifted, the initial hearing on the validity of the order need not be heard for seven days, the practical effect of the order being that a company's business operations may be shut-down for at least a week.

By no means should the plaintiff in a trade secret case be allowed to search the seized information for the simple reason that it may contain the confidential personal information of the defendant's clients, customers and employees, as well as the defendant's own trade secrets and other proprietary information.¹² Instead, if court personnel cannot do so, a special master or other third-party must be retained to review the seized materials. If the seized property includes digital data, this may include an expert in computer forensics. Thus, the expense of storing, evaluating

⁹ *Anton Piller KG v Manufacturing Processes Ltd & Ors* [1975] EWCA Civ 12, [1976] 1 All ER 779 (8 December 1975). See also, UK Parliament, Civil Procedure Act 1997, Section 7. Since *Anton Piller* orders were originally recognized in the United Kingdom, they have been severely criticized by members of the judiciary and others based upon the principle that individuals should not be deprived of their property without due process and concerns about the sanctity of one's home. See e.g., *Universal Thermosensors Ltd. v. Hibben* [1992] F.S.R. 361, *Nicholls V.C.*; *Columbia Pictures Industries, v. Robinson* [1986] F.S.R. 367, Scott J. This includes criticism by the late Sir Hugh Laddie, a highly-respected jurist and IP expert and the person who, as an attorney, advocated for the issuance of the seizure order that was granted in the *Anton Piller* case. Sir Laddie described the remedy that he is credited with inventing as a "Frankenstein's Monster." Obituary of Professor Sir Hugh Laddie, *The Telegraph*, 03 Dec. 2008, available at <http://www.telegraph.co.uk/news/obituaries/3546410/Professor-Sir-Hugh-Laddie.html>.

¹⁰ DTSA, § 2(a), ("(b)(2)(D)").

¹¹ *Id.*

¹² "Searches and seizures of computers and computer data present complex legal questions that, if resolved incorrectly, present a very real threat of massive intrusions into civil liberties." Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 76-77 (1994).

and sorting through the seized information to determine if it contains trade secrets is likely to be extremely high and the DTSA does not specify who will bear those costs.

Equally troubling is the fact that the DTSA contains language that can be interpreted to mean that the scope of any seizure order is not limited to existing legitimate (or even alleged) trade secrets. It states that courts may “issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.”¹³ The terms “propagation” and “dissemination” are not defined in the DTSA, are not terms previously used in connection with trade secret misappropriation and appear to encompass a broader set of behaviors than state trade secret laws. Trade secret misappropriation is defined under the UTSA (and the DTSA) as the wrongful acquisition, disclosure or use of trade secrets.¹⁴ As used in the proposed seizure remedy, the acts that may trigger a seizure of property are not the “threatened disclosure or use” of the alleged trade secrets as required for injunctive relief, but the threatened propagation or dissemination of such information (the act of sharing). Thus, a former employee of a company might be subject to a seizure order if there is a threat that information he holds might be shared with another (e.g., a new employer), even if neither the former employee nor the new employer threaten to publicly disclose or use such information.¹⁵ Furthermore, the property that can be seized could include equipment that can be used for the propagation and dissemination of information, disconnected from the actual trade secrets, such as a computer or smart phone.

Question 3: Testimony offered at the hearing indicated that a civil seizure order issued pursuant to the DTSA could not be used to seize data in the cloud because the DTSA requires that the defendant be in possession of the misappropriated trade secret. Do you agree with this assessment? Isn't a civil plaintiff likely to argue that a defendant possesses the data the defendant stores in the cloud? Doesn't the dictionary definition of "possession," which includes ownership or control, support this argument?

Response: The language of the DTSA is internally inconsistent and therefore confusing. As just noted, it appears to allow for the seizure of “property” that might be used in the propagation and dissemination of trade secrets even if the property itself does not contain the plaintiff’s trade secrets. Later, the DTSA specifies a number of conditions for the grant of a seizure order, including that the plaintiff “is likely to succeed in showing that the information is a trade secret”¹⁶ and that “the person against whom seizure would be ordered has possession of the trade

¹³ DTSA, § 2(a), (“(b) (2)(A)(i)”).

¹⁴ UTSA, § 1(2) and DTSA, § 2(b)(3) (“(5)(A) and (B)”).

¹⁵ This is the fact pattern of *Pepsico v. Redmond*, 54 F. 3d1262 (7th Cir. 1995), the case often cited in support of the inevitable disclosure doctrine. Both Mr. Redmond and his new employer (Quaker Oats) readily acknowledged (and agreed to abide by) the ongoing duty Mr. Redmond owed not to disclose or use trade secrets he learned while at Pepsico, but injunctive relief was ordered anyway based upon the argument that Redmond could not separate what he knew about Pepsico from his work with his new employer. Will a seizure remedy be issued based upon the alleged inevitable propagation or dissemination of such secrets?

¹⁶ DTSA, § 2(a) (“(b)(2)(A)(IV)(aa)”).

secret.”¹⁷ However, while the “matter to be seized” must be described with reasonable particularity, it need not be limited to the alleged trade secrets.¹⁸

There is nothing in the DTSA that specifically insulates service providers that store information on behalf of a defendant (including cloud storage providers and hard-copy document storage facilities) from being subjected to a seizure order. There is no indication of exactly how electronically stored information will be seized or what it means to be in “possession” of such information. Does “seizing” information that exists in digital form require that it be permanently erased from the computer servers of the person or company against whom a seizure order is issued? What if the information is also stored with a third-party cloud storage provider for back-up purposes; will all copies be seized by law enforcement and stored and sorted by the courts?

While the DTSA provides that “the person against whom seizure would be ordered” must have either “misappropriated the trade secret of the applicant by improper means” or “conspired to use improper means to misappropriate the trade secret of the applicant,”¹⁹ this language does little to insulate cloud storage providers from the reach of a seizure order. To understand why requires consideration of the definition of “misappropriation by improper means,” which includes “breach or inducement of a breach of a duty to maintain secrecy.”²⁰ If a cloud storage provider owes a duty of confidentiality to the trade secret owner, it might be subjected to a seizure order if it is shown that it breached its duty and, thereby, “misappropriated the trade secret of the applicant.” If no such duty of confidentiality exists (and cloud storage providers are loathe to agree to such a duty), then arguably the trade secrecy of the stored information has been lost, in which case the lawsuit should not be brought in the first place.²¹

The requirement that the person against whom seizure would be ordered must have “conspired to use improper means to misappropriate the trade secret of the applicant” further confuses and complicates the potential reach of any seizure order. If proof of possession of the alleged trade secret by the person against whom the seizure would be ordered is required, what does the conspiracy-prong add to the seizure provision? Usually, a conspiracy claim is included in a statute to punish preliminary behaviors that have not yet resulted in the primary wrongful act. But if the wrongful act of trade secret misappropriation has not yet occurred, how can the person against whom seizure would be ordered possess the alleged trade secrets? Might the conspiracy requirement be used to subject an individual or business, including a cloud storage provider, to a seizure order merely because they possess a misappropriated trade secret? Moreover, who “possesses” the information that is stored with a cloud storage provider: the

¹⁷ DTSA, § 2(a) (“(b)(2)(A)(IV)(cc)”).

¹⁸ DTSA, § 2(a) (“(b)(2)(A)(V)”).

¹⁹ DTSA, § 2(a) (“(b)(2)(A)(IV)(bb)”).

²⁰ DTSA, § 2(b)(3) (“(6)(A)”).

²¹ Sharon K. Sandeen, *Lost in the Cloud? Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 Virg. Jour. of L & Tech. (JoLT) 1 (2014).

client, the provider or both? Nothing in the DTSA precludes a court from ordering the seizure of information in defendant's "possession," wherever it might be stored.

Question 4: Are the protections in the DTSA against over seizure a meaningful constraint? Is a court that has found sufficient evidence to grant a civil seizure order likely to later rule that the seizure was wrongful or excessive? If law enforcement agents executing a civil seizure order over seize or act wrongfully would the plaintiff be liable for their actions?

Response: This question raises the very important point of how laws are actually applied in practice and whether the fee shifting provisions of the DTSA, including the damage remedy specified in the seizure provision, are effective in preventing abusive trade secret litigation. The proponents of the DTSA argue that the ability of defendants to obtain an award of attorney's fees in cases of "bad faith" assertion of trade secret claims²² and damages due to a "wrongful or excessive" seizure²³ are sufficient to deter abusive trade secret litigation. However, as Senator Whitehouse's question suggests, providing a remedy on paper and structuring the remedy so that it can be used effectively are two different things.

Significantly, neither the attorney's fees provision of the DTSA nor the damages provision of the seizure remedy provide defendants with relief based upon the simple fact that they prevailed on the merits in court. Rather, a successful damage claim can only be brought under the seizure provision if it can be shown that the defendant suffered damages "by reason of a wrongful or excessive seizure." A successful claim for attorney's fees requires a showing of "bad faith" on the part of the plaintiff with respect to either: (1) plaintiff's claim of misappropriation; or (2) plaintiff's opposition to a motion to terminate an injunction. It is unclear whether the damage claim for a wrongful or excessive seizure could include attorney's fees and, if so, whether the necessary standard of proof is "bad faith" or "wrongful or excessive."²⁴

Further confusing matters, the DTSA does not define "bad faith," "wrongful" or "excessive." It is clear, however, that for a defendant to be awarded a remedy in the form of either attorney's fees or damages, it will have to go to the time, trouble and expense of proving facts beyond merely prevailing in the underlying action. It is also clear that a significant amount of resources will have to be expended before the defendant will even get to the point of claiming attorney's fees and damages, resources that many entrepreneurs, employees and SMEs simply do not possess.

²² DTSA, §2(a) ("(b)(3)(D)").

²³ DTSA, §2(a) ("(b)(2)(G)").

²⁴ As Eric Goldman notes in a recent article, since explicit reference is made in the DTSA to the analogous provisions of the Trademark Act (15 U.S.C. 1116(d)(11)), the range of potential damages for wrongful or excessive seizures may include attorney's fees (Goldman, *supra* note 4, at 293), but the trademark statute uses a "wrongful" standard whereas the seizure provision uses a "wrongful or excessive" standard. It is not clear if this standard is intended to be easier to prove than the trademark standard and, if so, whether it will apply with respect to attorney's fees expended in conjunction with defending against a seizure order.

The commentary to the UTSA explains that “Section 4 allows a court to award reasonable attorney fees to a prevailing party in specified circumstances as a deterrent to specious claims of misappropriation, to specious efforts by a misappropriator to terminate injunctive relief, and to willful and malicious misappropriation.” As an example, the California courts have interpreted “bad faith” to require both proof of “objective speciousness” and “subjective bad faith.”²⁵ This is a very difficult and costly burden to meet and one that falls particularly hard on small businesses that may be victimized by the over-assertion of trade secret rights.

What the required proof will be under the seizure remedy remains to be defined by the federal courts, particularly since the language used is different from the existing “bad faith” language for an award of attorney’s fees under the UTSA. As Eric Goldman explained in a recent article:

With respect to the Seizure Provision’s effects, the devil is in details that Congress has not resolved (yet). If the courts interpret the Act to create strict liability for a wrongful seizure and award large damages from lost business opportunities, trade secret owners will be too afraid to use the provision. In contrast, if courts require subjective bad faith to establish a wrongful seizure and narrowly construe the damages from disruption and lost business opportunities, trade secret owners will seek ex parte seizures routinely.²⁶

Without more clarity regarding Congressional intent concerning the meaning of “wrongful or excessive,” at best, the meaning of the damages provision of the seizure remedy is sure to be highly litigated and, and worst, it will fail in its stated purpose of deterring abusive requests for such relief.

Question 5: Should civil seizure under the DTSA be limited to those instances where a defendant is likely to flee the United States? Should more be done to carve out routine employer-employee disputes from the civil seizure provisions of the DTSA?

Response: I believe that the seizure remedy should be eliminated from the DTSA in its entirety because of its potential for abuse and because the number of cases of egregious trade secret misappropriation involving alleged spies and other acts of wrongful acquisition are small in comparison to the number of cases involving former employees and alleged breaches of a duty of confidence. In this regard, it is interesting to note that at the time that the Economic Espionage Act of 1996 (the EEA) was debated, numerous concerns were expressed about the potential of exposing reputable businesses to criminal prosecution for trade secret misappropriation. At that

²⁵ Gemini Aluminum Corp. v. California Custom Shapes, Inc., 95 Cal. App. 4th 1249, 1262 (2002).

²⁶ Goldman, *supra* note 4, at 293.

time, it was agreed by the Clinton Administration that no EEA prosecutions would be brought unless they were first reviewed by the Attorney General of the United States. There should be similar concerns with respect to the use of the seizure provisions of the DTSA against reputable U.S. businesses and employees, particularly where the criminal enforcement tools of the U.S. government can (and should) be brought to bear against the most egregious forms of trade secret misappropriation.

The vast majority of trade secret misappropriation cases in the U.S. do not involve individuals fleeing overseas. A large percentage of them do not even involve legitimate trade secrets or provable acts of misappropriation. Often they involve former employees taking information from a former employer that they were given access to, did not know or have reason to know were trade secrets, or have no intention to disclose or use. These cases can typically be resolved through self-help and education, including informing former employees of their ongoing duties of confidentiality, if any.

In light of the paucity of cases to which the seizure remedy might apply, the argument in favor of the remedy becomes circular. On one hand it is argued that the seizure remedy is necessary to stop egregious behavior that many U.S. companies are facing, but on the other hand it is argued that it will be used infrequently. The critical issue is: How frequently will the remedy be asserted against the typical person (usually a former employee) or U.S.-based company accused of trade secret misappropriation? My concern, and that of other opponents of the DTSA, is that the seizure remedy will be used more frequently against U.S. companies and employees than alleged foreign spies. Further, even if the remedy is sought but not granted, it will impose significant costs on the federal courts. In cases where the remedy is granted but later rescinded, significant costs will also be imposed upon the defendant under circumstances where it cannot recoup such costs unless it can prove that the order was “wrongful” or “excessive.”

Senator Whitehouse was correct to note the emotional aspects of trade secret litigation, particularly in the employment context. Although most employers in the U.S. treat their employees as “at-will” so that the obligations that they owe to such employees are limited, they often expect a degree of loyalty that extends well beyond the termination of employment, even in cases where there is no express noncompete or nondisclosure agreement. This is why many trade secret cases fail. Former employers often mistake the “duty of loyalty” that they believe their employees owe (including even former employees) for trade secret misappropriation. Thus, in many ways, trade secret cases are the personal injury cases of business litigation because the asserted loss of (and threats to) business assets often lead courts to react positively to the plaintiff’s claims before there is clear proof of the existence of a trade secret. Particularly at the preliminary relief stage, courts often minimize plaintiff’s burden of proving the existence of trade secrets when there is evidence of bad acts, such as surreptitious copying of materials on a copying machine or downloading information to a jump drive. In effect, judges are blinded by

the asserted wrongs. This is where the potential for abuse arises and why a powerful new form of preliminary relief is troublesome.

Because of the foregoing, the opponents of the DTSA are very concerned about how the DTSA may affect employee mobility. The proponents argue that the language which reads “provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation described in paragraph (1)” is sufficient to protect employees. However, this language only addresses potential remedies by directing the courts to consider the impact of any injunction on employment. It does not address the broader concern about how expanded trade secret rights and remedies might be used to intimidate and control employees before litigation is even filed or, if it is filed, before a decision on the merits of the case. It also does not reject the inevitable disclosure doctrine or allow existing state law to apply with respect to such issue.

The proponents of the DTSA who appeared at the recent hearing characterized the controversial “inevitable disclosure doctrine” as merely circumstantial evidence of “threatened misappropriation.” However, the inevitable disclosure argument is typically raised in trade secret cases when there is little or no evidence that any tangible embodiments of trade secrets have been taken or maintained by the former-employee/defendant or when there is little evidence of threatened disclosure or use of the alleged trade secrets. The focus of the argument is on information that the former-employee/defendant has stored in her brain. The problem is that there is a fine-line between legitimate trade secrets stored in an individual’s brain and the general skill and knowledge that individuals gain on the job.²⁷

Unfortunately, for a variety of reasons (including the emotional reasons just mentioned), the reasonable efforts requirement of trade secrecy is not always applied stringently enough to preclude former-employees from being subjected to claims of trade secret misappropriation under circumstances where they had little or no prior notice of what their former employer claimed as a trade secret.²⁸ Also, the true extent of threats of trade secret litigation that are made against former employees is unknown because such threats typically take the form of a cease and desist letter first, only resulting in trade secret litigation if the former employee does not accept the former employer’s demands. Often, employees who are served with cease and desist letters do not have the financial means to hire an attorney to advise them concerning the validity of such claims and, thus, readily agree to their former employer’s demands. To the extent such demands overreach and require employees not to accept particular employment, they restrict employee mobility and are anticompetitive.

²⁷ See James H. A. Pooley, *Restrictive Employee Covenants in California*, 3 Santa Clara High Tech. L.J. 251, 281 (1988) (explaining that “it is exceedingly difficult to draw a line between an employer’s enforceable proprietary rights and the employee’s general knowledge and skills”).

²⁸ See David S. Levine, *School Boy’s Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 Wash. & Lee L. Rev. Online 323 (2015) (expressing concern that the DTSA will lead to even less stringent examination of the reasonable efforts requirement).

Unless putative trade secret owners engage in sufficient reasonable efforts to protect their trade secrets, particularly with respect to identifying claimed trade secrets, employees may actually be unaware of what information should be treated as a trade secret. Thus, while I remain opposed to the inevitable disclosure doctrine for the reasons expressed by California courts,²⁹ if and where the inevitable disclosure doctrine is applied, putative trade secret owners should be held to a heightened burden of proving that the subject employee was actually informed by her employer of the precise information that should be treated as a trade secret. This is particularly important with low-level and low-paid employees who do not regularly (or ever) deal with the proprietary information of their employers.

To avoid the misuse of the seizure remedy against former employees, an exemption is a possible answer. The key is to differentiate between the types of cases that are used to justify the seizure remedy (largely, espionage and wrongful acquisition cases) from the more typical trade secret case involving former employees and an alleged breach of a duty of confidence). This might be accomplished in several ways.

First, as I mentioned in my testimony, the DTSA should be amended to make it clear that it is to be interpreted in accordance with the commentary to the UTSA, which includes reference to many more limitations on the scope of trade secret rights than are contained in the DTSA. It should also be made clear that trade secrets do not include the general skill and knowledge that employees learn on the job.

Second, as Senator Whitehouse suggested, employee cases might be exempted altogether from the seizure remedy. At a minimum, I suggest that cases against former employees require evidence of an express confidentiality agreement and advance and direct notice to the subject employee that the information that is the subject of litigation was claimed as the employer's trade secret. Employees should not be sued for trade secret misappropriation and subjected to a seizure order (or criminal prosecution) when they had no prior knowledge of what their employer claimed as a trade secret. Unfortunately, the DTSA (and UTSA) scienter requirement of "knowledge or reason to know" is often applied too liberally in emotionally charged trade secret cases.

Third, the DTSA might be amended to include a provision similar to one that is contained in the proposed EU Trade Secret Directive. Article 13.1a of the draft Directive provides: "In accordance with their national law and practice, Member States may limit the liability for damages of employees towards their employers for the unlawful acquisition, use or disclosure of a trade secret of the employer when they act without intent."

²⁹ *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443 (2002).

In conclusion, I am concerned that the problem of trade secret misappropriation is being viewed primarily through the lens of large trade secret owners and not defendants (usually former employees and start-up companies) who are wrongly accused of trade secret misappropriation. If these individuals and companies survive an early trade secret misappropriation action brought against them, perhaps they are around to speak up about the pitfalls of an unbalanced system, but if they are not (and my experience tells me many are not), someone has to point out that there are two sides to the trade secret misappropriation story. The existing system of state laws, which is largely uniform, does a good job of balancing the interests of legitimate trade secret owners with those that are accused of trade secret misappropriation. Particularly because there is no existing federal jurisprudence with respect to civil trade secret claims and the DTSA does not include many of the limitations on the scope of trade secret protection that exist under state trade secret law, I am afraid the DTSA lacks the balance that is needed to prevent it from being abused.

Thank you for the opportunity to submit this letter and to testify concerning these important issues. If I can provide any additional information or insights, I am happy to do so.

Sincerely,

Sharon K. Sandeen

Sharon K. Sandeen
Professor of Law
Mitchell | Hamline School of Law
sharon.sandeen@mitchellhamline.edu

A P P E N D I X

to

PROTECTING TRADE SECRETS: THE IMPACT OF TRADE SECRET THEFT ON AMERICAN COMPETITIVENESS AND POTENTIAL SOLUTIONS TO REMEDY THIS HARM

The following submissions are 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
--------------------------------	-----

