

**TRADE SECRETS: PROMOTING AND PROTECTING
AMERICAN INNOVATION, COMPETITIVENESS
AND MARKET ACCESS IN FOREIGN MARKETS**

HEARING
BEFORE THE
SUBCOMMITTEE ON
COURTS, INTELLECTUAL PROPERTY,
AND THE INTERNET
OF THE
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRTEENTH CONGRESS
SECOND SESSION

—————
JUNE 24, 2014
—————

Serial No. 113-97

—————

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://judiciary.house.gov>

U.S. GOVERNMENT PRINTING OFFICE

88-436 PDF

WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, Jr., Wisconsin	JOHN CONYERS, JR., Michigan
HOWARD COBLE, North Carolina	JERROLD NADLER, New York
LAMAR SMITH, Texas	ROBERT C. "BOBBY" SCOTT, Virginia
STEVE CHABOT, Ohio	ZOE LOFGREN, California
SPENCER BACHUS, Alabama	SHEILA JACKSON LEE, Texas
DARRELL E. ISSA, California	STEVE COHEN, Tennessee
J. RANDY FORBES, Virginia	HENRY C. "HANK" JOHNSON, JR., Georgia
STEVE KING, Iowa	PEDRO R. PIERLUISI, Puerto Rico
TRENT FRANKS, Arizona	JUDY CHU, California
LOUIE GOHMERT, Texas	TED DEUTCH, Florida
JIM JORDAN, Ohio	LUIS V. GUTIERREZ, Illinois
TED POE, Texas	KAREN BASS, California
JASON CHAFFETZ, Utah	CEDRIC RICHMOND, Louisiana
TOM MARINO, Pennsylvania	SUZAN DeLBENE, Washington
TREY GOWDY, South Carolina	JOE GARCIA, Florida
RAÚL LABRADOR, Idaho	HAKEEM JEFFRIES, New York
BLAKE FARENTHOLD, Texas	DAVID N. CICILLINE, Rhode Island
GEORGE HOLDING, North Carolina	
DOUG COLLINS, Georgia	
RON DeSANTIS, Florida	
JASON T. SMITH, Missouri	
[Vacant]	

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

HOWARD COBLE, North Carolina, *Chairman*
TOM MARINO, Pennsylvania, *Vice-Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin	JERROLD NADLER, New York
LAMAR SMITH, Texas	JOHN CONYERS, JR., Michigan
STEVE CHABOT, Ohio	JUDY CHU, California
DARRELL E. ISSA, California	TED DEUTCH, Florida
TED POE, Texas	KAREN BASS, California
JASON CHAFFETZ, Utah	CEDRIC RICHMOND, Louisiana
BLAKE FARENTHOLD, Texas	SUZAN DeLBENE, Washington
GEORGE HOLDING, North Carolina	HAKEEM JEFFRIES, New York
DOUG COLLINS, Georgia	DAVID N. CICILLINE, Rhode Island
RON DeSANTIS, Florida	ZOE LOFGREN, California
JASON T. SMITH, Missouri	SHEILA JACKSON LEE, Texas
[Vacant]	STEVE COHEN, Tennessee

JOE KEELEY, *Chief Counsel*
HEATHER SAWYER, *Minority Counsel*

CONTENTS

JUNE 24, 2014

	Page
OPENING STATEMENTS	
The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Chairman, Subcommittee on Courts, Intellectual Property, and the Internet	1
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Ranking Member, Committee on the Judiciary, and Member, Subcommittee on Courts, Intellectual Property, and the Internet ..	2
The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary	3
The Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Ranking Member, Subcommittee on Courts, Intellectual Property, and the Internet	4
WITNESSES	
Richard A. Hertling, Of Counsel, Covington & Burling LLP, Protect Trade Secrets Coalition	
Oral Testimony	7
Prepared Statement	10
David M. Simon, Senior Vice President for Intellectual Property, salesforce.com Inc.	
Oral Testimony	21
Prepared Statement	23
Thaddeus Burns, Senior Counsel, Intellectual Property & Trade, General Electric	
Oral Testimony	33
Prepared Statement	35
Chris Moore, Senior Director, International Business Policy, National Association of Manufacturers	
Oral Testimony	44
Prepared Statement	46
LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING	
Material submitted by the Honorable Doug Collins., a Representative in Congress from the State of Georgia, and Member, Subcommittee on Courts, Intellectual Property, and the Internet	68

**TRADE SECRETS: PROMOTING AND
PROTECTING AMERICAN INNOVATION,
COMPETITIVENESS AND MARKET ACCESS
IN FOREIGN MARKETS**

TUESDAY, JUNE 24, 2014

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY,
AND THE INTERNET

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Subcommittee met, pursuant to call, at 2:49 p.m., in room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chairman of the Subcommittee) presiding.

Present: Representatives Coble, Marino, Goodlatte, Issa, Holding, Collins, DeSantis, Nadler, Conyers, Chu, DelBene, Jeffries, Cicilino, and Lofgren.

Staff Present: (Majority) Vishal Amin, Counsel; Olivia Lee, Clerk; (Minority) Heather Sawyer, Minority Counsel; and Jason Everett, Counsel.

Mr. COBLE. The Subcommittee on Courts, Intellectual Property, and the Internet will come to order.

Without objection, the Chair is authorized to declare recesses of the Subcommittee at any time.

I want to additionally apologize to all of you for the delay. We had several House votes. They do come—claim precedence over the rest of us, so thank you all for understanding.

I will give my opening statement now. The intellectual property comes in a variety of flavors. This Subcommittee works regularly on issues concerning patents, trademarks, and copyrights when considering IP in both the domestic and international context, but today we are here to talk about trade secrets. Trade secrets are another important part of the IP landscape.

For example, one of the most famous trade secrets in the world is the formula for Coca-Cola, and I am being very provincial now, but I am certain that there are a number of Carolina BBQ spices as well. Hopefully.

Trade secrets require no formal registration and can be protected for an unlimited time, but unlike patent protection, once a trade secret is disclosed, it instantly loses its value and the property right itself ceases to exist.

Further, there is no protection if a trade secret is uncovered unlawfully by others through reverse engineering or independent development. So there are definite tradeoffs between secured patent protection or could be an innovation of a trade secret. The United States has many laws in place to protect trade secrets, and in fact, we passed two trade secret bills during the last Congress; one fixing a loophole regarding computer source code and the other involved some criminal penalties for economic espionage. And as folks consider other ideas, in the future, we need to be mindful of unintended consequences and ensure that improvements to the code are meaningful and necessary and not being done simply because we can do it.

But as our companies operate on a global scale, at issue, most pressing concern to Congress is how certain foreign governments have begun adopting policies that determine trade secret protection and create an unlevel playing field for America's most innovative companies. Six countries promote trade secret theft by producing policies that result in forced technology transfer. These trade-distorted policies may seem benign but are nothing more than legalized theft, it seems to me, since policies force U.S. companies to provide trade secret information to a local partner or government agency as a condition of investment or market access.

Some countries have begun looking for a compulsory licensing of trade secrets to a third party. This is done to help a local competitor that claims it needs access to the trade secret to compete. Generally, this is just not right, it seems to me. The Administration needs to be using all of its trade tools, including action at the WTO, to help ensure that countries that promote such policies are held to account. I hope to hear more today from our witnesses in the steps that need to be taken to promote trade secret protection, America's—American innovation, economy, and create jobs.

I am now pleased to recognize the distinguished gentleman from Michigan, Mr. Conyers, for his opening statement

Mr. CONYERS. Thank you, Chairman Coble.

I join in welcoming the witnesses and look forward to this hearing. We are examining the trade secret laws and consider whether there should be revisions or updates in the law.

Let me say that copyright, patent, and trademark owners can enforce their rights in Federal court. Trade secret owners should have a similar remedy. Indeed, trade secrets are critical intellectual property rights and should receive protection of Federal laws in addition to the State laws that have traditionally protected them.

People are now able to travel across the State and national borders more easily, and many United States companies are finding that reliance on State laws and procedures is no longer adequate for trade secret protection. The inability of private parties to protect trade secrets in Federal court has generated calls for legislation to create such a right. Those who support such a right have noted that a Federal cause of action would give companies a critical tool to enforce their rights. A Federal civil cause of action would create national standards and allow companies to craft one set of nondisclosure policies on a 50 State basis.

I want to hear the witnesses discuss the benefits and potential down side of a Federal cause of action as well as any specific issues

that we should address in such legislation. We should consider what we can do to bolster the Administration's efforts to increase protection for trade secrets at home and abroad.

In 2013, the Administration, through the U.S. Intellectual Property Enforcement Coordinator, released the Administration strategy on mitigating the theft of U.S. trade secrets, a five-pronged strategic approach to addressing trade secret theft. That secret strategy calls for coordinated international engagement with trading partners, promotion of voluntary best practices by private industry, enhancement of domestic law enforcement operations, improvement of domestic legislation regarding trade secrets, and increased public awareness. The Administration also has expressed concerns about new reports, suggesting that some countries, most notably China, are playing an increasingly active role in theft of U.S. trade secrets. In response, the Administration has increased its enforcement efforts in this area as well.

In May of this year, for example, the Justice Department indicted five Chinese military hackers for economic espionage and trade secret theft for ongoing offenses involving six American companies. That indictment is a step in the right direction, but of course, much more remains to be done.

I look forward to hearing more about this from our witnesses and what we can and should do to strengthen trade secret laws. I thank the Chairman and yield back the balance of my time.

Mr. COBLE. I thank the gentleman.

The Chair recognizes the distinguished gentleman from Virginia, the Chairman of the House Judiciary Committee, Mr. Goodlatte for an opening statement

Mr. GOODLATTE. Thank you, Mr. Chairman.

Today we examine an important area of intellectual property trade secrets. Trade secrets occupy a unique place in the IP portfolios of our most innovative companies. They can include confidential formulas, manufacturing techniques, and even customer lists, but because they are unregistered and not formally reviewed like patents, there are no limitations on discovering a trade secret by fair lawful methods, such as reverse engineering or independent development. In innovative industries, that is simply the free market at work.

Though trade secrets are not formally reviewed, they are protected from misappropriation, which includes obtaining the trade secret through improper or unlawful means. And misappropriation can take many forms, whether it is an employee selling blueprints to a competitor or a foreign agent hacking into a server. In addition, one could argue that even a foreign government's policies to require forced technology transfer is a form of misappropriation. Though most States base their trade secret laws on the Uniform Trade Secrets Act, the Federal Government protects trade secrets through the Economic Espionage Act.

In the 112th Congress, this Committee helped enact two pieces of legislation to improve the protection of trade secrets. As other ideas are developed to improve trade secrets protection, it is important that we take the time to ensure that any new measures do not increase frivolous litigation or discovery costs, do not negatively impact our international trade obligations, or result in other negative

unintended consequences, and that any measure ultimately provides a meaningful benefit to innovators and innovative companies.

On the international front, the theft of trade secrets does not just come from the employee theft or industrial and economic espionage but also from foreign governments themselves. Some of it is plain cyber theft, but many countries have also begun adopting policies that severely undermine trade secrets. These policies, invariably designed to promote local innovation, result in forced technology transfers that open American companies to the blatant theft of their intellectual property. These trade distortive policies are anti-innovation, anti-competitive, and prevent fair market access in foreign markets.

If a country requires technology transfer as a condition for regulatory approval or market access, that is wrong. If a country uses their State-owned enterprises to seek noncommercial terms from American companies for their IP, that is wrong. Such policies amount to legalized theft. In the 2014 U.S. Trade Representatives Special Report 301—Special 301 Report, China was specifically called out to take serious steps to put an end to these activities and to deter further activity by rigorously investigating and prosecuting trade secret thefts conducted on by both cyber and conventional means.

When a country fails to provide basic legal protections for intellectual property, then we need to start thinking outside the box, looking at all of our trade tools. We need to start thinking creatively, utilizing our IP Attachés in U.S. Embassies, ensuring they have sufficient authority and resources, and we need to start considering our options for actions at the WTO.

Intellectual property powers the engine of American innovation and creativity. It creates new jobs and helps grow our economy. I look forward to hearing from all of our witnesses on the issues surrounding trade secrets.

Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman.

The Chair now recognizes the distinguished gentleman from New York, the Ranking Member of the Subcommittee, Mr. Nadler.

Mr. NADLER. Thank you, Mr. Chairman, for holding this hearing to examine the ongoing importance of trade secrets as a means of safeguarding intellectual property interests at home and abroad. With the need to focus on patent reform last year and the ongoing comprehensive review of the Copyright Act, it would be easy to neglect trade secrets, but doing so would be a major mistake.

Trade secrets proprietary business information derives its value from being and remaining secret, make up approximately two-thirds of the value of U.S. companies' information portfolios. American businesses own an estimated \$5 trillion of trade secrets with roughly \$300 billion of that stolen per year; \$300 billion worth of theft a year.

In a 2012 speech, former national security director Keith Alexander described cyber espionage as the greatest transfer of wealth in history, and many businesses view trade secret protection as more critical than any other form of intellectual property protection. The 2008 National Science Foundation survey, for example, show that firms with significant research and development activity

reported trade secrets as the most important form of intellectual property protection. Even companies without R&D activity rank trade secrets as the second most important form of intellectual property protection, only slightly behind trademarks and ahead of copyrights and patents.

The value of trade secrets to U.S. companies is matched only by their tremendous vulnerability to theft. Innovative technologies have made it easy to obtain information and transfer it across the globe with the click of a cell phone, tablet, or computer key. At the same time, U.S. companies are increasingly targeted for trade secret theft by competitors with some foreign governments actively encouraging and facilitating the theft of U.S. trade secrets.

Just this past May, for example, the Justice Department charged 5 members of the Chinese military with economic espionage. The defendants are accused of targeting six American companies and conspiring to steal information useful to competitors in China, including enterprises owned by the Chinese government. This indictment represents a mere tip of the iceberg. According to FBI Director James Comey, while this case is an important step forward, "There are many more victims, and there is much more to be done."

In light of their value and vulnerability, it is critical that our laws provide robust protection for trade secrets. Unfortunately, that does not seem to be the case. What we increasingly hear—what we increasingly are hearing from a diverse array of companies ranging from traditional manufacturers to leading-edge technology firms is that that lackluster legal protection is a major cause of concern. Congress has acted before to protect trade secrets at the Federal level. In 1996, we passed the Economic Espionage Act in response to increased incidents against American companies, and just this last Congress, we took steps to improve this law, closing a loophole that allowed the theft of certain trade secrets and increasing penalties for economic espionage. The Economic Espionage Act publishes trade secret theft and economic espionage, which is a misappropriation of trade secrets for the benefit of a foreign power.

The EEA can only be enforced by the Attorney General. There is no Federal cause of action for a private party seeking to enforce the law. As of 2008, fewer than 60 prosecutions had been brought, leading to concern that the act is an ineffective weapon against economic espionage.

Lacking a Federal cause of action, companies currently use State laws to protect trade secrets. While these laws were initially developed through particular case decisions in their articulation of governing American principles by the American Law Institute, nearly every State has now enacted the Uniform Trade Secrets Act. The Uniform Act provides key definitions in a civil cause of action for misappropriation of trade secrets. A prevailing party may obtain injunctive relief, damages, and reasonable attorney's fees in certain cases.

While this system appears to have worked relatively well for local and intrastate disputes, it has not proven efficient or effective for incidents that cross State and sometimes international borders. As you will hear from our witnesses today, our 50 State system

does not work in our increasingly mobile and globally interconnected world. Former employees and industrial spies are likely to carry or transfer secret information across State borders or overseas.

The limited jurisdiction of the State court system makes it more difficult to obtain discovery or to act quickly enough to enforce an order that might stop the immediate loss of company secrets. As a result, our witnesses, who represent a wide range of key stakeholder interests, all support creation of a Federal cause of action for trade secret theft. Along with several of my colleagues on both sides of the political aisle, I similarly favor doing and we are working on, legislation to achieve this.

It would be helpful to hear from our witnesses today regarding any particular issues that should be addressed or avoided in such a bill. I believe that we have an opportunity to work quickly and in a broadly bipartisan basis to ensure that our trade secrets law more robustly protects America's innovators and businesses. We already protect trademarks, copyrights, and patents through civil—through Federal civil remedies. It is time to do the same for trade secrets.

With that, I look forward to hearing from our witnesses today, and I yield back the balance of my time.

Mr. COBLE. I thank the gentleman for his opening statement. Statements from all other Members of the Subcommittee will be entered into the record without objection.

The witnesses written statements will be entered into the record in its entirety as well.

Gentlemen, prior to introducing you, I would like for you to stand and be sworn, if you will.

[Witnesses sworn.]

Mr. COBLE. Let the record reflect that all responded in the affirmative. You may be seated.

We have a very distinguished panel today, and I am pleased to welcome you with us. I, again, apologize for the belated response.

Our first witness this afternoon is Mr. Richard Hertling, Counsel of the Washington law firm of Covington & Burling, LLP. He is here today to testify on behalf of the Protect Trade Secrets Coalition. In his position, Mr. Hertling advises clients in the technology, intellectual property, and defense of cybersecurity legislative matters. Prior to his position at Covington, Mr. Hertling served this Committee with distinction for almost 5 years, most recently as Staff Director and Chief Counsel. He has also held numerous leadership positions in the Department of Justice and the U.S. Senate throughout his 23-year career in the Federal Government. He was awarded his J.D. degree from the University of Chicago School of Law and his bachelor's degree, magna cum laude with honors, from Brown University. We welcome Mr. Hertling back to the Committee and back to the Hill.

Our second witness, Mr. David Simon, Senior Vice President of Intellectual Property of Salesforce.com. In his position, Mr. Simon is responsible for the company's intellectual property portfolio worldwide. Prior to his position at Salesforce.com, he served as Chief Patent Counsel at Intel Corporation and Vice President of IP Strategy and Licensing at Rovi Corporation. Mr. Simon received

his J.D. degree from Georgetown University Law Center and his S.B. in Electrical Engineering and Political Science from the Massachusetts Institute of Technology.

Mr. Simon, good to have you with us as well.

Our third witness is Mr. Thaddeus Burns, member of the Trade Secrets Committee at IPO, the Intellectual Property Owners Association. IPO focuses on providing practical education on the topic of trade secrets to the organization's membership and to the public. Mr. Burns is currently Senior Counsel for Intellectual Property and Trade at General Electric. Prior to GE, he has served as Senior Counsel at Akin, Gump, Strauss, Hauer & Feld, the Intellectual Property Attaché in Geneva with USPTO and a law clerk with the U.S. Court of Appeals for the Fourth Circuit. Mr. Burns received his J.D. from the Catholic University of America, Columbus School of Law and his bachelor degree from Oberlin College.

Mr. Burns, good to have you with us.

Our final witness is Mr. Christopher Moore, Senior Director of International Business Policy at the National Association of Manufacturers. Prior to his position at NAM, Mr. Moore served as Director of Strategic Planning and Deputy Director of Policy with the United Nations World Food Programme. He also held senior positions in the State Department and the Office of the U.S. Trade Representative. He is an alumnus of Emory University and the London School of Economics.

Mr. Moore, good to have you with us.

Gentlemen, you will note there is a timing machine on your table, and we would ask for you to comply with the 5-minute rule, if you can. When the green light changes to amber, that is your notice that you have 5 minutes on which to wrap up. You won't be severely punished if you don't make that minute cut, but do the best you can.

Mr. Hertling, we will start with you.

TESTIMONY OF RICHARD A. HERTLING, OF COUNSEL, COVINGTON & BURLING LLP, PROTECT TRADE SECRETS COALITION

Mr. HERTLING. Thank you very much, Chairman Coble, Ranking Member Nadler, Ranking Member Conyers. Thank you for inviting me to testify before this Subcommittee today on trade secrets. It is indeed a distinct honor and privilege for me to be here to discuss this important topic. I appreciate that my written statement will be included in the record of the hearing, and I will focus my oral testimony on the background to the existing Federal legal landscape on trade secrets, as Committee staff requested.

My firm represents the Protect Trade Secrets Coalition, a cross-industry-sectors coalition of companies supporting legislation to complement the criminal penalties provided by the Economic Espionage Act of 1996 and protect the property interest that exists in trade secrets by creating a Federal civil remedy for trade secret misappropriation, similar to the remedies available for other forms of intellectual property.

As you know, immediately prior to joining Covington & Burling, I was staff director of this Committee, but among the matters with which I was involved earlier in my congressional career was the

bill that became the Economic Espionage Act of 1996. As far back as the mid-19th century, State common law provided protection of state—of trade secrets from misappropriation, and the traditional means of enforcing the law has been through a private civil lawsuit. Trade secrets, as several members have described, are commercially valuable information subject to reasonable measures to protect the confidentiality of that information.

The protection of trade secrets in the United States has been left largely to State laws. The ad hoc pattern of 50 different State laws started to change in the 1980's when States began to codify their trade secret laws by adopting provisions of the Uniform Trade Secrets Act, a model law developed by the National Commission on Uniform State Laws.

The development of an economy driven by technological advances, however, and increasing globalization of businesses and supply chains made trade secrets more valuable in interstate and international commerce and also more susceptible to misappropriation. Industry in the U.S. started to recognize that some foreign governments and firms were competing unfairly with U.S. competitors by stealing their trade secrets. Domestic firms were seeing their crown jewels stolen and taken overseas where firms with no investment to recoup could make the product and sell it for much less than the victimized U.S. firm. Investment and jobs were at stake in the United States.

The remedy for this form of theft, however, remained entirely in the hands of State law. In effect, the same tools available in the 1890's were the only ones still available in the 1990's, and so Congress came to consider the issue and ultimately enacted in 1996 the Economic Espionage Act.

During congressional consideration of that act, a number of firms requested that the bill include a private Federal civil remedy for the misappropriation of a trade secret to complement the criminal and civil injunctive remedies the bill gave to the Federal Government. That request, however, was made at the very end of the process, after a consensus on the bill had been achieved.

Although the addition of a private Federal civil remedy was seen as valuable, it was thought that the proposal needed to be vetted on its own terms and for its own merits. The intent was that Congress could turn to it the following year. The failure to include in the EEA, essentially a criminal statute, an ability for victimized firms to seek a civil remedy in Federal court was due only to the timing and not in any way to the merits of the proposal to include Federal civil remedy. For a variety of reasons, primarily that congressional attention on intellectual property was taken up first by what became the Digital Millennium Copyright Act and, subsequently, by patent reform, the addition of a civil trade secrets remedy wound up lying dormant for a number of years only to be renewed recently by Members of both Chambers, including Members of this Committee.

Since enactment of the Economic Espionage Act, the problem with trade secret theft has grown dramatically. Foreign competitors continue to try to steal their way to success on the back of intellectual property developed here in the United States. The FBI, however, has many priorities and limited resources and cannot re-

spond to every reported theft of trade secrets, even by foreign individuals and firms. Just as we rely on both criminal law and civil litigation as complementary tools to protect property interests in other areas, we should do so in this area as well.

A Federal civil remedy for trade secret misappropriation would provide an important addition to existing protections for trade secrets at the Federal and State levels and could bolster our economy and save U.S. jobs at no additional cost. In addition, it would help protect and promote U.S. interests around the world. Many countries do not provide adequate legal protection for trade secrets, and these weak regimes present significant risks for U.S. firms seeking to expand operations globally. Enhancing our own legal protections for trade secrets would serve as a model for other countries and arm our trade negotiators with a model they could point other countries to and encourage them to follow.

I thank you for your attention and will be pleased to respond to any questions. If I might just very briefly be permitted an additional moment to recognize Chairman Coble, who will be retiring at the end of this year, and thank him very much for his kindness to me during my service on the Committee and acknowledge his lifetime of dedicated service to our country, his State, and the people of the Sixth District of North Carolina, and particularly his work on IP issues during his career. Thank you.

[The prepared statement of Mr. Hertling follows:]

Hearing on

**“Trade Secrets: Promoting and Protecting
American Innovation, Competitiveness and
Market Access in Foreign Markets”**

**U.S. House of Representatives Committee on the Judiciary
Subcommittee on Courts, Intellectual Property and the Internet**

June 24, 2014

**Written Statement of Richard A. Hertling
Of Counsel
Covington & Burling LLP**

**Testimony of Richard A. Hertling
Of Counsel, Covington & Burling LLP
“Trade Secrets: Promoting and Protecting American Innovation,
Competitiveness and Market Access in Foreign Markets”
June 24, 2014**

Introduction and Summary

Good afternoon Chairman Coble, Ranking Member Nadler, and Members of the Subcommittee. Thank you for inviting me to testify today on trade secrets. It is a distinct honor and privilege to be here to discuss this very important topic.

As you know, my name is Richard Hertling, and I am of counsel to the Washington law firm of Covington & Burling LLP. Immediately prior to joining the firm, I was staff director of this committee, the capstone of my more-than-27-year career in federal service.

I am pleased to submit this testimony on behalf of Protect Trade Secrets Coalition, a cross-sector group of companies that is working to protect and defend trade secret property by supporting a harmonized, federal civil remedy for trade secret misappropriation.¹ The Coalition supports the Defend Trade Secrets Act, the bipartisan bill introduced by Senators Coons and Hatch. The Coalition appreciates this Committee’s interest in trade secret protection and would support efforts to bolster the viability of and the protection accorded to the property interest that businesses have in their trade secrets by providing for civil jurisdiction in federal court for the misappropriation of a trade secret to complement the criminal jurisdiction and civil jurisdiction provided to the Attorney General in the Economic Espionage Act of 1996 (“EEA”).

¹ Members of the Coalition include Abbott, Caterpillar, Corning Incorporated, Eli Lilly and Company, General Electric, Medtronic, Micron, Microsoft, Monsanto, NIKE, Pfizer, Phillips, The Procter & Gamble Company, and United Technologies Corporation.

Trade secrets are commercially valuable information not generally known or readily ascertainable to the public by proper means that are subject to reasonable measures to protect the confidentiality of the information. The prototypical example of a trade secret at common law is the customer list, but trade secrets today may include high-tech manufacturing processes, industrial techniques, formulas, or complex data analytic algorithms. Trade secrets constitute roughly two-thirds of the value of companies' information portfolios and are an integral part of a company's competitive advantage, according to a recent Forrester Consulting report.²

American businesses are increasingly the targets of sophisticated efforts to steal proprietary information, harming our global competitiveness. Theft can come through cyber-attack, voluntary or involuntary disclosure by an employee, or misappropriation by a joint venture partner. Often the theft is state-sponsored. Government sources estimated more than a decade ago that the loss of intellectual property for American businesses from cyber espionage is \$200 billion to \$300 billion per year, and those figures are almost certainly higher today.³

The EEA, which made trade secret theft a federal crime, was Congress's first effort to protect American businesses' valuable trade secrets. As I will discuss, many of the problems that animated the passage of that law are of increasing concern today, including the ease with which trade secrets can be stolen using modern technology and the critical nature of trade secrets for our national economy and national security.

² Forrester Consulting, *The Value of Corporate Secrets*, at 2 (March 2010), *available at* <http://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf>.

³ Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage - 2002*, NCIX 2003-10006 (Feb. 2003), *available at* <http://www.fas.org/irp/ops/ci/docs/2002.pdf>; National Bureau of Asian Research, *Report of the Commission on the Theft of American Intellectual Property*, at 11 (May 2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

I. The Economic Espionage Act of 1996

Trade secrets began to receive protection at common law during the middle of the 19th century. As there was scarcely a national market, much less an international market, the law governing and protecting trade secrets developed at the state level because with poor communications and transportation, trade secrets tended to be valuable only within a particular community.

The ad hoc pattern of 50 different state trade secret laws started to change in the 1980's, when states began to codify their laws by adopting the provisions of the Uniform Trade Secrets Act ("UTSA"), a model law developed and proposed to the states by the National Commission on Uniform State Laws. Today, 48 of the 50 states have enacted the UTSA, although often with a number of variances from the proposal, modestly undermining the goal of true uniformity.

It was against this background of state common law and then state statutory protection for trade secrets that the federal government ventured into the field to provide national protection for trade secrets. In 1995, the Department of Justice submitted to Congress a draft bill to make the misappropriation of commercial trade secrets a federal crime. The bill was born of a realization that the trade secrets of American businesses, which had become more and more important to the companies' prosperity, were increasingly under threat.⁴ The threats came from disgruntled employees hoping to harm their former employers or turn profits for themselves by selling trade secrets; from outsiders targeting a company for theft; and, increasingly, from foreign governments using their espionage capabilities against American companies.⁵

⁴ See H.R. Rep. No. 104-788, Economic Espionage Act of 1996, at 4-5 (1996).

⁵ *Id.* at 5.

The Report from this Committee that accompanied the Economic Espionage Act of 1996 found that “the nation’s economic interests are a part of its national security interests” and, thus, “threats to the nation’s economic interests are threats to the nation’s vital security interests.”⁶ The Director of the Federal Bureau of Investigation, Louis Freeh, testified before this Committee in 1996 that the FBI was investigating reports and allegations of economic espionage against U.S. companies by individuals or organizations from 23 different countries.⁷ Despite the increasing attempts at trade secret theft and the challenges such theft posed to our economy, Director Freeh testified that the FBI faced difficulties in prosecuting trade secret theft cases because federal law did not specifically cover the misappropriation of trade secrets.⁸ In some cases, the FBI had conducted investigations only to have federal prosecutors decline to prosecute because of a lack of statutory criminal authority to do so.

The EEA was designed to address that gap in federal criminal law. While federal law had long protected patents, copyrights and trademarks, trade secrets had been left unprotected, even though, as the House Report found, they form “an integral part of America’s economic well-being.”⁹ The House found that state laws “do not fill the gaps left by federal law,” because of the limitations of state laws.¹⁰ “These problems underscore the importance of developing a systematic approach to the problem of economic espionage.”¹¹

⁶ *Id.* at 4.

⁷ *Id.*

⁸ *Id.* at 6.

⁹ *Id.* at 4.

¹⁰ *Id.* at 6-7.

¹¹ *Id.* at 7.

The Senate Committee on the Judiciary also held hearings on what became the EEA and collected data. According to the Senate Judiciary Committee Report, “proprietary economic information is vital to the prosperity of the American economy, [] is increasingly the target of thieves, and [] our current laws are inadequate to punish people who steal the information.”¹² The Senate Judiciary Committee found that as a result of trade secret theft, “American companies have been severely damaged,” losing millions of dollars, jobs, and market share.¹³

Ultimately, the EEA passed by a vote of 399-3 in the House and by unanimous consent in the Senate and is now codified at 18 U.S.C. § 1831 *et seq.* The EEA makes it a criminal offense to misappropriate a trade secret for the benefit of any “foreign government, foreign instrumentality, or foreign agent.”¹⁴ The act also criminalizes the misappropriation of a trade secret “that is related to or included in a product that is produced for or placed in interstate or foreign commerce.”¹⁵ And the act authorizes the Attorney General to initiate a civil action to obtain appropriate injunctive relief for a violation of the law.¹⁶

¹² S. Rep. No. 104-359, The Industrial Espionage Act of 1996, at 5-6 (1996).

¹³ *Id.* at 9 (relying on report of the National Counterintelligence Center).

¹⁴ 18 U.S.C. § 1831(a).

¹⁵ *Id.* § 1831(b).

¹⁶ *Id.* § 1836. Towards the conclusion of Senate consideration of the EEA, a number of businesses requested that the bill include a federal civil remedy for the misappropriation of a trade secret to complement the bill’s criminal provisions and the civil injunctive remedy it provided to the Attorney General. That request was made when the process was quite advanced and a general consensus surrounding the Senate bill had been reached. The provision was not included because it was raised too late in the process, but the thought was that the Congress could turn to that issue the following year. It was seen as a potentially valuable addition, but one that needed to be vetted on its own. For a variety of reasons, primarily that congressional attention on intellectual property issues was next absorbed by the subject that led to enactment of the Digital Millennium Copyright Act and subsequently by patent reform, the addition of a private federal civil remedy was not taken up following enactment of the EEA and lay dormant for a number of years thereafter, only to be renewed recently by members of both chambers, including members of this committee.

II. Recent Legislation

At the end of last Congress, this Committee was responsible for enacting two important laws to strengthen enforcement of trade secret laws. The Foreign and Economic Espionage Penalty Enhancement Act of 2012, P.L. 112-269, introduced by then-Chairman Smith increased penalties specifically for trade secret theft under the EEA for crimes that the perpetrator knows or intends to benefit a foreign government, instrumentality or agent. Fines for individuals were increased from a maximum of \$500,000 to \$5 million, and fines for organizations were increased to \$10 million or three times the value of the stolen trade secret, including expenses for research and design. A House Report on the bill explained that “[b]y strengthening penalties and enhancing criminal deterrence, the bill protects U.S. jobs and technologies while promoting investments and innovation.”¹⁷ The House Report recognized the “significant and growing threat presented by criminals who engage in espionage on behalf of foreign adversaries and competitors.”¹⁸

Congress also sent to the President the Theft of Trade Secrets Clarification Act of 2012, P.L. 112-236, which clarified the scope of the EEA to overturn the Second Circuit’s decision in *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012), but made sure that the EEA continued to apply only to trade secrets related to products or services used in interstate commerce.

These recent legislative successes are important and promising steps to strengthening U.S. trade secrets law, and they have created an environment in which trade secrets are recognized as critical intellectual property entitled to the protection of federal laws in addition to the state laws that have traditionally protected them. They still have not put trade secrets — so

¹⁷ H.R. Rep. No. 112-610, Foreign and Economic Espionage Penalty Enhancement Act of 2012, at 2 (2012).

¹⁸ *Id.* at 1.

valuable to America's most innovative companies — on par with other forms of intellectual property, including patents, trademarks, and copyrights, all of which enjoy protection under a federal civil remedy. Owners of those other forms of intellectual property can protect what is rightfully theirs by taking action in federal court under the patent, copyright, and trademark laws.

Recognizing the value of American trade secrets, Congress has also approved free trade agreements that include specific protections for trade secrets. The U.S.-Colombia Trade Promotion Agreement, for instance, which took effect on May 15, 2012, contains explicit trade secret protections for pharmaceutical and agricultural products, as well as other intellectual property rights protections.¹⁹

III. Congress Should Enact a Federal Civil Remedy for the Misappropriation of Trade Secrets

The EEA, as amended last Congress, provides an important tool in fighting the theft of trade secrets and demonstrates a commitment by Congress to aid in protecting this vital form of U.S. intellectual property. Since enactment of the EEA, the problem of trade-secret theft has grown dramatically. Foreign competitors of U.S. business are trying to steal their way to success on the back of intellectual property developed here in the U.S. Although the EEA has been used successfully in many instances, the FBI has several priorities and limited resources and, as a result, cannot always respond to reports of the theft of a trade secret, even by foreign individuals and firms. Just as we as a society rely on both criminal law and the complementary tools of civil legal process to allow parties to protect their property interests, we should do so in this arena as well.

¹⁹ See M. Angeles Villarreal, Cong. Research Serv., RL34470, *The U.S. Colombia Free Trade Agreement: Background and Issues*, at 5 (2014).

The methods thieves use in their attempts to steal American trade secrets are growing more sophisticated by the day, and our laws must keep pace. American businesses that compete globally will lose their competitive edge — and put at risk thousands of well-paying U.S. jobs — if they cannot quickly pursue and stop thieves who steal their hard-earned secrets to sell to the highest foreign bidder. Federal law must provide our country's innovators and job creators with the tools they need to keep their trade secrets from falling into the wrong hands. The failure to do so risks the global competitiveness of the U.S. economy, which more than ever depends on our innovative intellectual property to provide our competitive advantage over foreign businesses.

Civil trade secret laws originated at the state level, in an era when trade secret theft was largely a local matter. State trade secret laws work well when, for instance, an employee of a local business steals a customer list and takes it to the business down the street. For companies that operate across state and national borders and have their trade secrets threatened by competitors around the globe, the array of state laws is inefficient and inadequate for several reasons.

First, companies need compliance plans to protect their trade secrets. Under the array of state laws, a company that operates in more than one state bears additional and unnecessary costs to protect this form of intellectual property. Second, trade secret theft today is increasingly likely to involve the movement of the secret across state lines. Such multi-jurisdictional movement makes discovery and service of process difficult. Federal courts permit subpoenas to be issued nationwide, but state courts are often not as efficient at obtaining discovery in other states. And third, trade secret cases require swift action by courts across state lines to preserve evidence and protect the trade secret from being divulged. This is particularly true when the

theft is by an individual looking to flee the country, as is increasingly the case. State courts lack the ability of the federal system to serve defendants and prevent the disclosure of the trade secret or destruction of evidence.

Once a trade secret has been divulged, or is made known to a competitor, trade secret protection may be lost forever and the harm from disclosure is often irreparable. Given the mobility we enjoy today, the ease with which people and information travel across state and national borders, relying on disparate state laws and procedures is no longer adequate for the protection of trade secrets in the 21st century. The world of business has changed dramatically in a decade, not to mention since trade secret laws were first developed in the 19th century. U.S. businesses need remedies that enable them to respond immediately and effectively across state lines to protect their trade secrets.

The Senate is considering the Defend Trade Secrets Act, S. 2267, which will create a uniform federal civil remedy for trade secret misappropriation and provide a mechanism to obtain expedited relief when there is a threat that stolen U.S. trade secrets are about to be disclosed or the evidence destroyed. A consistent, harmonized legal framework will provide a more efficient and effective legal structure to protect the valuable intellectual property of American businesses and help protect and promote U.S. global competitiveness and preserve high-quality U.S. jobs. It will also put trade secret protection in-line with the remedies available for owners of other forms of intellectual property. Further, by creating a uniform standard, the legislation will encourage companies to create one set of best practices to protect their trade secrets in every state.

IV. Conclusion

In the information age, knowledge and innovation are our greatest strengths as a country. But for that same reason, they are also the target of sophisticated thieves hoping for a quick

payday on the backs of American businesses. A federal civil remedy for trade-secret theft would provide an important addition to existing protections for trade secrets at the federal and state levels and could potentially bolster our economy at no additional cost.

Mr. COBLE. Mr. Hertling, I thank you for that. I was going to recognize you and welcome you back to the Hill, whether you had made that comment or not, but I thank you for that. I think you are the only witness, Mr. Hertling, who did have Hill experience, so it is good to have you back on the Hill.

Mr. HERTLING. Thank you.

Mr. COBLE. Good to have the other three witnesses as well.

Mr. Simon, you are recognized for 5 minutes.

**TESTIMONY OF DAVID M. SIMON, SENIOR VICE PRESIDENT
FOR INTELLECTUAL PROPERTY, SALESFORCE.COM INC.**

Mr. SIMON. Thank you, Mr. Chairman.

Mr. COBLE. Mr. Simon, pull that mike a little closer to you. I'm not sure you're on yet.

Mr. SIMON. Okay.

Mr. COBLE. That is better.

Mr. SIMON. Thank you, Mr. Chairman, Ranking Member Nadler, and Members of the Judiciary Committee. I want to thank you for the opportunity to discuss the need for a Federal trade secret law on behalf of Salesforce.com.

Trade secrets are vital and important to us. Having been named Forbes magazine's most innovative company for the last 3 years, trade secret law is central to protecting our intellectual property. Unlike conventional software, almost all our software stays in our data centers. Our customers entrust their own and their user status for storage by us so their data can be processed by our servers. Yet it is vital and important to us that any legislation take into account some fundamental differences that have arisen as a result of Internet business models, such as the ones we use, in contrast to old rules based on seizure for physical goods.

Trade secrets differ from other forms of IP in several respects, as many have noted. No government agency needs to examine our secrets to obtain protection as opposed to patents or trademarks. Unlike copyrights, no registration is required before filing a lawsuit. Protection is immediate. As long as our secret information is not accessible to others, has actual or potential value, and is subject to reasonable efforts to keep it secret, the law in the U.S. provides, while disparate, powerful civil and criminal remedies to stop others who try to steal our own or our customers secrets. Given the simplicity of this protection and these strong sanctions, it is little wonder that the National Science Foundation found by a factor of two, U.S. managers believe trade secrets are the most important form of IP protection available.

We appreciate the need for both a strong trade secret protection and strong remedies. I was involved in one of the earliest Economic Espionage Act prosecutions and the ability to seize the stolen trade secrets hidden in the thief's house was key to the success of the prosecution. However, many of the proposals that we have seen provide a seizure power to private civil litigants that we view is far too strong. They fail to take into account the differences between trade secrets and other IP that I just outlined and the difference between physical goods and the Internet economy.

The seizure provisions fail to even take into account that often what is involved is third party's property. If one assumes that one

of our 100,000 customers has misappropriated someone's secrets, that does not justify having marshals enter our storage networks and starting to seize our disk drives. Not only are these drives our property, but the way our proprietary workload and security protocols for data storage work, the data for any one customer is highly likely to be intermixed with the data of hundreds of other customers on any one disk drive. Any drive that were seized would probably also include dozens, if not hundreds of third party secrets. Seizure of the drives also is likely to result in business interruption for the dozens or hundreds of innocent customers whose data is seized. For these reasons alone, we believe that ex parte seizures of innocent third parties who host data for others should be prohibited.

Further, proposed in these overly generous ex parte provisions point too often to counterfeit marks and copyrights to justify their position regarding seizures from third parties. However, that ignores fundamental differences between trademarks and trade secrets. Marks and copyrights in seizure matters are almost invariably concerning physical things. Trade secrets, by their very nature, ethereal. Unlike trademarks and copyrights, trade secrets do not require any form of government approval or registration. Judging on counterfeit marks and copyrights do not require technical expertise. Seizure by marshal requires, on the other hand, of trade secrets also—excuse me—on trademarks also does not require technical expertise. Seizure of computer information stored on disk drives clearly does.

With few district court judges or marshals trained in the details of how computer storage networks work, the right procedures to obtain through secret and unbalanced ex parte hearings needs to be carefully cabined. Nor does the emergency application for relief from a seizure order provide an adequate remedy. District court judges, as this Committee knows, are tremendously overburdened, and Federal Rule of Civil Procedure 65 permits a judge to keep a seizure order in place for up to 14 days without a hearing. The Internet economy often provides the interruption of a customer service, can no—can last no longer than a total of 5 minutes in an entire year, so current seizure rules permit an interruption that is approximately 4,000 times longer than what is often contractually mandated for business on the internet.

In short, trademarks and copyright cases involve physical things that are well understood generally by the legal system. Internet business models of hosting together all sorts of third party information are little understood and need different models. We look forward to working with the Committee on achieving the right balance for a strong trade secret law that also balances the needs of the Internet economy.

Thank you, and I will be happy to answer any questions you may have.

[The prepared statement of Mr. Simon follows:]

Prepared Statement of David M. Simon
Senior Vice President for Intellectual Property
salesforce.com, Inc.

Before the

United States House of Representatives
Committee on the Judiciary,
Hearing of the Subcommittee on Courts, Intellectual Property
and the Internet

On

Trade Secrets: Promoting and Protecting American Innovation,
Competitiveness and Market Access in Foreign Markets

Mr. Chairman, Ranking Member Nadler and members of the House Judiciary Committee, I want to thank you for the opportunity to discuss the need for a federal trade secret law on behalf of salesforce.com. This subcommittee's jurisdiction over both intellectual property and the Internet provides the best forum for balancing the need for robust protection of trade secrets and the privacy of millions of users whose business and lives have come to depend upon the Internet from an overbroad trade secret seizure remedy.

I also believe that my company salesforce.com is well suited to testify about that balance. As Forbes magazine's most innovative company in the world for each of the last three years, trade secrets play a vital role in securing our intellectual property. Offsetting our needs for robust trade secret protection is the even more compelling need to protect the data of our hundred thousand plus business customers and 22,000 charities and educational customers. These customers range from the giants of industry and large multinational charities to small businesses and charities.

To be clear, we believe that federal protection of our trade secrets would be helpful and we support the Congressional efforts to strengthen those protections. Nonetheless, in seeking that protection, we cannot violate our customers' and their users' trust. That trust is core to our business. Our customers, both large and small, trust us to protect their data. They trust us to ensure that we will protect the sanctity and availability of their data. They trust us to ensure that they can reap the benefits that the Internet offers without having their businesses interrupted while protecting their trade secrets. And they trust us to protect their users' privacy. The trust and faith of our customers and their users leads me to be here today to express our concerns with the seizure remedies that we have seen in some of the trade secret proposals. These remedies fail to take into account Internet business models that have emerged over the past decade. Not limiting those remedies could result in the loss of this trust that is so vital to our success by leading to the interruption of our customers' businesses and by comprising the secrecy of their data.

The Importance of Trade Secrets to salesforce.com and the Need for Legislation

While we have concerns about remedies in current proposals, trade secrets are among the most important ways we protect our intellectual property. By the very nature of our offerings, which are almost exclusively software as a service (SAAS), virtually all of the actual software sits on our servers and never leaves our secure environment. Generally speaking, our customers' data sits on those servers too. However, since the vast majority of our code is kept under wraps, the knowledge that the law protects the secrecy of our fifteen year, multibillion dollar investment in our code and computing environment is critical to maintaining the trust of our customers and investors. This code and this environment are

protectable as trade secrets as they are not generally known or readily accessible, have economic value as shown by our multi-year thirty percent year on year growth to a \$ 4 billion per year company and are rigorously kept secret.

And we are not the only company that relies upon trade secret protection. Almost all of our 100,000 plus business customers and 22,000 charitable and educational customers require us to keep their information and data that they entrust to us secret. If the law did not aid us in preserving our customers' secrets, our efforts to gain and keep our customers' trust would be for naught. We know this not only from the probing questions that our customers ask to assure themselves about our security but also from research that shows trade secrets are considered by far the most important form of intellectual property protection.¹

However, the current legal environment for trade secrets has several shortcomings. As many others have noted, US trade secret law is far from consistent. Substantive trade secret law is largely controlled by state laws and in some instances purely by state courts that may still rely on outdated common law doctrines. Even though most states have adopted the Uniform Trade Secret Act, others have not. Further, even the states that have adopted the UTSA have many inconsistencies; the actual individual state statutory texts differ and state court interpretations about even identical versions of the UTSA are far from consistent.² As another example, the definition of trade secrets in the Economic Espionage Act differs from the definition for the same term in the Uniform Trade Secrets Act.³

While some of these differences are subtle, the absence of a uniform federal trade secret law is manifest with respect to international protection. While TRIPs provides an international regime for trade secret law, the protection that is mandated is unfortunately vague. The heart of the relevant clause in TRIPs is vague; it asks whether the trade secret has been acquired or used "in a manner contrary to

¹ According to the National Science Foundation, almost two times the number of managers considers trade secrets the most important form of intellectual property
² D. Almeling, Four Reasons to Enact a Federal Trade Secrets Act 19 Fordham Int. Property & Media Law Review 769, 774 (2009); see also Firetrace USA LLC v. Jesclard, 800 F.Supp.2d 1042 (D. Ariz. 2011)(noting substantial diversity among state court interpretations about whether the Uniform Trade Secrets Act preempts common law remedies).

³ The Uniform Trade Secret Act defines a trade secret as "Trade secret" means information . . . [d]erives independent economic value . . . from not being generally known to . . . other persons who can obtain economic value from its disclosure or use. California Civil Code § 3426.1(d). The EEA defines a trade secret as to information that "derives independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839(3).

honest commercial practices.”⁴ As a result, in Europe alone, trade secret law, which to date is not yet controlled by a European Union Directive, is a patchwork of different forms of protection. What is contrary to honest commercial practices in one country may be considered acceptable in other countries. Thus, in some states trade secret is viewed largely as a creature of contract while in other states, the scope of protection varies with the type of secret at issue.⁵

Far more serious, however, is many countries’ failure to recognize trade secrets as a form of property.⁶ That refusal to recognize trade secrets as a species of property can have major consequences with enforcement authorities. For example, some European authorities have disclosed companies’ trade secrets under the logic that the harm in disclosing a trade secret involves purely commercial interests and is not irreparable.⁷ It may not be a coincidence that in denigrating trade secrets as a form of intellectual property, at least some countries’ regulators seem to adversely impact foreign companies from the United States and elsewhere.

While my understanding is that the United States Trade Representative historically has favored stronger trade secret protection, the representative’s staff have felt hamstrung by the inconsistent protections offered for trade secrets at the state and federal level. The lack of consistent protection means that in negotiations the USTR in trying to improve foreign trade secret protection in bilateral and multilateral talks can only seek the lowest common denominator of those state and federal laws. That lowest common denominator approach arises according to my discussions with prior USTR staffs from their need not to advocate for treaty provisions that are inconsistent with domestic U.S. law.⁸ Since we have almost fifty different versions of trade secret law, the only approach that the USTR can take is to advocate for the lowest common denominator instead of advocating for strong trade secret protection.⁹ The lack of consistent protection means that the USTR is

⁴ Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations 320 (1999), 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994).

⁵ See, e.g., Report of the European Commission Conference of 29 June 2012, “Trade Secrets: Supporting Innovation, Protecting Know-How” 9 (available at ec.europa.eu/internal_market/iprenforcement/docs/conference20120629/ts_summary_consolidatedfinal20120913_en.pdf).

⁶ *Id.* at 15.

⁷ Case T-201/04 R Microsoft v. Commission [2004] ECR II-4463.

⁸ See generally Testimony of Ambassador Marantis, Hearing before the Subcommittee on Trade of the Committee on Ways and Means, U.S. House of Representatives, 120th Congress, First Session, December 14, 2011 Serial No. 112-TR4 (2012).

⁹ To be clear, within the constraint of a lack of a national trade secret policy, the USTR is an excellent resource. For example, the USTR reports regularly highlight inadequacies in trade secret protection with a focus on the adequacy of remedies

restricted in bilateral and multilateral negotiations from trying to improve foreign trade secret protection. Thus, we believe that providing a robust national trade secret policy embodied in a national law will aid the USTR in the development of a robust international trade secret regime without local biases or discrimination that result in inadequate protection.

While we firmly believe that providing a robust federal trade law will aid all businesses, we also believe that the remedies of such a law must recognize that commercial processes have changed since the Uniform Trade Secret Act was drafted in the pre-Internet era. For the reasons that we will now point out, the remedies provisions need to be updated to take into account new commercial realities.

Background on salesforce.com and its Customers in the Internet Age

To understand why the remedies drafted in a pre-Internet era are inadequate today, one needs to understand how software as a service, whether provided by salesforce.com or our competitors, works for hundreds of millions of users here in the US and around the world. salesforce.com relies on the Internet to provide a variety of software as a service. To process and retrieve that data in our service, our customers such as Wells Fargo and the American Red Cross log into their accounts over the Internet and submit their queries to access their data stored on our servers and receive processed information back. They are able to use all of our offerings to run their business without the complexity of running the software themselves.

Our customers' data and our software are stored in large storage arrays that we call pods. While there are always exceptions, few customers have dedicated storage for their information in our system. Rather, systems such as ours scatter the customer data among a host of storage devices. As a result, the data is sometimes in geographically different locations. Individual customer data at the physical level is intermixed with data of other customers according to complex algorithms that take into account workloads, access speed and security. While an individual customer's data may be arrayed across dozens or hundreds of storage devices intermixed with others' data, no customer has the ability to access the other customer's data without that customer's permission. Any one physical drive at any moment in time could have fragments of hundreds of customers' data. In the blink of the eye, our systems that monitor work loads and security may move some or all of those fragments to different systems with different customers' data in our quest for flawless performance. Notwithstanding this intermixing of data, we have a reputation of providing a secure and robust environment for our customers to store and access the data that drive their billion dollar businesses.

and prevention of discriminatory rules. See US Trade Representative, 2014 Special Report 301 Report 16 (available at ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf).

There are a couple of points to draw from this structure, which is not atypical of businesses that host other people's data and provide software as a service over the Internet. Physically removing or seizing any one physical drive unit will generally remove only a fraction of a typical customer's data. Worse, physically removing that drive may also remove data for dozens, if not hundreds, of other customers' data on that unit. And removing that data could interrupt our customers' business, costing them millions of dollars each and in some instances involving medical customers could even jeopardizing people's lives. It is the current proposals' seizure provisions' failure to take into account how information is handled in the information age that concern us.

Seizures in the Salesforce.com Environment

We understand the need for the seizure authority in trade secret law. In a prior job, I was involved with a criminal investigation and subsequent prosecution of economic espionage. Without the FBI's ability to seize thousands of pages of electronic documents that had been stolen, I am not sure that the case could have been brought.

The problem with the seizure provisions included in many proposals we have seen for a federal trade secret law is they do not take into account this new and increasingly common way of doing business over the Internet. Rather, all of the proposals are based off of normal seizure rules in trademark counterfeiting statutes¹⁰ and copyright statutes¹¹ and in Federal Rule of Civil Procedure 65.¹² These rules and statutes were originally drafted before there was an Internet and, in some instances, were first drafted when computer disk drives had not even been invented.¹³

Consideration of how these rules operate in normal trademark and copyright seizure cases demonstrates a need to change the model for the law. First, ex parte seizures are usually authorized in a sealed courtroom with only the plaintiff and counsel present. Based on the facts presented solely by the plaintiff's counsel, the judge makes a determination of whether the goods are a counterfeit. Ordinarily,

¹⁰ The Lanham Act provides for seizure of counterfeit trademark goods. 15 USC § 1116(d).

¹¹ The Copyright Act incorporates by reference certain subsections of §1116(d). See 17 USC § 503(a)(3).

¹² While on its face, Federal Rule of Civil Procedure 65 does not refer to seizures, courts have approved the appropriateness of using Rule 65 to authorize ex parte seizure orders. See, e.g., First Technology Safety Systems, Inc. v. Depinet, 11 F.3d 641 (6th Cir. 1993)(finding § 503(a)(3) inapt and analyzing the appropriateness of a seizure under Rule 65).

¹³ Federal Rule of Civil Procedure 65 was first adopted in 1937. Section 1116(d) was added in 1984 by Pub. L. 98-473, 88 Stat. 1949 (1984).

that requires no technical expertise. In a trade secret case, however, what is a trade secret requires a technical analysis—an analysis that few judges are able to make on their own.¹⁴

These technical determinations go far beyond what is or is not a trade secret. Often trade secret plaintiffs want to seize hard drives to see whether forensics can establish what the alleged wrongdoer may have erased.¹⁵ An expert may submit a truthful declaration about forensics about what information can be gathered from a disk drive taken from a personal computer. The typical trial judge with a degree in history or political science may well be swayed by such “evidence” along with having heard war stories over the years regarding what can be discovered from a disk drive. Yet, the non-party hosting the data will not be present and will be unable to tutor the judge that a PC environment is totally irrelevant to a cloud-based storage warehouse with data being replicated and shifted constantly, irrespective of what the data owner is doing. Nor will the party who hosts the data be able to explain to the judge that this forensic analysis could expose otherwise legally protected third party data, such as health records. Grave harm could be done in the face of such overly zealous or poorly informed private litigants.

Further, the plaintiff who is asking for the ex parte relief will ask the judge for a de minimus bond. Judges have broad discretion in setting bonds and the bond amounts are often hastily arrived at with little or no consideration of the real harms. Many judges believe that requiring significant security or bonds will deny plaintiffs the relief they seek and therefore set de minimus amounts for the security.¹⁶ While a party can recover against security ordered by the court, recovery by the injured party exceeding the amount of the security is a rare exception.¹⁷ That is a first problem with current security requirements for injunctions as security is often too low in view of the potential for harm. Further, Federal Rule of Civil Procedure 65 has a major shortcoming as the amount of security posted only covers the harm to parties in the litigation.¹⁸ The result is that if a court grants a seizure order against

¹⁴ While it is noted that in technical patent cases judges often get tutorials from both sides in the litigation and can appoint their own technical experts, in the context of an ex-parte hearing in a sealed courtroom, these aids are not available to the court.

¹⁵ See *Lexis-Nexis v. Beer*, 41 F.Supp.2d 950 (D. Minn. 1999)(forensic analysis of defendants’ hard drive showed erasure of plaintiff’s files).

¹⁶ In *Bragg v. Robertson*, 54 F. Supp. 2d 635 (S.D. W. Va. 1999) where the court granted a \$5000 bond and then the appellate court reversed the granting of the injunction, leaving the plaintiff with no effective remedy. *Bragg v. W. Va. Coal Ass’n*, 248 F.3d 275 (4th Cir. 2001).

¹⁷ *Intl Assn of Machinists v. Eastern Airlines, Inc.*, 925 F.2d 6, 10 (1st Cir. 1991).

¹⁸ Federal Rule of Civil Procedure 65 (c) “The court may issue a preliminary injunction or a temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained.” See *O. Grosskopf*

an alleged misappropriator that harms innocent third parties such as salesforce.com, or its customers, there is no ability to recover against the security, even if the amount set was adequate. Thus, current security and bond practice for seizures have several shortcomings.

That harm does not stop at the courtroom, however. When the marshal accompanied by plaintiff's representatives arrives at the storage site, the same technical issues that confronted the district court judge also confront the marshal.¹⁹ Assuming the site owner who hosts the alleged misappropriator's data decides not to risk a contempt citation and admits the marshal (and the marshals do have guns and badges after all), the marshal will be confronted with row after row of equipment racks with hundreds of cables. The site owner is then faced with a Hobson's choice. Either it must comply with the court order, if even possible, by removing disk drives and interrupting the business not only for the alleged misappropriator, but also of dozens or hundreds of innocent customers. Alternatively, the owner of the storage site may refuse compliance so that the businesses of thousands of thousands of customers continue to run but risk contempt citations.

Proposed Solutions

Despite highlighting a number of potential problems with trade secret seizures, we do believe in strong trade secret remedies but subject to certain protections. We believe that the remedy needs procedural and substantive safeguards that are not reflected in the copyright and trademark law remedies that antedate the Internet and software as a service. Our belief is that courts should be prescribed from ordering any seizure of third parties hard disk drives absent compelling evidence of wrong doing by the third-party. Absent such evidence, the appropriate remedy for those who host third-party information is to require the third-party hosting entity to deny access to the specified information and create a copy of the relevant information.

If Congress believes that there are truly unique situation where the harm to third parties justifies seizure of media from a business that hosts third party data, then several protections must be provided. First, the law needs to explicitly recognize that ex parte orders for the seizure of property owned by innocent third parties should be ordered in only the rarest of circumstances. Most hosting

& B. Medina, Remedies for Wrongfully-Issued Preliminary Injunctions, 32 Seattle Law Review 903 ,909 (2009).

¹⁹ See generally A. Kramer & M. Sommers, Taking an Aggressive Stance Against Counterfeiters: An Overview of Trademark Counterfeiting Litigation under the Lanham Act, IP Litigator, September/October 1999 (last viewed at <http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=d0fb159b-947e-427a-b03a-e6d60cf272f5>).

agencies already have the ability to either deny access to accounts or download all of the information in the account that can then be sequestered in case of subsequent attempts to change the information. salesforce.com regularly accomplishes these tasks when responding to subpoenas or other judicial orders. Once access has been denied and the information has been copied, the court can provide for an evidentiary hearing permitting a third-party hosting entity and others who may be harmed by a seizure order to argue to the court whether a seizure is the appropriate remedy on a full evidentiary record. Simply put, there needs to be a heavy thumb on the scales for when the courts so that ex-parte seizures in such circumstances are truly rare.

Second, to avoid harm to the innocent host and their other customers, the law should compel a plaintiff seeking a seizure has to come forward with clear and convincing evidence that the harm it will suffer grossly outweighs the harm the seizure may impose upon these third parties, including the business disruption they may suffer. That showing should also expressly require the party seeking such extraordinary relief to demonstrate clear and convincing evidence why other less damaging alternatives such as denial of access to the information and storing a copy of the information of concern is inadequate.

Third, the court should ensure the information of the innocent third parties is not placed in jeopardy. In particular, upon seizure, the court should direct that the media be placed in the custody of a trusted third-party who will segregate the alleged misappropriator's information from other information and only the directly relevant information may be provided to the plaintiff's counsel under a suitable attorneys eyes only protective order. Otherwise, we could be allowing the information of innocent customers to be put in jeopardy by the process.

Fourth, current procedural rules permit up to fourteen days before a court is required to permit others' to seek judicial intervention to either expunge or limit a seizure order. That is simply too long of a period. Given the potential disruption to innocent hosts and third-parties, the host and any customer or user should be permitted to seek emergency relief from the order within four hours. Many customers insist on "seven-nine's service (99.99999%) up time." Translated into laymen's terms, that means they expect less than six minutes of interruption in an entire year to their service. Anything longer simply results in too much harm. As a result, the right to seek urgent relief from an ex-parte order is just as important as the right for plaintiffs to be able to obtain prompt ex-parte relief and rules need to reflect this urgency.

Fifth, the security that the court requires to protect against erroneous seizure orders cannot be the limit that is placed upon third-parties inadvertently harmed by the order. Current law only requires bonds for parties but non-parties will need protection if seizures are permitted under this regime. Arbitrary limits from security regimens designed to protect only plaintiffs are demonstrably inadequate. My experience in trademark and copyright cases is that these security amounts are

often an afterthought and bonds rarely exceed \$100,000. Judges even have discretion to set the security at zero.²⁰ Rather, in entering the order, the court should require security commensurate with the number of potentially impacted parties and the magnitude of their businesses along with providing an advisory to the plaintiff that the plaintiff is liable for all harms that the seizure order can ensue. Such financial incentives have long been recognized as a way to avoid over zealous litigants; even the drafters of the Uniform Trade Secret Act included a provision to deal with abusive trade secret plaintiffs.²¹ Simply put, changes in technology during the last twenty years raise the need for adequate protection from such overzealousness where the potential harm to third parties have escalated since the drafting of the UTSA.

Conclusion

While we believe in strong trade secret remedies, we also believe that if we are going to enhance our trade secret protections then the seizure provisions need to also be updated to reflect modern commercial practices. Information stored over the Internet by alleged misappropriators is intertwined with third parties' information and seizure orders places those third parties' businesses and confidential information at risk. Given this committee's special purview over the Internet, we trust that any legislation will provide adequate protections.

²⁰ *District 17, United Mine Workers Assoc. v. A & M Trucking, Inc.*, 991 F.2d 108, 110 n.2(4th Cir.1993)(“The court’s complete silence as to the bond requirement for the injunction distinguishes the instant case from those in which a court, in its discretion, chooses to set the bond amount at zero.”)

²¹ See, e.g., Section 4 of the Uniform Trade Secret Act, providing for attorneys fees for “claims of misappropriation in bad faith.”

Mr. COBLE. Thank you, Mr. Simon.
Mr. Burns.

**TESTIMONY OF THADDEUS BURNS, SENIOR COUNSEL,
INTELLECTUAL PROPERTY & TRADE, GENERAL ELECTRIC**

Mr. BURNS. Good afternoon, Chairman Coble, Ranking Members Nadler and Conyers, and Members of the Committee, thank you for inviting me to testify today on the importance of trade secret protection for job-creating companies in America. My name is Thaddeus Burns, and I am Senior Counsel, Intellectual Property and Trade, at General Electric, a company that has been at the forefront of innovation since 1892. I am here today on behalf of the Intellectual Property Owners Association, a trade association representing more than 200 companies and 12,500 individuals in all industries and fields of technology. Trade secrets are an increasingly important form of intellectual property for IPO members. We invest significant resource to develop proprietary know-how, such as manufacturing processes, industrial techniques, formulas, codes, and designs. The value of our trade secrets is not lost on competitors here and around the world, and the theft of our intellectual property has become a growing problem.

The threat comes from numerous sources, and the rise of global supply chains and perpetual connectivity has made it even easier for would-be thieves. And when our trade secrets land in the hands of a rival, we are put at a competitive disadvantage. Trade secret theft has become more sophisticated, and companies have responded by raising our internal defenses, but the law also needs to keep pace. The current legal tools available to remedy trade secret theft are unnecessarily inefficient and inconsistent with other areas of intellectual property law.

The Economic Espionage Act is the Federal law that protects trade secrets but, as a criminal law, has its limitations. The FBI and Department of Justice do an excellent job, but they have limited resources, numerous priorities, and would never be in a position to bring charges in all instances of trade secret theft.

Most States have adopted civil remedies based on the Uniform Trade Secrets Act. These laws work well to remedy local and intrastate trade secret theft, such as the case of an employee who takes a customer list to the competitor across town, but State courts are not well suited to respond to the nature of trade secret theft today, which is increasingly likely to involve the movement of trade secrets across State and even international lines and requires swift action by courts to preserve evidence and protect the trade secret from being divulged.

IPO, therefore, supports the creation of a Federal civil remedy for trade secret misappropriation which would allow a trade secret owner to act more quickly across State lines. Owners of other forms of intellectual property, copyright, patents, and trademarks can enforce their rights in Federal court. IPO urges this Committee to consider effective and balanced legislation to create a similar remedy for trade secret owners that responds to the increasingly sophisticated nature of trade secret theft today.

Importantly, a Federal civil remedy will not increase litigation. Businesses will never be shy about protecting our property rights

when our investment in R&D are stolen. We will act to protect our trade secrets, whether it means going to State court or Federal court, but a Federal remedy will be more efficient and effective.

A Federal civil remedy is also important to our global competitiveness. The ability of American companies to access foreign markets is affected by the protection those markets provide for intellectual property. The U.S. Trade Representative's Office prepares a Special 301 Report each year identifying trade partners in marketplaces that have inadequate IP protection. IPO submitted comments earlier this year as part of that process which highlights the problem of inadequate trade secret protection.

If the United States leads by example, however, we have an excellent opportunity to raise and harmonize the global framework for trade secret protection. Enacting legislation that creates the gold standard for trade secret protection will be important as the EU considers its trade secrets directive and as the United States negotiates multilateral trade agreements and bilateral investment treaties.

In conclusion, IPO supports a Federal civil remedy for trade secret theft because our member companies, creators of innovative products and demand around the world, and creators of good well-paying jobs in the United States, know that our value is in our ideas and our creativity. We are increasingly being targeted by sophisticated efforts to steal our proprietary information. A Federal civil remedy will provide important tools we need to safeguard our valuable know-how and to continue to lead the world in creating new and innovative technologies, products, and services.

Thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Burns follows:]

Hearing on

**“Trade Secrets: Promoting and Protecting
American Innovation, Competitiveness and
Market Access in Foreign Markets”**

**U.S. House of Representatives Committee on the Judiciary
Subcommittee on Courts, Intellectual Property and the Internet**

June 24, 2014

**Written Statement of Thaddeus Burns
Senior Counsel, Intellectual Property & Trade
General Electric**

on behalf of

**Intellectual Property Owners Association
(IPO)**

**Testimony of Thaddeus Burns
Senior Counsel, Intellectual Property & Trade, General Electric
on behalf of
Intellectual Property Owners Association (IPO)**

**“Trade Secrets: Promoting and Protecting American Innovation,
Competitiveness and Market Access in Foreign Markets”
June 24, 2014**

Introduction and Summary

Good afternoon Chairman Coble, Ranking Member Nadler, and Members of the Committee. Thank you for inviting me to testify today on the importance of trade secret protection for American companies.

My name is Thaddeus Burns, and I am Senior Counsel, Intellectual Property & Trade, at General Electric, a company that has been at the forefront of innovation since 1892. I am here today on behalf of Intellectual Property Owners Association (“IPO”), a trade association representing companies and individuals in all industries and fields of technology who own, or are interested in, intellectual property rights. IPO’s membership includes more than 200 companies and more than 12,500 individuals who are involved in the association either through their companies or as inventor, author, law firm, or attorney members.

Trade secrets are an increasingly important part of IPO members’ intellectual property portfolios. IPO members have developed, at significant cost, a host of trade secrets that give each of us a competitive edge and help us outcompete in today’s challenging global markets. These trade secrets are manufacturing processes, industrial techniques, proprietary technologies, formulas, codes, designs, and customer lists. Our competitiveness in the global economy

depends on this information remaining confidential. In all, trade secrets constitute roughly two-thirds of the value of companies' information portfolios.¹

The value of our trade secrets is not lost on competitors here and around the world. Trade secret misappropriation is a large and growing problem. The threat comes from company insiders who would take our trade secrets and sell them to the highest bidder, and outsiders including both competitors who try to infiltrate our networks and foreign governments and companies overseas using their espionage capabilities against American companies. The rise of sophisticated technology, perpetual connectivity, and globalized supply chains has made it even easier for would-be thieves to access competitively sensitive information. And when that information lands in the hands of a rival, the rival can replicate market-leading innovations at a fraction of the cost, bypassing the years of research and development we put into our products.

We have raised our defenses and are employing the best technologies and strategies to protect our intellectual property. But federal law has not kept pace with the technological innovation that has enabled increased trade secret theft. IPO therefore supports the creation of a federal civil remedy for trade secret misappropriation, to enhance trade secret protection for innovators and give us the tools to protect ourselves. Owners of other forms of intellectual property - copyrights, patents, and trademarks - can enforce their rights in federal court. Trade secret owners should have a similar remedy. At stake are the continued competitiveness of market-leading American companies and the millions of jobs we provide.

¹ Forrester Consulting, *The Value of Corporate Secrets*, at 2 (March 2010), *available at* <http://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf>.

I. The Current Legal Regime Does Not Provide Sufficient Trade Secret Protection

The current legal tools available to remedy trade secret theft are unnecessarily inefficient and inconsistent with other areas of intellectual property law. In the United States, these tools comprise the Economic Espionage Act of 1996 (“EEA”), a criminal law, and an array of state laws that provide civil relief.

The EEA is an important law that makes it a crime to steal trade secrets for the benefit of a foreign government or for economic gain. But the EEA is a criminal statute, and criminal law to protect intellectual property has two important limitations. First, the Department of Justice has limited resources and is not in a position to bring charges in all cases of interstate trade secret theft. Second, criminal law punishes the defendant, but the process for compensating the victim is unwieldy, particularly when compared to relief available under civil law.

Federal statutes provide owners of other forms of intellectual property (patents, copyrights, and trademarks) the right to bring a civil action in federal court to recover damages and, in appropriate cases, enjoin further infringement. There is, however, no analogous federal right to enforce trade secrets. We believe there should be. A federal civil remedy would provide a consistent, unified framework for intellectual property protection at the federal level. The tactics employed by those seeking to steal trade secrets are becoming increasingly sophisticated and frighteningly effective; our law simply must keep pace.

Most states have adopted civil remedies based on the Uniform Trade Secrets Act. These laws work well to remedy local and intrastate trade secret theft, such as the case of an employee who takes a customer list to the competitor across town. But today, the increased digitization of critical data and increased global trade have made it easier than ever before to misappropriate vast quantities of data and transport it across state and international boundaries. As a result, trade secret misappropriation cases today often involve actors and witnesses in multiple

jurisdictions within the United States and, increasingly, overseas. State courts, unlike federal courts, are not able to provide for prompt nationwide service of process to join parties and to secure testimony and other evidence. And the fact that data can be copied and transferred far more quickly than in the past heightens the need for immediate relief to halt misappropriation, before the value of a trade secret is lost.

The need for immediate action to remedy trade secret theft is perhaps most pronounced when the theft is by an individual looking to flee the country. State courts are not well equipped to respond to applications for urgent assistance in cases where the defendant has crossed state lines, and they lack the ability of the federal system to protect a trade secret stolen by such a defendant. Whatever the mode of misappropriation, once the trade secret has been divulged, or is made known to a competitor, trade secret protection may be lost forever and the harm from disclosure is often irreparable.

II. IPO Supports a Federal Remedy for Trade Secret Misappropriation

Innovative companies would benefit greatly from a uniform federal remedy that reflects the sophisticated nature of trade secret misappropriation today. IPO supports efforts to create a federal remedy that give trade secret owners access to federal courts to respond quickly to trade secret misappropriation. In IPO's view, an effective remedy would provide the advantages of federal service of process and provide for the speedy entry of orders, including on an *ex parte* basis when warranted to prevent an imminent misappropriation, the dissemination of a stolen trade secret, and to preserve evidence.

Any legislation should be balanced, however, and provide adequate protection against improper use of the statute - particularly when an *ex parte* process is used. While the federal civil remedy should authorize the seizure of a stolen trade secret in limited, appropriate circumstances, the provision must contain safeguards to prevent abuse, including damages in the

event of wrongful seizure and protection of the information seized to protect against inappropriate access to the information.

A federal civil remedy will not lead to increased litigation. Businesses will never be shy about protecting our rights when our investments in research and development, protected by trade secret law, are stolen. We will act to protect our trade secrets, whether it means going to state court or federal court. But a federal remedy will be more efficient and effective. We will be able to go to a single federal judge, rather than running to multiple state courts to stop interstate and international misappropriation.

The need is urgent. The U.S. Department of Defense has noted that “[e]very year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies.”² In a 2012 speech, General Keith Alexander, the then-head of the National Security Agency and U.S. Cyber Command, stated that IP theft due to cyber espionage is the “greatest transfer of wealth in history,” estimating that U.S. companies lose \$250 billion per year due to IP theft.³ In the United States, federal cases of trade secret theft doubled between 1988 and 1995, doubled again between 1995 and 2004, and are projected to double again by 2017.⁴

The effect of trade secret misappropriation can be measured in dollars lost, jobs cut, new hiring not undertaken, and innovation stifled. For example, when a Ford Motor Co. engineer

² Dep’t of Defense, *Strategy for Operating in Cyberspace*, at 4 (July 2011), available at <http://www.defense.gov/news/d20110714cyber.pdf>.

³ Josh Rogin, *NSA Chief: Cybercrime Constitutes the “Greatest Transfer of Wealth in History,”* The Cable, July 9, 2012, available at http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

⁴ David S. Almeling, *et al.*, *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 293 (2010).

copied 4,000 documents and went to work for a competitor, Ford estimated its losses at \$50 million.⁵ A technology company shut down after its proprietary source code was misappropriated.⁶ The Commission on the Theft of American Intellectual Property, co-chaired by Dennis Blair and Jon Huntsman, found that “illegal theft of intellectual property is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone.”⁷

The passage of legislation to create a federal civil remedy will provide an important additional tool to protect American innovation and promote investment in research and development, and the jobs and economic prosperity such R&D will generate.

III. Protection of Trade Secrets Abroad

The ability of American companies to access foreign markets is affected by the protection those markets provide for intellectual property. The Office of the United States Trade Representative (USTR) prepares a “Special 301 Report” each year that identifies trade barriers to American companies due to inadequate or ineffective intellectual property protection. The Special 301 Report is an important tool for putting trade partners on notice about concerns related to their intellectual property protection and, in some instances, for setting the stage for

⁵ See Matthew Dolan, *Ex-Ford Engineer Pleads Guilty in Trade-Secrets Case*, Wall St. J., Nov. 17, 2010.

⁶ See S. Rep. No. 104-359, at 9 (1996) (reporting how the source code of Ellery Systems of Boulder, Colorado, which supplied software technology to government projects, was stolen, destroying the financial viability of the company).

⁷ The National Bureau on Asian Research, *The Report of the Commission on the Theft of American Intellectual Property*, at 1 (May 2013), available at http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

trade enforcement action. In 2013, for the first time, USTR included a designated section on trade secret theft in its Special 301 Report.

IPO submitted comments earlier this year to USTR in response to USTR's request for public comment in preparation for the Special 301 Report. IPO's comments highlighted the problem of trade secret misappropriation overseas and discussed where there are significant problems around the world. Issues of concern include forced regulatory disclosure of trade secrets, compulsory licensing, uneven enforcement, difficulties in evidence gathering to prove trade secret theft, and an overall lack of effective intellectual property protection. Inadequate protection of trade secrets abroad harms not only companies whose property is stolen, but also the country where the theft occurs, because companies are then less likely to form joint ventures and make high-value global supply chain investments in those countries.

Despite the challenges, we see some near-term opportunities to strengthen the global framework for intellectual property rights. The United States must be a leader in trade secret protection. A federal civil remedy for trade secret misappropriation is important for our global trade agenda. To date, the United States has not consistently received cooperation from international jurisdictions in protecting trade secrets in part because it does not have its own federal civil statute to reference in encouraging the adoption and enforcement of similar legislation by its treaty partners. Many countries provide insufficient protections for trade secrets, which presents significant economic risks to American companies seeking to expand operations globally. Establishing such a remedy is particularly important as the European Union considers its Trade Secrets Directive and as the United States negotiates multilateral trade agreements and bilateral investment treaties.

The issue of trade secret protection has already been included in draft negotiating agendas for both U.S. and EU negotiators in the Transatlantic Trade and Investment Partnership (TTIP) negotiations. Including trade secrets in a future TTIP Agreement will allow the U.S. and EU to set the “gold standard” for trade secrets protection worldwide. Trade secrets language has also been included in the Trans-Pacific Partnership (TPP) negotiations. Japan’s entry into the negotiations provides a further opportunity to strengthen trade secrets protection in the agreement and throughout the Asia-Pacific region.

IV. Conclusion

IPO supports a federal civil remedy for trade secret theft because our member companies — creators of innovative products in demand around the world and creators of good, well-paying jobs in the United States — know that our value is in our ideas and our creativity. We are increasingly being targeted by sophisticated efforts to steal our proprietary information. In our global, information-based economy, the U.S.’s most valuable currency is our knowledge. A federal civil remedy will provide important tools we need to safeguard our valuable know-how and to continue to lead the world in creating new and innovative technologies, products, and services.

Mr. COBLE. Thank you, Mr. Burns.
Mr. Moore.

TESTIMONY OF CHRIS MOORE, SENIOR DIRECTOR, INTERNATIONAL BUSINESS POLICY, NATIONAL ASSOCIATION OF MANUFACTURERS

Mr. MOORE. Chairman Coble, Ranking Member Nadler, and Members of the Subcommittee, thank you for your focus on the protection of trade secrets and for the opportunity to testify today. My name is Chris Moore, and I am Senior Director for International Business Policy at the National Association of Manufacturers. The NAM is the largest industrial trade association in the United States with more than 12,000 members in all 50 States.

Mr. Chairman, U.S. global leadership in manufacturing depends on the strong protection and enforcement of intellectual property rights, including trademarks, copyrights, patents, and trade secrets, both at home and abroad. Today, trade secrets are more important than ever before to manufacturers small and large. Trade secrets are acquired and developed at significant cost and through many years of company experience and investment. They provide a powerful business advantage in highly competitive sectors, like manufacturing, but trade secrets are not exclusive rights. Once disclosed, their value is lost forever. Theft has a measurable real world impact. It costs good-paying American jobs and can even put entire businesses at risk.

Trade secrets are particularly vital for small- and medium-sized businesses that account for the vast majority of NAM members. For many of these firms, trade secrets are their intellectual property, but trade secrets increasingly are at risk in today's more mobile and interconnected global economy. Trade secrets theft is increasingly interstate and international in scope. Manufacturers, small and large, are doing everything they can to harden their networks and safeguard their trade secrets. Congress and the Administration also have critical roles to play in ensuring America's laws and policies are equal to today's threats.

Specifically, NAM urges the Committee to support legislation that would provide access to Federal civil enforcement for trade secret misappropriation. Such access is vital because State courts are not always well suited to working quickly across State and national boundaries to facilitate discovery, serve defendants or witnesses, or prevent a party from leaving the country. The time it takes to bring action in multiple State courts gives thieves the advantage and prevents trade secret owners from acting promptly to protect proprietary information and preserve evidence. The cost of taking action across jurisdictions can effectively bar businesses and especially small businesses from using a key tool to defend their rights.

Mr. Chairman, the fact that trade secret owners don't have the same access to Federal civil enforcement as owners of every other intellectual property right leaves them without an essential means to deter theft and recover losses. It also makes it harder for the United States to lead internationally and to work with our overseas trading partners to improve trade secret protection and enforcement around the world.

Trade secret protection and enforcement is still inadequate in many countries and regions, putting industrial know-how and technology at risk. But with access to Federal civil enforcement, along with effective criminal protection of trade secrets already provided for under the Economic Espionage Act, there are concrete opportunities to strengthen protection and enforcement overseas. Through trade agreement negotiations and through ongoing engagement in bilateral and multilateral forums, the United States can make common cause with Europe, with Japan, and others around the world that are facing similar challenges and beginning to pursue their own solutions.

Chairman Coble, Ranking Member Nadler, and Members of the Subcommittee, manufacturers need your help to ensure they can effectively and efficiently protect and enforce their trade secrets at home and abroad.

Thank you for the opportunity to testify this afternoon. I look forward to answering any questions you may have.

[The prepared statement of Mr. Moore follows:]



Testimony

of Chris Moore
Senior Director
International Business Policy
National Association of Manufacturers

*before the House Judiciary Committee
Subcommittee on Courts, Intellectual Property and the Internet*

*on "Trade Secrets: Promoting and Protecting American Innovation,
Competitiveness and Market Access in Foreign Markets"*

June 24, 2014



**TESTIMONY
OF CHRIS MOORE
SENIOR DIRECTOR, INTERNATIONAL BUSINESS POLICY
NATIONAL ASSOCIATION OF MANUFACTURERS**

**“TRADE SECRETS: PROMOTING AND PROTECTING AMERICAN INNOVATION,
COMPETITIVENESS AND MARKET ACCESS IN FOREIGN MARKETS”
JUNE 24, 2014**

**BEFORE THE
HOUSE JUDICIARY COMMITTEE, SUBCOMMITTEE
ON COURTS, INTELLECTUAL PROPERTY AND THE INTERNET**

Chairman Coble, Ranking Member Nadler and members of the Subcommittee on Courts, Intellectual Property and the Internet, thank you for your focus on the protection of trade secrets and for the opportunity to testify today.

My name is Chris Moore, and I am the Senior Director for International Business Policy at the National Association of Manufacturers (NAM). The NAM (www.nam.org) is the largest industrial trade association in the United States, representing more than 12,000 manufacturers in all 50 states. Manufacturing employs nearly 12 million women and men across the country, contributed more than \$2.08 trillion to the U.S. economy in 2013 and accounts for two-thirds of private sector research and development.

Today, trade secrets are more important than ever to manufacturers small and large. These vital intangible assets include everything from proprietary manufacturing plans, processes, techniques, codes and formulas to research, marketing data and customer lists. The trade secrets of publicly traded U.S.

companies alone are worth an estimated \$5 trillion. The trade secrets of privately held firms surely add much more to the total.

Trade secrets are acquired and developed at significant cost and through many years of company experience and investment. They provide a powerful business advantage in highly competitive sectors like manufacturing – but only as long as they remain confidential. Trade secrets are not exclusive rights. Once disclosed, their value is lost forever. Theft has a real, measurable, real-world impact. It costs good-paying U.S. jobs and can even put entire businesses at risk.

Trade secrets are particularly important for small and medium-sized businesses that account for the vast majority of NAM members. For many of these firms, trade secrets are their intellectual property. They rely on trade secrets to protect their innovations, often because they are less expensive to retain and enforce than patents. They leverage the expertise of their employees to manufacture custom products that meet specific customer performance requirements through proprietary processes.

That's why addressing the serious and growing threat of trade secrets theft is so essential. The trade secrets on which many small and medium-sized businesses rely are increasingly at risk in today's mobile and interconnected global marketplace. Estimates of losses from trade secrets theft range from one to three percent of GDP in the United States and other advanced developed economies.¹ The head of the National Security Agency believes theft costs American companies \$250 billion per year.²

¹ Center for Responsible Enterprise and Trade and PWC, "[Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats.](#)" February 2014.

² Josh Rogin, "[NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History.'](#)" *Foreign Policy*, July 9, 2012.

In our parents' or grandparents' day, trade secrets often were stolen by individual employees acting alone. They took paper documents and sold them to competitors across town. Now, trade secrets are digital and vulnerable to anonymous hackers operating as part of criminal enterprises. Proprietary information that might once have taken a moving truck to transport can walk out the door on a thumb drive and be sold to competitors half a world away.

Manufacturers small and large are doing everything they can to harden their networks and safeguard their trade secrets. They protect their trade secrets through non-disclosure contracts, technological security measures and other means. They educate their employees about the importance of protecting proprietary information and the potential business impact if trade secrets are stolen or disclosed. Those measures are costly, but unfortunately all too necessary.

But there is only so much individual businesses can do alone. Congress and the Administration have critical roles to play in ensuring America's laws and policies are equal to today's threats. The good news is that Washington is recognizing the problem. Congress has introduced and passed legislation that is helping to upgrade our nation's laws for the 21st century.³ The White House has organized federal agencies behind a strategy to mitigate trade secret theft.⁴

Those are critical steps, but they're not enough. We need to step up our game. We need to ensure federal law keeps pace with technological changes that increasingly enable trade secret theft. That's why the NAM supports measures that enhance trade secret protection, raise the stakes for criminals and enable businesses to better protect and enforce their rights, including legislation

³ See, for example, the Foreign and Economic Espionage Penalty Enforcement Act, which was passed by Congress and was signed into law on January 14, 2013.

⁴ Office of the Intellectual Property Enforcement Coordinator, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013.

that would provide access to federal civil enforcement of trade secret misappropriation.

Access to federal court is critical for businesses of all kinds. State civil trade secret laws alone often are not sufficient to deter and remedy interstate theft. State courts are not always well suited to working quickly across state and national boundaries to facilitate discovery, serve defendants or witnesses, or prevent a party from leaving the country. State laws can vary, making it harder for firms to craft consistent policies.

When a trade secret is stolen, its owner must act quickly to protect proprietary information and preserve evidence. Without access to federal courts, thieves have the advantage. As an NAM Board member and small business owner testified before the Senate Judiciary Committee last month: "there are at least six airports with international flights within a two-hour drive from my facility. Five of those airports are in other states. By the time multiple state courts take action, the criminals will be long gone."⁵

Beyond any delays, taking civil action to protect trade secrets across multiple jurisdictions is also difficult and costly, particularly for small businesses. Unless small businesses have legal firms on retainer in different states, which most do not have, they effectively are barred from using a key tool to defend their rights. That needs to change, and the NAM urges the Judiciary Committee to support legislation providing access to federal courts for trade secret theft.

The fact that trade secret owners do not have the same access to federal civil enforcement as owners of every other form of intellectual property right – including patents, trademarks and copyrights – leaves them without an essential means to deter theft and recover any losses. It also makes it harder for the

⁵ [Testimony of Drew Greenblatt](#), President and Owner of Marlin Steel Wire Products, before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, May 13, 2014.

United States to lead internationally and to work with our overseas partners to improve trade secret protection and enforcement around the world.

Trade secret theft is increasingly global in scope.⁶ As the NAM highlighted in its written comments for the Office of the U.S. Trade Representative's 2014 Special 301 Report: "[t]rade secret protection and enforcement is still inadequate or non-existent in many countries and regions, putting industrial know-how and technology at risk and making it harder for U.S. companies to trade, do business and collaborate with local partners and suppliers in countries around the world."

The United States must meet the global challenge of trade secrets theft with global solutions. With access to federal civil enforcement, along with effective criminal protection of trade secrets already provided for under the Economic Espionage Act, there are concrete opportunities to strengthen protection and enforcement abroad.

Trade secrets are already on the table in ongoing Transatlantic Trade and Investment Partnership (T-TIP) and Trans-Pacific Partnership (TPP) negotiations and the NAM is seeking outcomes that will provide improved protection U.S. trade secrets in foreign markets. To ensure strong outcomes on trade secrets and other issues in these and other negotiations, it is also vital that Congress act soon to pass trade promotion authority, the Congressional-Executive framework that empowers Congress to set negotiating objectives, requires the Administration to consult with Congress and other stakeholders before, during and at the conclusion of the negotiations, and provides for Congressional consideration of the final agreement. The Congressional Bipartisan Trade Priorities Act of 2014 (H.R. 3830),⁷ introduced by Ways and Means Chairman Camp and Senate leaders, is a well-crafted bill that would ensure stronger and

⁶ See, for example, Office of the National Counterintelligence Executive, "[Foreign Spies Stealing U.S. Economic Secrets in Cyberspace](#)," October 2011; and Defense Security Service, "[Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting](#)," 2013.

⁷ The NAM submitted these comments on this legislation found [here](#).

better outcomes in TPP and T-TIP trade negotiations if this legislation can be moved quickly toward passage.

Through trade agreement negotiations and through ongoing engagement in bilateral and multilateral forums, the United States can make common cause with Europe, Japan and others around the world that are facing the same challenges and beginning to pursue their own solutions. Our partners have a shared stake in the success of that endeavor. They should be eager to work with us and to contribute ideas and solutions from their own experience. To achieve these results, U.S. leadership is essential.

* * * * *

Chairman Coble, Ranking Member Nadler and members of the Subcommittee, trade secrets are vital for manufacturers small and large. America's trade secrets laws and policies much keep pace with today's threats. Manufacturers need your help to ensure they can effectively and efficiently protect and enforce their trade secrets.

The NAM applauds your attention to this critical challenge and your interest in solutions. With strong global partnerships and with improvements to U.S. laws, including access to federal civil enforcement, we can have a real impact at home and abroad.

Thank you for the opportunity to testify this afternoon. I look forward to answering any questions you may have.

Mr. COBLE. We have a distinguished panel, and I thank you all for your contribution and being here.

Gentlemen, we try to comply with the 5-minute rule as well, so if you all can be terse in your response, we would be appreciative.

Mr. Burns and Mr. Moore, with the recent elections in India bringing in a new pro-business, pro-reform prime minister, we are hopeful that the IP environment in that country will improve. What steps should the new government take to promote greater protection for trade secrets, Mr. Burns and Mr. Moore?

Mr. BURNS. Well, I think you have—this is an excellent question, Mr. Chairman, and I think you have pointed out one of the very bright spots right now when it comes to the world of intellectual IP diplomacy. I think the first step is going to be engaged in dialogue because it has been for many months that there has not been an effective dialogue between the government of India and the United States on key intellectual property issues. I think we all anticipate that this new administration in India will begin that process again and will allow us to begin to better understand where those key differences are and where there are opportunities to move forward in a mutually advantageous spirit.

Mr. COBLE. I thank you, sir.

Mr. Moore, you want to add to that?

Mr. MOORE. Thank you, Mr. Chairman.

I agree with my colleague. As you may be aware, manufacturers across many different sectors have faced a number of different challenges in the Indian market over the last couple of years, and we are very pleased and encouraged by what we are hearing from India's new government, their commitment to a good business environment, to open trade and investment, agree that beginning that conversation and having that dialogue will be critical as a first step and something that we hope to see early on in the new Indian administration as a way to begin to address some of the challenges and look at opportunities to work together constructively on issues like trade secrets.

Mr. COBLE. I thank you, sir.

Mr. Hertling, what are the limits of relying solely on the criminal provisions of the Economic Espionage Act at the Federal level?

Mr. HERTLING. Well, you can look at the limits in a couple of different ways. First of all, I would reiterate that there is very few, in fact, no area of law that I can think of, in which the sole remedy is limited to criminal enforcement, particularly for IP, the misappropriation or however—whatever the term of art would be used in patents. Of course, it is not misappropriation in that field. Everybody—owners of any form of intellectual property have the ability to enforce their rights through civil litigation as well as, in some instances, you can have criminal prosecution, depending on the nature of the theft or misappropriation if it violates other criminal laws.

So, it is, in part, a question of equivalence here to provide trade secrets the equivalent rights—trade secret owners the equivalent rights of the owners of other forms of intellectual property. It is also, like now, trade secret owners have a civil remedy. It is at State law, and as we are finding, as owners of trade secrets are finding, that remedy in the modern world where much of the theft

is international in nature and doesn't respect national borders, much less State borders, a remedy limited to State law is inefficient and ineffective in many instances.

So, this is not a question of criminal law versus civil law, per se, but it is taking the existing civil remedies and making them more effective and more efficient. Looking purely at the criminal law context, of course, one of the reasons why in other areas of the law we don't rely solely on criminal law as the enforcement mechanism is that law enforcement is busy. The FBI has many priorities, very important ones. They can't respond to every claim to bring their investigative resources to bear. Prosecutors have to make the same kind of call as to what kind of cases they are going to file, and then, finally, I would say the criminal law is very good at punishing acts that have already occurred. But the goal here, particularly in seeking civil remedies, including seizure remedies, is to prevent the information from being used wrongly in the first place by the thief or the company on whose behalf the thief is operating. So the criminal law is fine. It is post hoc punishment, but you want to bar the—you want to close the barn door before the horse gets out, and the civil law is a much more effective remedy in that respect.

Mr. COBLE. Thank you, sir.

Mr. Simon, let me try to get one more question in before the red light turns one. Could you speak more, Mr. Simon, to the unique role that trade secrets play in your business and the issue that cloud and Internet-based companies face when it comes to trade secret protection, specifically when you are contacted by the authorities regarding misappropriated—appropriated data that is put in the, quote, “cloud,” close quote, by a customer?

Mr. SIMON. Thank you. So, you know, from our perspective, there are certain things that are relatively easy to do, such as securing data, denying access to data. There are other things that are very difficult to do, like giving possession to physical media, as I testified earlier. So, from our perspective, what we are really focused on is wanting to make sure that whatever remedy exists, and we understand there may need to be a remedy, and we are not opposed to that, that it take the businesses into account and the security of both our data and our customer's data into account. If I may, I just would like to interject one additional somewhat of a short comment—

Mr. COBLE. Sure.

Mr. SIMON [continuing]. On criminal procedures in trade secret context. So criminal trials, by their very nature, tend to be much more open than civil trials, and having been through on behalf of a former client, and Economic Espionage Act case, one of the difficulties is, once that case goes to trial, a lot of information is going to be available in the public that would not ordinarily be available in a civil trade secret case. So, because of the constitutional issues that are involved, there are also some shortcomings to criminal prosecutions under the EEA.

Mr. COBLE. I thank you, Mr. Simon.

My time has expired.

The gentleman from Michigan, Mr. Conyers.

Mr. Nadler, you would—who? Okay. Mr. Nadler from New York is recognized for his questions.

Mr. NADLER. Thank you. Everyone's testimony supports a creation of a Federal civil cause of action. Does anyone know of anyone who opposes that? We know of no opposition to that proposal.

Mr. HERTLING. Ranking Member Nadler, let me start on behalf of Protect Trade Secrets Coalition. We represent a lot of different industry sectors, and we have also been undertaking, on behalf of the Coalition, outreach to other industry sectors, to public interest organizations, trade associations and the like, and we have not yet encountered anybody who opposes the concept of a Federal civil remedy for the misappropriation of trade secrets.

Mr. NADLER. So it is all the details. Would creation of a Federal civil cause of action lead to increased litigation? Anybody?

Mr. HERTLING. I will take that again. I don't believe so. We—I think, as Mr. Burns testified, companies are already using civil legal proceedings.

Mr. NADLER. You simply move the litigation from civil to—

Mr. HERTLING. I would use the local—

Mr. NADLER. From State to Federal, it might eliminate duplicative of the State—

Mr. HERTLING. And in fact, Mr. Nadler, it might even reduce, at the margins, litigation because you would no longer need to file in multiple States to enforce.

Mr. NADLER. And so, as you say, reduce that.

Mr. Simon has raised some concerns about seizure provisions, ex parte provisions in existing legislative proposals. Does any—do you believe that this is an issue that can be resolved in a manner that strikes an appropriate balance and satisfies all stakeholder interests, and what would be the key elements of such an agreement with respect to ex parte proceedings or seizures? Anyone? Mr. Simon?

Mr. SIMON. Thank you. So, I think it is possible. It—but it requires somewhat different thinking. Like the example I gave of the current rules regarding seizure for physical goods, where you have 14 days before you—up to 14 days before you are going to be in front of the judge. When you are having hundreds of millions of dollars per hour go by that are being lost because a business is down, 14 days is way too long. There are other things that—

Mr. NADLER. Fourteen days for what?

Mr. SIMON. Fourteen days. So under the Federal Rule of Civil Procedure 65, you have up to—the Court can say that it will keep a TRO in place for up to 14 days. From what—before you get a hearing in front of the judge as to whether or not—

Mr. NADLER. That's obviously too long.

Mr. SIMON. Sorry. So that is an example of a concern. It requires thinking on a different timeline, and I understand with an overburdened judiciary, that is difficult.

It is a question of how do you fashion the remedies, what is the right set of remedies, and it is also technically complex because different companies, even different companies in our own industry when we have been talking to several about this, have very different approaches to how they handle customer data and what they

do with the customer data, and as a result, that has to be taken into account

Mr. NADLER. So as we seek to develop legislation, if we were going to do so on a Federal cause of action, the controversies, if any, are going to be on what limitations and so forth we put on seizures?

Mr. SIMON. I think that will probably be one area. There may be some others, but to our company, that is probably the most serious.

Mr. NADLER. Does anyone else want to answer this?

Yes, Mr. Burns.

Mr. BURNS. Yeah, I can certainly elaborate on that, and I am very much in agreement with you. I think when we started having this discussion, all of us were thinking with a Lanham Act headset on, and we know the Lanham Act is really aimed at essentially seizing goods, so you are trying to find the infringing embodiment of a Lacoste shirt, right?

Mr. NADLER. A what?

Mr. BURNS. This is a—a Lacoste shirt, you know, this is a very different environment that we are in. What we are really—our objectives here are really about preserving evidence so that you can have a proceeding on the merits that looks at all the facts and also to prevent further leakage beyond what has already taken place, whether it is in a digital environment or a physical environment.

So I fully agree with you, if there is going to be a seizure provision, it needs to be a very narrowly tailored one, something of last resort that is aimed at that bad faith individual who is about to get on a plane, fly to another country with a PIN drive full of confidential data.

Mr. NADLER. Thank you. Mr. Burns, China is often identified as a problem with regard to theft of U.S. trade secrets. In fact, I saw something I think I read recently that I saw that there was a national holiday in China a few weeks ago and that hacking of American companies went down 40 percent that day. People were entitled to their day off, I suppose. Now, I assume the problems are not limited to China. How has the lack of protection impacted U.S. companies seeking to expand operations globally, and what do you think can be done to encourage other countries to provide more robust protection?

Mr. BURNS. Well, I think you are absolutely correct. This is a global problem that we experience in all the jurisdictions in which we are doing business, and the challenge is to take the kinds of steps that are in our power today to try to improve the situation.

And my sense is that when the United States Government is dealing with foreign trading entities, whether it is China or India or the European Union, if we come to a discussion from a position of strength and can say with a clear conscience that we have done our very best, that we have a strong Federal civil cause of action in place within our own jurisdiction, we are much more likely to be taken seriously by interlocutors from other governments.

Mr. NADLER. Does anyone else want to answer that?

If not, my time is expired, and I yield back. Thank you.

Mr. COBLE. I thank the gentleman.

The distinguished gentleman from North Carolina.

Mr. HOLDING. Thank you, Mr. Chairman.

Is anyone able to quantify the amount of litigation currently going on in State court regarding trade secrets?

That might be a little bit difficult, but the—I am sure our friends in the Federal courts would want to know what type of a wave of litigation is headed to Federal court if we give a Federal cause of action.

Mr. SIMON. So, in California, obviously, particularly in Silicon Valley, many key trade secret cases have been brought over the years, but it is a relatively small percentage of cases in a year, at least from what I have heard. I would say it is in the order of 10's to maybe 100 per year in, you know, in the Bay area, is you know, probably the number I heard in talking to judges. Actual reliable statistics, I am not sure.

Mr. HOLDING. And the creation of a Federal cause of action would not preclude the States from continuing to have State law causes of action for trade secrets, would they? Mr. Burns?

Mr. BURNS. That is exactly right.

Mr. HOLDING. And of course, how would removal work? I mean, just to get into the—I mean, I don't know if anyone has thought through this, but as I sit here and since we have complete agreement that there needs to be a Federal cause of action, I started to think about some of the more nuances of it, so having spent my legal career prior to sitting in Federal court, you know, sometimes, you know, certain parties want their action to be in Federal court.

Defendants, you know, in a plaintiff's action, often want to try to get removal into Federal court, so how would you see that playing out? Would you see plaintiffs going into State courts? Are there any particularly favorable State courts that we would be seeing plaintiffs going to and then removal actions, trying to get those removed to Federal court? Has anyone thought that through?

Mr. Simon.

Mr. SIMON. It has been a long time since I removed a case to Federal court, but I think the one way it may play out is plaintiffs, in seeking to avoid having to deal with the delay of a removal petition, may just go straight to Federal court first, and that is from a timing standpoint since you are generally as a plaintiff seeking emergency relief, you do not want to file in State court and then have you know, start to get your emergency relief and then have somebody remove it to Federal court.

Mr. HOLDING. All right.

Mr. BURNS. If I could just—

Mr. HOLDING. Mr. Burns.

Mr. BURNS [continuing]. Add one point. I also think if there is Federal court jurisdiction in this case, we would tend to see much more local cases being the subject of State court litigation. So, purely intrastate type cases, and in those cases, there is very little—there is probably very little incentive to remove to Federal court because both parties are locally situated and are comfortable probably with dealing with a local State court.

Mr. HOLDING. All right. Well, you know, the variances between discovery, you know, local rules, you have got your State rules and then your Federal rules, and then you have got your local rules of these particular district court, it could get interesting.

The—you know, we have spoken a lot about the challenges that our U.S. companies are facing abroad, so, if anyone wants to talk about extra-territoriality, and you know, how the statute could be composed in such a way to try to protect our companies doing business abroad, you know, and take it through where maybe the instance of the infringer, you know, the violator you know, has no assets here in the United States that we could get to or that question.

Mr. Simon, you want to take a hack at that or Mr. Hertling?

Mr. SIMON. Well, I think there probably is a balance that can be struck there. I certainly don't think we want to go where at one point U.S. antitrust enforcement seem to have gone to which was the extreme being U.S. courts trying to tell Swiss watchmakers what they can do in Switzerland doesn't work too well. There are analogues in the antitrust area that may be worth taking a look at. There is a difficulty, though, if you have somebody who is a bad actor and is completely outside the jurisdiction of the U.S. courts, has no assets that are subject to U.S. courts, that can become very difficult if you have to go to a country that may be hostile to the remedy that you are seeking.

Mr. HOLDING. Mr. Hertling, you want to chime in there.

Mr. HERTLING. Yeah, the other point I would make is I think one of the important values, as a number of us have alluded to, of having a Federal civil cause of action is that it would provide a model for other countries, and I think ultimately the most effective relief for the problem you have identified, is to get other countries to improve the quality of their legal systems and the protections that they can provide in their own courts.

And I think if we can achieve that through the intercession of our trade negotiators and if our trade negotiators have an effective national level remedy in the United States, it will make them more effective at achieving sound national level remedial systems globally.

Mr. HOLDING. Good.

Mr. Chairman, I yield back.

Mr. MARINO [presiding]. Thank you.

Mr. Conyers.

Mr. CONYERS. Thank you very much.

This has been very important, gentlemen. We thank you for your testimony. Is, Mr. Simon, the seizure issue one of the things that when we start putting together a bill, and some of us are going to do that, that we have to be careful of, since there has been so much increasingly new and modern technology coming into the digital era?

Mr. SIMON. Yes. You know, there are a couple of things, and it is you know, I have to admit, you know, because some people have asked me for suggestions, and I am struggling with them right now, quite frankly. Part of it is because you have to deal with many different ways that people do things. Part of it is you also have to try to have as much vision as you can as to what is going to happen 3, 4, 5, 10 years out, and that is not easy, particularly with the speed with which technology is moving.

But, you know, from our perspective, the one thing we don't want to end up having, is to have legislation and 3, 4, 5 years out, it is

we are looking at what we would like to do from a business purpose and we are looking at what the law requires, and there is an inconsistency there that prevents us from changing the way we want to do business.

So, you know, we hope that whatever remedies can be fashioned can be very flexible because that is what we think we need.

Mr. CONYERS. Do I get out of your response that we might make things worse if we don't carefully create a Federal civil law on this subject?

Mr. SIMON. I am not sure you would necessarily make things worse. I think what might happen, though, is that there might be individual business models that otherwise might make a lot of sense, but because of, for example, some remedy that Congress has mandated, is required, the technology just won't work for that purpose.

So, I want to be very careful with what I would say because I think overall getting a Federal legislation would be very helpful, but I also want to say that, you know, we have to try to do the best job we can on the remedies.

Mr. CONYERS. Uh-huh. Thank you.

Mr. Moore, small businesses, I think, are very up against it. In the first instance, under the present circumstances, it is just my suspicion that most of them can't even afford to deal very seriously at this stage with this whole question of secrecy. Now, is there—will we be able to help them when we finally come together on a secrecy law between both ourselves and the Senate? And I understand the Senate has—at least has a bill, and we are going to be working on one.

Mr. MOORE. Thank you very much.

Small businesses really don't have a choice about addressing this challenge. It is there. They need to address that it is something that affects them as well as large companies. I do think that you see the challenge of trade secrets theft affecting smaller businesses more acutely. Certainly for many of those businesses, trade secrets make up a larger share of their intellectual property portfolio than you might find in some larger businesses that might rely more heavily on patents, for example.

You see that small business owners are busy running their businesses and less focused on the threats and some of the challenges that are out there, and of course, for small businesses, the cost of protecting and enforcing their rights may be higher relative to their total revenue than you might find in a larger firm.

Certainly we think that having a Federal civil cause of action for trade secrets theft would be very important to enable them to effectively secure and enforce their rights domestically.

Thank you.

Mr. CONYERS. Uh-huh. Mr. Hertling, it is good to see you again, have you back in your old digs once more.

It seemed like to me that it took us quite awhile to get around to trade secrets, and yet, now that we are around to it, everybody says it is very important that we deal with it. I am amazed that it hadn't come up before as a matter of importance.

Mr. HERTLING. Well, I think it did. I mean, it was brought up in the context of the 1996 Economic Espionage Act, and it was just

brought up relatively late in the process, and so I think that the notion was, at the time, let's do the criminal statute first and then we will get around to it, but then all of a sudden the issue surrounding—that prompted the ultimate enactment of the Digital Millennium Copyright Act took over, and then, from there, the Committee's IP focus turned to patent reform.

So, the issue has been lingering out there, but now we think the time is ripe. We know obviously the Committee is conducting its broad copyright review and those are important issues, and of course, the patent issue, the House passed the patent litigation reform bill last year, and those issues are still out there, but we think that these issues are now ripe for legislation.

And we think, unlike perhaps some of those other issues, as we have heard, while there needs to be great care taken with striking the appropriate balance, this is an area in which there do not appear to be any significant disputes that should derail the adoption of legislation.

Mr. CONYERS. And I am excited about getting this moving, and I really appreciate the bipartisan tone of the discussion that we are entering in around here. That is important as well.

And I thank Chairman Coble and yield back the balance of my time

Mr. COBLE [presiding]. I thank the gentleman.

The distinguished gentleman from California, Mr. Issa is recognized for 5 minutes.

Mr. ISSA. Thank you, Mr. Chairman.

Fourteen years ago when I came here, they called me distinguished, too, but I was younger, and Richard, it is good to see you back.

You know, there are two things that worry me around here. One of them is when a major piece of legislation or initiative is immediately bipartisan, I wonder, well, who is protecting the other side and secondly, whenever we are talking about expanding intellectual property, I think back to a time before I got here when the powers that be decided to retroactively expand patent rights so that some people whose patents were about to expire got extra time, and it was envisioned in the bill, for God only knows what reason, and then, of course, in copyright, we retroactively made "I Got You Babe" last longer along with black and white Mickey Mouse. No comment other than it just happened to be a symbol.

And so as I look at federalizing, if you will, the civil cause of action, I have a couple of questions—more than a couple of questions and because I am one of the non-lawyers here on the Committee, I will put my spectacles on so I will look more lawyerly and I will read just quickly. "To promote the progress of science and useful arts by securing for a limited time to authors and inventors the exclusive right to the respective writings and discoveries."

A trade secret is in fact a discovery; would you-all agree? It is what you know that somebody else doesn't know, Mr. Burns, right? Just yes or no.

Mr. BURNS. I think it—I think in some instances, absolutely. In other instances, it could be something distinct, yeah, but it is not a discovery in the sense that a discovery of—in the technical—

Mr. ISSA. It is what you know that someone else doesn't know.

Mr. BURNS. Absolutely. Yes, sir.

Mr. ISSA. So you know something somebody else doesn't know, and the basic concept of trade secret is, as long as you can keep it a secret, you can keep it in perpetuity and monetize the benefit; is that right? I just want to make sure we define the term here. So—

Mr. BURNS. If I could respond—

Mr. ISSA. Well, these are yes or nos, please. The Chairman is very indulgent, but I have only got a couple of minutes.

Mr. BURNS. Okay. Please.

Mr. ISSA. Yes, these are in fact that. So, the questions as we federalize the civil action are, do I give you the future revenue stream you have lost in perpetuity, do I give you what you would have gotten had you disclosed it under patent rules and gotten anywhere from 19 to 12 years, depending on—or 10 years depending upon the time it takes before it is granted, do I give you the copyright equivalent.

So, as we federalize, the first question is, the loss is a monetized loss, and that is what you are here seeking. How do I fairly make sure that what you deprived everyone from knowing because you knew and they didn't know, and you did not enter it into commerce for mutual benefit only for your own benefit—how do I fairly assess since there is no constitutional mandate?

Trade secrets don't exist under the constitution. The right doesn't exist. This is a statutory giving to people who keep something a secret and have a loss as a result of that entity, that secret being stolen from them. I understand the criminal part. That is settled. How do I come up with the monetary one?

Richard, I would start with you. Put a dollar figure on it, and it has got to be probably more than you made here as a staffer.

Mr. HERTLING. Probably more than that.

Mr. ISSA. And no litigation.

Mr. HERTLING. More than I make in the private sector. I think those are very—that is a very good question, Chairman Issa. I know you are not Chairman of this Committee, but I will still use—

Mr. ISSA. I am a patient man.

Mr. HERTLING. But I think the—and I am not an expert on this, and I said earlier to Mr. Simon, benefit of sitting next to a real lawyer, but I think the question you have raised is one that courts today have to struggle with because, again, these sorts of remedial actions are being brought every day in the State Courts around the country.

Mr. ISSA. Right.

Mr. HERTLING. And so—

Mr. ISSA. And so I guess my question is, before we—as we proceed to looking at a national and hopefully a global policy, is it, in your opinion, critical that we look at what is being done throughout the various States and perhaps foreign countries and we figure out where we are comfortable monetizing the loss of a secret, in other words, the formula for it so that we can issue the kind of guidance to the courts in the way of damages, because I can certainly envision that the future revenue of Coca-Cola lost, if that secret formula is disclosed, can bankrupt almost anybody.

And if I am the recipient of it, maybe harmlessly from the thief but in fact the recipient, I can see my entire wealth run out.

So, my question to all of you is, shouldn't we embark on an analysis, not of do we do it, because harmonizing that which is disparate throughout the States is appropriate for us to consider, but in harmonizing, isn't our most important task to figure out how it is going to be valued, including calculation of length, value, and the societal balance between your rights, if you will, for your secret and the lack of benefit as a result of it not being ever made public otherwise?

And Mr. Chairman, if you would let them answer, I would appreciate it.

Mr. COBLE. Without objection

Mr. SIMON. Thank you.

If I may, Mr. Chairman, if you look at the case law under the Uniform Trade Secret Act, at least the one that comes to mind, there are a couple of things that I think address your concern about a perpetual remedy, if you will.

First of all, injunctive relief is generally—misappropriation of trade secrets is generally given only for the reverse engineering period, whatever that would be deemed to be. Normally, I rarely seen it be longer than a few years. I am not saying there isn't a case that goes longer than that, but it is rarely longer than that a few years.

When you go to the monetary relief, which is actually the way these cases play out, much rarer, because normally the injunction ends the case, when typically the grant—it is like trademark law, 99 percent of the cases settle after preliminary injunction is granted or denied.

Mr. ISSA. I have been before the ITC. I know these things.

Mr. SIMON. Yeah. So the way it works from the damages standpoint, the question is, what are you going to be able to convince the trier of fact, be it judge or jury, you are entitled to either for a reasonable royalty, which is available sometimes, for lost profits or for unjust enrichment. I am not aware of—I mean, there have been some very stiff trade secret awards recently. I think DuPont got one close to a billion dollars not too long ago for some pretty heinous acts, as I understand it.

Mr. ISSA. Outside of here, that is real money.

Mr. SIMON. Yeah. But you know, that is a very exceptional case and involved very egregious acts with, if I recall correctly, actors from outside the United States.

Mr. ISSA. Thank you, Mr. Chairman. I appreciate your indulgence, and I appreciate our—this direction toward harmonizing these trade secrets.

Mr. COBLE. You are indeed welcome.

I believe the distinguished lady from California is next in line, Ms. Lofgren.

Ms. Washington, were you here earlier?

Okay. I stand corrected. The gentlelady from Washington is—

Ms. DELBENE. Thank you.

Thank you, Mr. Chair, and thank you-all for being here today. I think everyone has been advocating for creating a new Federal civil cause of action for trade secret misappropriation, and I appre-

ciate the interstate nature of this issue and believe that there is merit to having a Federal cause of action. I think it is important that we also don't take away any rights from States in this process, too, as we put together legislation.

One of the things that I believe Mr. Holding touched on earlier was the amount of litigation, and I think Mr. Goodlatte also mentioned potential frivolous litigation, and so maybe, Mr. Hertling, I was wondering, you know, what do you think about the issue of increased litigation or frivolous litigation if we had a Federal cause of action, and do you believe that we would see increased litigation as a result?

Mr. HERTLING. Thank you very much, Ms. DelBene.

I don't think that you would see an increase in litigation or an increase specifically in frivolous litigation. Of course, frivolous litigation is always in the eye of the beholder. To the defendant, it is always frivolous, right, but I think here the net result of the creation of a Federal civil remedy would be in appropriate cases, particularly those would have to be at least of an interstate nature, but of an interstate or international nature, you would shift the locus of the litigation from State courts to Federal courts.

The cases are going to be filed anyway. Today, they are being filed in State courts or they are being filed in Federal court under diversity jurisdiction. I don't think you would see a dramatic change in the number of cases or in the quality of cases being brought as a result of the creation of a carefully crafted, well balanced Federal statute.

Ms. DELBENE. Mr. Burns, I think you mentioned that our trade negotiators would be in a better position to use a Federal civil cause of action to show the U.S. is setting a high standard when it comes to trade secret litigation or trade secret protection. Can you talk a bit more about how you think our leadership on this issue would be helpful when it comes to negotiations of trade agreements?

Mr. BURNS. Absolutely. I think there are a number of ongoing negotiations right now, and then also some things we call "bilateral dialogues" that take place with important trading partners.

So, in the context of the Trans-Pacific Partnership, having such a statute on the books in the United States, I believe, puts us in a much stronger position to be advocating a robust trade secret, if not chapter, paragraph within an IP chapter, within a TPP negotiation. I also think that, particularly with respect to the bilateral negotiations that are between the United States and the European Union on what is called the TTIP treaty, this is a very good timing to have this legislation come forward.

As we all know, the European Union has already began the legislative process of a directive that would harmonize trade secret protection within the EU, so the Commission, in November of last year, introduced its proposal. That proposal was adopted by the counsel of the European Union, and then will be forwarded to the new parliament some time in the next couple of months with the likely adoption by the early next year.

The idea of having trade secret language in the TTIP agreement is to in a sense codify an understood best practice, an understood Transatlantic best practice, and bringing the United States into the

realm of best practice when it comes to protecting trade secrets is a very important part of delivering that entire package.

Ms. DELBENE. So I would say we need to figure out what we would be doing in legislation before that would happen.

Mr. BURNS. I would say ideally sooner rather than later. It is always better to come to a negotiation from a position of strength with legislation that is not—that cannot be easily criticized by a trading partner with whom we are trying to enter into a treaty. We would be likely to get other consideration in exchange for that, as part of that negotiation.

Ms. DELBENE. Thank you.

I yield back, Mr. Chair.

Mr. COBLE. I thank the gentlelady.

The gentleman from Florida, Mr. DeSantis.

Mr. DESANTIS. Thank you, Mr. Chairman. Thank you to the witnesses.

Just as I am reading through some of the—I know the Administration put out a report last year about trade secret theft. I mean, is it safe to say that China, in terms of international theft, is overwhelming the biggest culprit?

Mr. SIMON. I don't feel qualified to comment on that. I have no basis for it. I can read the same reports that you do. You know, it—but I do want to point out China is not alone.

Mr. DESANTIS. No, and there is not, but it seems like there were a lot of people who were either investigated or prosecuted for passing information to Chinese universities and companies, and I know India appeared a number of times.

So, when you are in a situation where you have trade secrets stolen from a U.S. company, somebody maybe who is working there, they pass it along to a company overseas, you know, yeah, we prosecute the individual who did it, but what are the potential remedies for the company once the information has actually been passed, and what do you suggest that Congress do to make that more effective?

Sure.

Mr. BURNS. Let me comment on that.

I agree with you. I think that it is really important to recognize this as the global issue that it is.

And by the way, it is also important to recognize that China has a Federal trade secret law that has national application that can be used in China, and we have used it quite, with some success in China.

So, countries around the world are in the process of examining their own sort of trade secret conscience, as it were, and making sure that that they have a system in place that makes it likely that people who have their trade secret stolen from them get a serious opportunity to get to justice.

So, from our perspective, in order to globalize that best practice, again, the most constructive thing that this Committee can do is to go back and look at our own system and take the action that I think, in pretty much unanimity, U.S. industry is asking for, and that is, a Federal civil cause of action that will improve our legislative situation in the U.S. and also just bolster our prestige when

it comes to negotiating better trade secret protection in other countries around the world.

Mr. DESANTIS. Can you describe this move in some countries to compulsory licensing and how that affects the ability of American businesses to operate overseas?

You want to take that?

Mr. BURNS. Compulsory licensing is a measure that is understood under international law, that allows for governments to engage in the transfer of intellectual property rights to another party. It is something that exists in international law. It is provided for in the TRIPs agreement, so that is the reality of international law.

It is not—I think countries that engage in it on a regular basis, it is not like putting the welcome mat out for foreign investment. It is like saying to people, “come invest in our country, oh, and by the way, your property rights are at risk,” but it is something that is legally cognizable under the international treaties that are in place today.

Mr. DESANTIS. Very well. Well, I appreciate it.

And I yield back the balance of my time.

Mr. COBLE. I thank the gentleman.

The distinguished lady from California is recognized.

Ms. LOFGREN. Thank you, Mr. Chairman.

This has been very helpful, and I am wondering, I think I saw Mr. Simon on the flight out, so I especially appreciate that he came all the way from the Bay area to be here today.

And here is a question I have for you or anybody else on the panel. You can't quantify it, but I do think that there is sort of a growing trend, maybe is not quite the right word, in the valley where people are shying away from the patent system.

A lot of engineers feel that it is—that the patent system is actually a drag an innovation, and also it takes so long to get anything patented, and I think, this may not be true, but not every trade secret is patentable but probably everything that is patentable could be a trade secret, and so that leads me to wonder about, as you know, I have a kind of a very skimpy bill on it, a civil action. I think it needs a lot more work, but it was a marker at least. Whether we might be getting into a situation, I don't want to create another patent troll situation. I don't want to create another situation where unenforceable noncompete agreements are gone around through another cause of action that we have created. Do you have thoughts or guidance on those two issues, Mr. Simon?

Mr. SIMON. Sure. Thank you. You know, obviously, as you know, there is a lot of concern, particularly in the software industry about patents.

A couple of things to point out that are different fundamentally from trade secrets, to patents. One is that you with a trade secret, unlike a patent, you don't start out with the premise that it has to take clear and convincing evidence to disprove that the invention is patentable. It is the other way around. The owner of the right has to prove by a preponderance of the evidence generally that you in fact have the trade secret, not always the easiest thing in the world to do.

The second thing is that there are things that are patentable that make very little sense to patent. There are things that are

patentable that make very little sense to keep as a trade secret. Just by way of example, my understanding, the pharmaceutical industry, because of the disclosure requirements of the FDA—

Ms. LOFGREN. Right.

Mr. SIMON. Almost all—

Ms. LOFGREN. Yes.

Mr. SIMON [continuing]. Formulations—

Ms. LOFGREN. I am thinking more in the IT areas.

Mr. SIMON. Yeah. In the IT area, it plays back and forth. There is a lot of stuff we deliberately do not want to patent because we do not want to tell our competitors how to do it and there is no way to figure it out from our products. In other areas, it may make much less sense to take that approach.

The other thing I just want to go back to a point Mr. Conyers raised earlier if I may, very briefly, is that one of the nice things about trade secrets is the protection is much cheaper to acquire—

Ms. LOFGREN. Right.

Mr. SIMON [continuing]. Than a patent, so it is much more readily usable by a small business, and from that standpoint, yeah, I think it is actually a pro-small business perspective, too.

Ms. LOFGREN. I want to—I don't know if anybody else has comments on this point. I don't see anybody leaping forward. I am interested in your comment about China's cause of action and the capacity to gain relief in China. I think that the theft of intellectual property, and most especially trade secrets, is severe in the valley, and China is a major offender, and in many cases, it is quite obvious it is not just an individual person going back to China. It is the Chinese Government that is actually sponsoring this activity.

Have you seen success in Chinese courts when it is the Chinese Government that is actually behind the theft?

Mr. BURNS. I am not aware of any cases of that nature.

Ms. LOFGREN. Okay. I am.

Mr. Moore, do you have any advice on that?

Mr. MOORE. I am not aware of any cases brought in China against the Chinese Government.

Ms. LOFGREN. Right.

Mr. MOORE. But certainly our members report a number of different challenges with protecting their trade secrets in the Chinese market, not least because of how their confidential business information may be treated, both as it is coming into the country but also during a court proceeding.

Ms. LOFGREN. Okay. Well, it is also that there is a lot of theft going on in the valley itself where information is vacuumed out.

I just think that this is an excellent panel. I see that it is just the, what we call the "nerd caucus" left here listening, but I certainly appreciate the information. I look forward to further work on it.

And yield back, Mr. Chairman.

Mr. COBLE. I thank the gentlelady.

The distinguished gentleman from Georgia is recognized.

Mr. COLLINS. Thank you, Mr. Chairman.

Again, it is like I said, these are the ones where you sort of separate those or are willing to sit and listen, and I was listening when I was in over at another meeting to your opening statements and

others, and I think this is something that it may not make the front pages the, you know, I will say “sexiest headlines” and all, but it matters to real Americans, it matters to real jobs, and I think that is an impact that we can’t ignore.

Mr. Hertling, do you have a sense of the loss to the U.S. economic—to U.S. economy caused by this trade secret theft?

Mr. HERTLING. There are a couple of recent estimates that are relatively consistent. Last year, as it has been noted I think in Mr. Moore’s testimony, written testimony, General Alexander, the former head of the National Security Agency, estimated the cost at approximately 250 billion with a “B” dollars per year.

And then earlier this year, an organization called “The Center for Responsible Enterprise and Trade” joined with PWC to publish a report called “Economic Impact of Trade Secret Theft,” in February 2014 in which they estimated somewhere between 1 and 3 percent of GDP is the value of the theft of trade secrets, which puts it at what I would guess to be about \$160 to \$480 billion per year.

Mr. COLLINS. So even Washington, D.C., we are talking real numbers. I mean, this would be Bs that we could lead to Ts in trillions and numbers that most of us when we were in—at least my age in, you know, kindergarten and others, you know, trillion was a number we didn’t even talk about. I mean, billions were those numbers.

So this is real economic hurt to our economy that we have to—

Mr. HERTLING. There are a lot of zeroes on the back of those numbers, and behind each of these zeroes is U.S. investment foregone and U.S. jobs lost.

Mr. COLLINS. Yes. I can see that. Mr. Burns, were you going to say something about that?

Mr. BURNS. Otherwise stated, I believe the CREATE report assesses this as somewhere between 1 to 3 percent of GDP.

Mr. COLLINS. In fact, Mr. Chairman, I ask unanimous consent to enter the Economic Impact of Trade Secret Theft study which was just referenced into the record.

Mr. COBLE. Without objection.

[The information referred to follows:]

Economic Impact of Trade Secret Theft:

A framework for companies to safeguard trade secrets and mitigate potential threats

February 2014

CREATE.org
Center for Responsible Enterprise & Trade



About this report

The Center for Responsible Enterprise And Trade (CREATe.org) has collaborated with PricewaterhouseCoopers LLP (PwC) to assess the economic impact of trade secret theft. Our effort has culminated in a report that focuses on four issues that are critical to understanding trade secret theft and how to improve companies' ability to protect their most valuable information:

- ▶ an estimate of trade secret theft across advanced industrial economies;
- ▶ a threat assessment focusing on what threat actors are most active in targeting trade secrets;
- ▶ an original framework for companies to assess the value of their own trade secrets; and
- ▶ a look forward 10-15 years in the future to consider what forces and drivers may make trade secrets more or less secure.

Governments, companies and individuals all play a role in improving trade secret protection. It is in every company's self-interest to improve trade secret protection and to use their leverage to encourage the companies they work with to do the same. Creating a shared sense of urgency can enable companies to dedicate resources to improve trade secret protection. Historically, such improvements have been viewed as a cost, not an investment. Our expectation is that this report will help companies shift that calculation of cost versus investment, enable companies to have a better understanding of who threatens their trade secrets and to provide new thinking and tools to help companies secure their trade secrets now and in the future.

Pamela Passman
President and CEO - CREATe.org
ppassman@create.org

Sanjay Subramanian
PwC | Principal
sanjay.subramanian@us.pwc.com

George Prokop
PwC | Managing Director
george.w.prokop@us.pwc.com

Table of contents

Introduction	2
Scope, Approach and Limitations	5
Estimate of Trade Secret Theft	7
Analysis of Threat Actors Engaged in Trade Secret Theft	10
A Framework for Individual Companies to Safeguard Trade Secrets and Mitigate Potential Threats	13
How Do Future Expectations of Trade Secret Loss Impact Private Sector Decisions Today?	24
Conclusion	31
Acknowledgments	32
Endnotes	32

Introduction

In the private sector, trade secrets are fundamental building blocks that drive investment, innovation, and economic growth. The development of trade secrets also benefits the public good by enhancing economic security and stability.

For several years, the theft of trade secrets, often through cyber-enabled means, has been an important issue for the United States and other industrial economies. The deleterious impact of trade secret theft in both the private and public sectors all but ensures that this issue will remain a leading international priority requiring joint solutions to mitigate the ongoing threat and foster greater economic security throughout the international community.

The public sector has expressed a clear willingness to drive policy developments, foster international dialogue across governments, create public-private partnerships and prosecute actors responsible for trade secret theft. The private sector has an equally critical role to play in protecting trade secrets. The private sector's entrepreneurial spirit coupled with investor expectations will continue to drive companies to invest in research and development ("R&D") and develop new and innovative technologies. At the same time, companies must also invest in new measures to identify and mitigate their exposure to trade secret theft by fully understanding their own vulnerabilities and the threat actors targeting their enterprise.

Protecting trade secrets is critical for the continued prosperity and economic security of businesses around the world. In recent years, private and public sector organizations—universities, industry associations, think tanks, and government agencies—have studied this issue in depth. This paper addresses the broader economic issues referenced in other studies (e.g., national level estimates of trade secret theft); however, it primarily focuses on a framework for individual companies to:

1. Apply a risk-based approach to identify and prioritize their trade secret assets;
2. Analyze the direct and indirect economic losses attributable to a trade secret theft;
3. Understand the types of threat actors and how they may seek to inflict economic harm, as well as how those actors align with the company's vulnerabilities;
4. Develop new strategies to safeguard investment underpinning future trade secrets and mitigate the potential economic losses attributable to trade secret theft; and
5. Develop return on investment guidelines for implementing measures to improve trade secret protection internally and in the supply chain.

"The effects of [IP] theft are twofold. The first is the tremendous loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses. American companies of all sizes are victimized. The second and even more pernicious effect is that illegal theft of intellectual property is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone. Unless current trends are reversed, there is a risk of stifling innovation, with adverse consequences for both developed and still developing countries."

– The Report of the Commission on the Theft of American Intellectual Property, 2013

The observations surrounding the assessment of the economic impact of trade secret theft and the accompanying company-level framework are grounded in an analysis of authoritative literature, our collective experience analyzing the economic impact of illicit activities, extensive open source research, our understanding of leading corporate governance and compliance protocols, and feedback garnered from workshops with leading private sector organizations. Our observations from these efforts include:

1. Estimates of trade secret theft range from one to three percent of the Gross Domestic Product ("GDP") of the United States and other advanced industrial economies.

Although numerous studies have attempted to analyze the losses attributable to trade secret theft, they have had mixed results, primarily due to concerns about the adequacy, completeness and reliability of private sector information. Beyond concerns about data, the analytic approaches of leading studies vary widely, resulting in disparate estimates of losses. Moreover, concerns about the potential adverse impact to a company's reputation in the market and ongoing relationships with customers limit the type of information companies are willing to disclose – either to industry partners or governments – about trade secret theft or internal vulnerabilities. Notwithstanding the challenges of developing national level estimates of trade secret theft, our analysis leverages multiple studies on illicit economic activity across the United States and advanced industrial nations as a proxy for the theft of trade secrets, resulting in an estimate of 1 to 3 percent of U.S. GDP.

2. The national level estimate of trade secret theft is important as a guide to policy creation, industry awareness and advocacy, but is less relevant to individual companies.

At the company level, firms can gain tangible benefits from understanding the relative value of their trade secrets. Analyzing the portfolio of trade secrets that a company keeps and understanding the potential direct and indirect costs (e.g., lost revenue, disruption of business, tarnished reputation) that their theft would inflict is a critical step in a broader company process of prioritizing limited resources to protect trade secrets. In doing so, a company can develop viable estimates on the return on investment it would get from improving trade secret protection, as the probability and severity of a potential breach can be factored into these calculations.

"A consensus among economists has emerged that trade secrets play an important role in protecting the returns to innovation and that trade secret protection is an integral and important part of the overall system of protection available to EU firms to protect their intangible assets, like patents and copyrights."

– European Commission Study on Trade Secrets and Confidential Business Information in the Internal Market, April 2013

Introduction

3. A company-level approach to estimating losses attributable to trade secret theft will drive more reliable national level results, but companies can do more than serve as the subjects of anecdotes.

In many instances, companies are referenced in anecdotes about trade secret theft, but refrain from proactive contributions to a broader public dialogue on this issue due to aforementioned concerns about adverse press, stakeholder relationships, market considerations, and/or regulatory exposure. Reticence may also exist because most companies do not yet have standard procedures to consistently or systematically identify or prioritize their trade secret portfolio, let alone consistent means to assess the economic impact of the loss of trade secrets. Better informed dialogue among the private sector, coupled with a framework for considering these complex issues at the company level, may yield substantial long-term benefits to both public and private sector stakeholders.

4. Increasing company-level awareness of the internal and external threat environment facilitates enhanced protection of trade secrets, an improvement in the quality of the national level estimate of trade secret theft over time, and the potential for a long-term reduction in losses.

Threat actors come in many forms. Malicious insiders, competitors, nation states, hacktivists and transnational organized crime are only a few examples. Gaining an understanding about who those actors are, their motivations and typologies, and their target selection process can enhance the private sector's understanding of how these actors may seek to exploit a company's vulnerabilities. Similarly, understanding the means by which they go about stealing trade secrets can highlight internal vulnerabilities that companies can prioritize for fixing. For example, while the current focus may be on cyber-enabled means of stealing trade secrets, many threat actors still rely on physical means such as recruitment of insiders and placement of agents within companies for purposes of stealing critical data. Keeping current on trends related to threat actors and their methods helps companies take meaningful steps to better safeguard their assets and mitigate such threats.

5. Modeling future scenarios highlights the drivers influencing trends in trade secret theft and provides insights that enable companies to create long-term strategies to protect trade secrets.

By looking forward and considering how threats against trade secrets and other forms of intellectual property may evolve over the next 10-15 years, companies can increase their awareness of how these drivers and factors, if not properly aligned, could make it harder to protect trade secrets. These scenarios can enable companies to visualize and plan for a more secure future for their trade secrets and, at the same time, enhance their ability to make investment decisions today.

6. Management will be better able to formulate and implement new strategies to safeguard investments and mitigate threat if armed with a greater understanding of current and future trends, threat actors seeking to engage in illicit activity, companies' own trade secret portfolios and organizational vulnerabilities.

To maintain competitive advantage in the global marketplace, companies will continue to make significant investments to develop new products and services, the protection of which will be critical. Coupled with the consistent threat of a trade secret theft event and the deleterious impact it can have, management can justify the need to increase company, supply chain and business partner awareness of the threats and trends, and implement protective measures to safeguard these valuable investments. These protective measures can include improved IP protection management systems and improved technology.

Scope, Approach and Limitations

CREATe.org and PwC collaborated to (i) analyze the economic impact of trade secret theft in advanced industrial economies, and (ii) develop a company-level framework to aid the private sector in its efforts to address this important issue. This study furthers CREATe.org's mission as a non-profit organization dedicated to helping companies and their suppliers and business partners reduce counterfeiting, piracy, trade secret theft and corruption.

Definition: Trade Secret

For the purposes of this report, we use the definition of a "trade secret" set forth in the U.S. Economic Espionage Act ("EEA"). It is similar to the definition of trade secrets under the Uniform Trade Secrets Act that has been enacted by 47 U.S. states and several U.S. territories, consistent with Article 39 of the World Trade Organization's Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) and Article 2 of the Japanese Unfair Competition Prevention Act. Under the EEA, trade secrets are:

...all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, analyses, 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 it - (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public...²

Approach

This study is based in part on CREATe.org's efforts in the market to heighten trade secret awareness, increase and improve collaboration amongst companies and between the private and public sectors, and assist companies in fostering a better understanding of the tools companies have at their disposal to categorize, document, and protect their trade secrets through improved management systems and utilization of technology.

Our approach reflects the significant and growing body of literature on the topic of trade secret theft. It estimates the losses attributable to trade secret theft across advanced industrial economies using a proxy approach that measures other forms of illicit economic activity. However, recognizing that this approach only serves as an estimate, we collectively developed a framework to assess the economic impact of a trade secret theft event at a company level by applying more traditional economic analyses and techniques. The framework relies on dual methodologies including: (a) a direct method to estimate the lost future revenue and profitability associated with the theft of a trade secret, and (b) an indirect method evaluating the more intangible adverse impacts of such an event, as measured through various non-financial performance indicators. Our approach incorporates inputs on threat actors, probability and severity of incidents, organizational protections and vulnerabilities, and future trends analysis that companies should consider. These inputs drive the economic impact of a trade secret theft event and are important elements that companies should factor into their assessment of how to protect their trade secrets. In this context, the study may be viewed as a guide for individual companies, and as a path forward to a future national level estimate.

The study is broken into the following phases:

Scope, Approach and Limitations

1. An estimate of trade secret theft across advanced industrial economies;
2. An analysis of the threat actors who are actively engaged in trade secret theft;
3. A framework enabling companies to conduct their own internal evaluations and inventories of existing trade secrets, assess their vulnerabilities to loss, estimate the economic impact of a trade secret theft event, and provide new insights on how to protect these assets; and
4. An outlook for the future of trade secret theft using the results of a futures modeling exercise—drawing from workshops with private sector participants—that present scenarios for future developments and concerns.

Taken together, these sections represent a broad approach to evaluating the aggregate impact of trade secret theft by starting at the company level, and giving companies the tools needed to effectively manage and protect their trade secrets. This practical approach recognizes that fostering greater activity and awareness of this issue among individual companies may produce significant advancements on this challenge.

Limitations

The framework is an approach we collectively developed based on our experience and interaction with numerous companies and organizations facing trade secret theft. It is meant to serve as a guide for companies to document and analyze their trade secrets so they may apply their resources in a cost effective and efficient manner. Application of the framework will not necessarily prevent a trade secret theft event, but may enable companies to better identify and mitigate threats as they arise due to greater understanding of the threat landscape and their internal vulnerabilities, and to be more strategic in allocating resources to protect their trade secrets.

Our outlook section in which we discuss the results of our futures modeling exercise addresses how trade secret theft issues may play out globally, not only in the U.S. The scenarios should not be read as predictions, but rather as a survey of how trends could evolve under certain future conditions. They were created using four drivers in different combinations. These drivers are only four among many that will likely play a critical role in trade secret protection in the years ahead.

Our approach reflects the significant and growing body of literature on the topic of trade secret theft.

Estimate of Trade Secret Theft

Estimating the value of trade secrets at a national or global level presents significant challenges. In this section we will address these challenges and present an approach to estimating the economic impact of trade secret theft.

Obstacles to Estimating Trade Secret Value

Trade secrets, intellectual property (“IP”), and other intangible assets represent a large and growing share of U.S. and global economic activity. The growing number of patents issued by the U.S. Patent and Trademark Office illustrates the essential role intangible assets play in supporting a dynamic global economy. From 1990 to 2010, the pace of innovation in the private sector spurred the growth of intellectual property and the number of patents issued in the U.S. increased by 40.6 percent, jumping from 99,200 patents issued in 1990 to 244,300 in 2010. Notwithstanding the central and powerful role that IP plays in the global economy, there is no consensus on the exact value of trade secrets or how to estimate such a figure.

Numerous academic, industry, non-profit and government reports highlight the challenges in estimating the overall value of trade secrets and the economic impact of those that are stolen. For example, a May 2013 study by the Commission on the Theft of American Intellectual Property (“Commission”)—an independent and bipartisan group chaired by Admiral Dennis Blair and Ambassador Jon Huntsman—assessed various dimensions of international IP theft and its impact on American businesses. The Commission concluded that the exact value of IP theft was “unknowable,” but added that existing assessments of loss have underestimated the impact of IP and trade secret theft. The Commission offered three explanations for why trade secret value was so difficult to measure:

1. Loss is measured in different ways in different sectors;
2. Companies do not often report their losses and are not incentivized to do so out of fear of impact on stock prices and marketplace reputation; and

3. Surveys are often used to measure loss and they are not sufficiently dependable to offer details on such a vast problem.³

In another example, a 2010 Government Accountability Office (“GAO”) study analyzed the economic effects of counterfeit and pirated goods and found that “it was not feasible to develop our own estimates [of the total value of counterfeit or pirated goods] or attempt to quantify the economic impact of counterfeiting and piracy on the U.S. economy.”⁴ Noting the lack of data as a primary challenge to quantifying the economic impacts of counterfeiting intellectual property and goods, the GAO concluded that “neither governments nor industry were able to provide solid assessments of their respective situations” suggesting the need for individual companies to evaluate the worth of their own trade secrets.⁵

After reviewing these and other studies, as well as conducting an independent analysis of trade secret theft, we noted additional considerations that impede estimation of the value of trade secrets:

- The volume of data required to construct an accurate assessment that withstands scrutiny is significant, and would face substantial legal and analytic challenges;
- Some companies are simply unaware that their trade secrets have been stolen, while other companies are reluctant to report such losses to third parties due to concerns about reputational or financial repercussions; and
- Such an assessment would by its nature be somewhat fleeting. As soon as such a figure was agreed to, the value of the trade secrets at the heart of the analysis would have already begun to shift across individual companies or industry sectors.

Purpose of Utilizing Proxies to Estimate Trade Secret Theft

Given the inherent methodological challenges of estimating the value of trade secrets at a national or global level, a proxy approach to estimating the value

Estimate of Trade Secret Theft

of trade secrets can be useful and provides interesting insights. Seemingly unrelated activities—such as research and development spending, occupational fraud, and tax evasion—share important traits with trade secrets, and provide insightful context that enables reasonable estimation of the economic impact of trade secret theft.

Proxy for the Value of Trade Secret Theft: Research and Development

A core proxy for the value of trade secrets involves private sector expenditures on R&D. There are numerous valuable trade secrets that are not related to R&D (such as customer lists, sales data, marketing information, etc.) but R&D represents investment in new ideas, methods, tools and techniques—each of which are critical elements of many trade secrets. Since the early 1980s, R&D expenditures in the United States have exceeded 2.5 percent of GDP; U.S. Government figures report the figure as \$414 billion or 2.7 percent of GDP in 2011.⁸

Global R&D investment trends are similar to U.S. trends. Battelle and *Research & Development Magazine's* 2014 "Global R&D Funding Forecast" examine global R&D for the top 40 world economies (ranked by nominal GDP) and levels of actual and projected spending. As illustrated in Figure 1, they conclude that R&D for the top 40 national GDPs averaged nearly 2 percent in the last three years and are forecast to maintain this level in 2014. Over the last three years, R&D as a percentage of global GDP has also remained steady at 1.8 percent.⁹

Current R&D spending, of course, generates other forms of trade secrets, and represents only a fraction of the economic value generated by R&D. Researchers have estimated that \$1.00 of spending on R&D produces about \$2.90 in other economic activity during the same year and between \$16.00 and \$69.00 over the next 10 years.¹⁰⁻¹¹ On this basis, the value of trade secrets in the marketplace represents a significantly greater component of GDP than illustrated by R&D spending alone.

Proxy for the Estimate of Trade Secret Theft: Illicit Economic Activity

Proxies involving illicit economic activity also clarify the potential impact of trade secrets theft. Such measures capture economic behavior that may inflict harm on the global economy and, like trade secret theft, are under-

Figure 1: R&D as a percentage of GDP

	2011	2012	2013	2014
U.S.	2.7%	2.8%	2.8%	2.8%
China	1.5%	1.8%	1.9%	2.0%
Japan	3.5%	3.4%	3.4%	3.4%
South Africa	1.0%	1.0%	1.0%	1.0%
Germany	2.9%	2.8%	2.8%	2.9%
Australia	2.3%	2.3%	2.3%	2.3%
UK	1.8%	1.8%	1.8%	1.8%
Russia	1.5%	1.5%	1.5%	1.5%
Qatar	2.8%	2.8%	2.8%	2.7%
Brazil	1.2%	1.3%	1.3%	1.3%
Average (Top 40)**	2.0%	2.0%	2.0%	2.0%
Rest of World	0.4%	0.4%	0.4%	0.4%
Global Average	1.8%	1.8%	1.8%	1.8%

*2014 figures are projected

**Top 40 world economies by GDP

Source: 2013 & 2014 Global R&D Funding Forecast, Battelle and R&D Magazine
Sub-Sources: IWI, World Bank, CIA World Fact Book

reported and difficult to measure. Also, in a manner similar to their approach to trade secrets, certain threat actors will target these areas for a variety of economic (e.g., market share, profitability) and non-economic (e.g., increase influence, advance social causes) reasons:

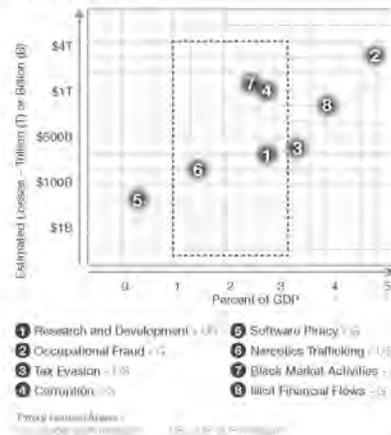
- **Occupational Fraud:** Companies worldwide lose as much as \$3.5 trillion, or 5 percent of global GDP due to occupational fraud and abuse, according to a 2012 report based on the analysis of nearly 1,400 fraud cases by the Association of Certified Fraud Examiners ("ACFE").¹² Facing a similar set of threat actors as trade secret theft—namely malicious insiders with unparalleled access to systems, these perpetrators make measuring fraud and abuse difficult.
- **U.S. Tax Evasion:** In a 2013 study the U.S. Internal Revenue Service ("IRS") estimates the tax gap—the difference between what taxes are owed and what taxes are collected—to be approximately \$450 billion, or 3.25 percent of U.S. GDP. The IRS assesses that the tax gap is a result of nonfiling, underreporting and underpayment—and that it can be challenging to determine what activity is illegal.¹³

- **Corruption:** Another significant issue that often defies exact accounting is global corruption, defined traditionally as the abuse of public office for private gain. Like trade secret theft, corruption poses a unique threat to both the public and private sector by eroding confidence in the rule of law as well as undermining competition. A study sponsored by the World Bank estimates the annual cost of such activities as some \$1 trillion, or 2.9 percent of global GDP in 2005.¹⁴
- **Copyright Infringement and Software Piracy:** Copyright theft, copyright infringement and software piracy are widely recognized challenges for advanced industrial economies. A 2012 Business Software Alliance (“BSA”) report noted, for example, that some 42 percent of global personal computer users employ pirated software, reaching a commercial value of \$64.3 billion in 2011, or 0.1 percent of global GDP. A diverse group of threat actors targeting trade secrets may also be interested in pirating software. Criminal groups are known to pirate software strictly for profit, while hacktivists may attempt to damage the reputation of software companies by creating pirated software that damages systems and users, resulting in negative publicity for the software’s true originators.¹⁵
- **Narcotics Trafficking:** Like the theft of trade secrets, the trafficking of narcotics inflicts a variety of economic costs, including workers’ lost productivity, medical treatment, and the administration of justice. In a 2011 study of the impact of illicit drug use in the United States, the U.S. Department of Justice estimated the cost in 2007 to be as high as \$193 billion, or about 1.4 percent of U.S. GDP in 2007.¹⁶
- **Black Market Activities:** At the global level, the value of black-market activities is estimated at \$1.8 trillion – approximately 2.5 percent of global GDP – according to information compiled on the crowd-sourced database Havocscope. This estimate includes a diverse range of activities that are challenging to quantify: counterfeiting of products like aircraft parts, food, weapons, cosmetics, watches, and clothing; trade in endangered wildlife; art theft; illegal gambling; bootlegging of tobacco and alcohol; and human trafficking.¹⁷

- **Illicit Financial Flows:** The illegal movement of money from developing countries to financial institutions in developed states is, in some ways, a mirror image of the theft of trade secrets, which typically involves the illicit transfer of sensitive information in the opposite direction. In a 2013 study of 55 developing countries funded by the Ford Foundation, economists’ estimated that illicit financial outflows—most in the form of mis-invoicing of trade—amounted to \$947 billion in 2011, some 3.7 percent of these countries’ combined GDP.¹⁸

Taken together, these proxy measures provide context for trade secret theft as yet another form of illicit economic activity and corroborate its significant impact on national economies. As illustrated in Figure 2, most of these measures are clustered between 1 and 3 percent of GDP. While it is difficult to accurately measure economic losses attributable to trade secret theft at a national or industry level, this proxy approach provides a reasonable estimate of the economic impact of trade secret theft given the similarities between trade secret theft and other forms of illicit activity.

Figure 2: Proxies for Estimate of Trade Secret Theft



Analysis of Threat Actors Engaged in Trade Secret Theft

Numerous actors—foreign intelligence services, competitors, transnational criminal organizations, hacktivists and malicious insiders—target and steal companies' trade secrets for various reasons. Social engineering schemes such as tailored spear-phishing campaigns that implant malware to steal trade secrets, or duping employees into revealing sensitive corporate information, exemplify the means by which these actors engage in trade secret theft. Constantly evolving technologies in smart phones, laptops, and tablets that employees use for work provide additional means for threat actors to access a company's secrets. Threat actors' motivations are equally diverse. Some seek personal financial gain, while others hope to advance national interests or political and social causes.

Many threat actors are known to target and steal trade secrets. The threat actors profiled in this section were selected using a risk-based methodology that considered several factors:

- ▶ A well-documented track record of attacking multinational companies;
- ▶ Intent to misappropriate companies' trade secrets and critical data;
- ▶ The capability, as demonstrated by past attacks and by U.S. and other government reporting, to target companies' trade secrets for their own profit or to advance another country's interests;
- ▶ Intent to attack companies and institutions that are rich in trade secrets and other valuable corporate data;
- ▶ Consistent focus on specific industries and sectors—information and communications technology, aerospace & defense, marine systems, clean technologies, advanced materials and manufacturing, healthcare and pharmaceuticals, agricultural technology, energy and natural resources—consistent with the 2011 Economic Espionage Report;¹⁰ and
- ▶ Demonstrated impact on companies due to the theft of trade secrets.

The more effectively that companies can understand these actors and their respective typologies, the better equipped they will be to manage their trade secret portfolios and apply appropriate protection measures that are calibrated to the economic value of specific trade secrets, the type of actor and the type of threat. Companies able to understand who may seek to steal their trade secrets are better able to view those secrets through the lens of a threat actor, and therefore apply appropriate resources to enhance their security.

Nation States

Nation states have unmatched resources and capabilities for stealing trade secrets, and usually want to acquire foreign trade secrets to strengthen their existing military capabilities and bolster national champion companies in the global marketplace.²⁰ Many foreign intelligence and security services attempt to acquire trade secrets and sensitive economic information on behalf of their governments, commonly using covert means. Nation states may also use other national agencies, regulatory powers, or state-supported organizations. Some even publicly claim this is part of their missions. For example, the decree establishing Russia's Foreign Intelligence Service assigns it responsibility for "protecting the country's economic development and scientific progress."²¹ Other examples of nation state actors trying to collect trade secrets from companies include:

- ▶ The head of a German satellite company told U.S. diplomats in 2009 that France represented a greater danger to his country's IP than any other country.²²
- ▶ In 2011, a former employee of a major American chemical company pled guilty to committing economic espionage that benefitted elements of the Chinese government.²³
- ▶ South Korean intelligence officers have been found trying to obtain economic secrets from Australian officials in 2013, according to multiple reports.²⁴

¹⁰ | Economic Impact of Trade Secret Theft

Malicious Insiders

Current and former employees, third parties acting as consultants or lawyers, and suppliers often have unique access to corporate trade secrets and other information that, if released, could inflict significant harm on a company. Respondents to PwC's 2013 U.S. State of Cybercrime Survey identified current and former employees as one of the greatest cyber security threats they faced.²⁵ Insiders' knowledge of companies' systems, where and how information is stored, and specific details on the production or use of trade secrets makes insiders a uniquely dangerous threat. The threat from malicious insiders is all the greater because insiders often cooperate with other threat actors who can provide money, other resources, or ideological motivation. Examples of the cost insiders inflict on companies with high value trade secrets include:

- In 2012, a former employee of a North American automotive company and the employee's spouse were found guilty of stealing trade secrets related to hybrid vehicle technology worth \$40 million. The couple intended to sell the information to a Chinese competitor.²⁶
- An employee of a large U.S. futures exchange company pleaded guilty in late 2012 to stealing more than 10,000 files containing source code for a proprietary electronic trading platform. Prosecutors estimated the value of these trade secrets between \$50 and \$100 million. The employee said he and two business partners had planned to use this source code to develop their own company.²⁷
- In 2011, a former employee of an automotive company was sentenced to 70 months in prison for copying some 4,000 documents on the design of engine-transmission and electric power supply systems. The employee intended to take these documents to a new job with the China branch of another North American company.²⁸

"Ultimately, cybercrime is not strictly speaking a technology problem. It is a strategy problem, a human problem and a process problem."

– PwC Global Economic Crime Survey, 2014

Cultural and technological factors may heighten the insider threat in coming years. A study noted that the nature of U.S. employees' loyalty to their employers is changing because of the much higher rate of lifetime job changes in the 21st century, as compared to the mid-20th century. At the same time, growing numbers of people with highly sought-after technical skills often cross international borders for work, which means more employees with potentially competing sources of loyalty. Additionally, the growing prevalence of "bring your own device" policies and the ease and speed with which employees can move data across multiple programs and applications hampers security and monitoring efforts. These factors could increase the population of malicious insiders with increased access and a diminished sense of obligation to their employer – factors that may increase the risk that they will use their status to expose trade secrets and other sensitive corporate data.²⁹

Competitors

Competitors can target companies' trade secrets independently or with assistance from national governments; cases involving competitors stealing trade secrets represent a large portion of U.S. Department of Justice trade secret theft cases. From these cases we see that competitors can use several methods, including recruiting employees of the targeted company who are disgruntled or have personal ties to the competitor's home country to steal trade secrets or sensitive corporate data. Other methods include bribery, extortion, or the promise of a new job.

Even when acting independently of national governments, corporate competitors often have the resources to exercise state-like power. The repeated use of insiders and corporate spies to access critical and sensitive data is illustrated by recent trade secret theft cases involving competitors:

- ▶ A sting set up by U.S. law enforcement uncovered attempts to bribe an undercover agent posing as a corrupt lab technician of a major U.S. pharmaceutical company that had recently spent millions to develop formulas for a new drug. The indictment noted that the successful theft of the formula could have resulted in billions of dollars of losses for the company.³²
- ▶ In a case involving Asian and North American chemicals companies, the Asian firm is alleged to have hired current and former employees of the North American company as consultants in order to have them reveal confidential and proprietary information. This enabled the Asian company to replicate a proprietary manufacturing process and earn at least \$225 million in proceeds from the theft of the trade secrets.³³

Transnational Organized Crime ("TOC")

Transnational Organized Crime groups have successfully attacked numerous corporate information technology networks to access payment systems and steal personally identifiable information, personal health information, and payment card information, inflicting massive financial damage on their targets.³⁴ As TOC groups expand their activities beyond long-standing

activities such as gambling or racketeering, many well-established groups are increasingly leveraging the Internet for all manner of cybercrimes.³⁵ In this role they are serving as facilitators that enable other threat actors, such as unscrupulous competitors or intelligence services, as they attempt to steal trade secrets.³⁴

A computer security company recently noted the emergence of "cybercrime-as-a-service,"³⁶ and TOC groups often work with other established cyber criminals, purchasing information they have stolen via electronic means for the purposes of furthering their own traditional organized crime agendas.³⁵ In 2013, the Director of National Intelligence warned that cybercriminals could "enable access to critical infrastructure systems or get into the hands of state and non-state actors." This dimension of cybercrime is increasing the availability of hacking tools that can be used to steal trade secrets, potentially allowing threat actors to easily rent or buy sensitive corporate or other information.³⁷

Hacktivists

Hacktivists seek to expose sensitive corporate information—potentially including trade secrets—to advance political or social ends. These groups have used cyber intrusion skills and data gleaned from disgruntled insiders to obtain and publish Personally Identifiable Information (PII) and sensitive business information of key executives, employees, and business partners. As with TOC groups, hacktivists have the technical knowledge and capabilities to steal trade secrets, and they could partner with other threat actors for ideological or financial reasons.

Greater awareness of the threat actors attempting to steal trade secrets, their capabilities, and typologies can position company management to understand their vulnerabilities to theft by these actors and to formulate and implement strategies to mitigate these threats. The following section incorporates this understanding and lays out a scalable framework that companies can use to (i) assess the company-level economic impact attributable to trade secrets theft, and (ii) enhance their ability to safeguard investments and mitigate future losses.

A Framework for Individual Companies to Safeguard Trade Secrets and Mitigate Potential Threats ►

The growing threat of trade secret theft and the adverse economic implications it creates for the private sector require companies to be increasingly proactive in managing this threat to achieve their strategic, operational and financial goals.

In response, CREATE.org and PwC developed a multi-level framework for private sector organizations to analyze their trade secret portfolios. The framework provides a platform to identify and categorize trade secrets leading to an analysis that yields insights into threat actors seeking to induce economic harm, vulnerabilities in companies' existing control structure and a model to assess losses attributable to the theft of a trade secret. Collectively, this framework provides companies with a means to identify potential gaps or exposures in their trade secret protection strategies and ideas to further their ability to safeguard their investment and mitigate future losses. It also provides critical information that enables companies to better understand the return on investment of improved trade secret protection and how to strategically allocate resources. An illustration of the framework is presented in Figure 3.

This section of the paper describes the activities and key points for management's consideration for each level of the framework. As a reference to illustrate the framework's application, each level provides further explanatory guidance on how *ABC Widgets, Inc.* ("ABC") proceeds through the framework. *In our example, ABC is a large, global, publicly-traded, U.S.-based alternative energy company, with a widely-dispersed third-party supply chain and aggressive plans to expand into new markets.*

In our scenario, ABC's executives and board members are becoming increasingly aware of advanced threats to its intellectual property and, in particular, its trade secrets based on recent media reports about attacks against ABC's competitors. At a quarterly board meeting, ABC's directors question management about its plans to mitigate such threats. Reluctantly, ABC's management acknowledges that they have not yet thoroughly identified its portfolio of trade secrets, nor implemented a trade secret protection management system, and will quickly endeavor to analyze these issues with the goal to seek opportunities to strengthen the company's ability to mitigate such threats.

Figure 3: A framework for assessing the business impact of trade secret loss



Level 1: Identify Trade Secrets

Our collective experiences indicate that many companies fail to effectively manage their trade secret portfolios for multiple reasons, including a lack of consensus on what assets actually constitute the portfolio. Some companies' reticence may also stem from their interpretation of "reasonable measures [are] taken to protect [trade secrets] the information"²⁸—mistakenly deducing that any specific documentation of trade secrets potentially creates exposure for the company in the event of a breach. Reasons for this could include concerns about incomplete documentation, lack of follow through, or other such errors or inconsistent practices, but the net result is the fear that courts will find the company has not met the reasonable measures standard. Such companies may prefer taking a general, blanket approach to security and confidentiality that could apply to any information the company may later identify as a trade secret. Our view is that individual companies must weigh the benefits of this thorough approach against the risks, costs, and the company's ability to abide by the basic tenets of the framework, while also considering the risks inherent in not closely protecting the company's most sensitive trade secrets.

This first level of the framework takes the organization through the basic, yet critical step of identifying and categorizing its trade secrets. To best protect those trade secrets whose theft would cause the most harm, companies should first document, locate and inventory their trade secrets. This first step gathers key stakeholders—senior executives, business unit leaders, corporate functional leaders—to inventory the trade secrets maintained by the company. Ultimately, forming a cross-functional team with senior management support is critical to this step and those that follow. Discussion and debate of what constitutes a trade secret for the company is encouraged, as stakeholders should emerge from Level 1 with a broad consensus of not only the definition of a trade secret for their company, but also a list of the company's trade secrets aggregated into categories such as those summarized in Figure 4.

In response to the Board of Directors' queries, ABC embarks on a process to identify its trade secrets. ABC's Compliance Counsel is designated by ABC's Executive Leadership Team to lead the effort. Having recently attended a conference on intellectual property matters, she too started to become aware of the emerging threats to ABC's trade secrets.

Figure 4: Trade Secret Categories

Category of Trade Secrets	Examples
Product Information	New hardware designs; adaptations/updates of existing products
Research & Development	Long-term R&D; basic or applied research; geology R&D
Critical & Unique Business Processes	Inventory/distribution; manufacturing processes; business model based on application of processes
Sensitive Business Information	M&A prospects/plans; market research/studies; customer list/information; information on key suppliers/business partners; expansion plans; corporate strategy
IT Systems and Applications	Novel application of IT that could create new markets; system architecture designs; source code; algorithms

She researches applicable laws, regulations and standards governing trade secrets. She also studies ABC's existing policies and determines that ABC does not maintain a central repository or conduct standardized procedures to manage their portfolio of trade secrets. Recognizing that much work needs to be done, she initiates a working session with a cross-functional team of ABC's senior executives, business unit leaders and corporate functional leaders to inventory the company's existing trade secrets across the categories highlighted in Figure 4.

Before the working session, ABC's Compliance Counsel distributes a working definition of a trade secret and encourages participants to engage in a lively debate. Participants arrive at the working session with their lists, which they present, discuss, and compile into a master list that aligns with ABC's views about what constitutes a trade secret. The meeting results in a categorized list of valuable trade secrets reflecting critical elements of ABC's business model.

Following the working session, the Chief Information Security Officer ("CISO") tasks staff to leverage technology solutions to search across the organization for the assets identified during the working session. Using tools that search based on keywords and other identifiers, trade secrets from the master list are found on various servers, in files with non-relevant file names, and on shared-file sites created for reasons unrelated to the trade secret itself. The results for the location of each trade secret found are noted on the master list, to be incorporated later into the vulnerability assessment. The CISO will also work with other business leaders to find trade secrets—which could exist off the network, in hand-written notes, prototypes, etc.—to ensure that as many trade secrets as possible are located regardless of their presence on IT systems.

By completing Level 1, companies have an agreed-upon list of a company's critical trade secrets—a critical first step in this framework. Many of the trade secrets are also located across the organization, which will contribute to understanding how vulnerable they are to theft. However, as organizations continue to design new technologies or engage in new ventures, they will continue to develop and/or acquire new trade secrets. Therefore, management must establish procedures to continuously refresh this inventory on a periodic basis to facilitate its completeness.

Level 2: Threat Actor and Vulnerability Assessment

A risk assessment focused on threats and vulnerabilities forms a critical step in the framework. As noted earlier, threat actors take many different forms, each of which poses a significant threat to a company's intellectual property. Analysis of existing trade secret protection management systems—the compliance and security program policies, procedures and internal controls—enable management to identify vulnerabilities in its current protocols that may create unnecessary risk and exposure for the company. Evaluating the maturity of the overall trade secret protection program and the specific processes is an effective way to understand the vulnerabilities.

2.1: Threat Actor Assessment

Operating in today's global marketplace exposes companies to unique and varied threat actors. As such, management must understand the scope of the company's operating environment (e.g., office locations, sales/marketplace footprint, supply chain, product/service mix, key personnel, and growth strategies) in context of the potential threat actors seeking to engage in illicit activity to adversely impact the company. Assessing the risk posed by individual threat actors within this construct, the probability that they will attempt to steal a company's trade secrets, and the severity of such an event, is critical to determining which trade secrets merit the highest level of protection and enables management to implement more effective protective measures.

As part of its threat assessment, ABC's Compliance Counsel analyzes the company's operating environment, including markets in which the company operates, major customers, significant supply chain and business partners, key executives, employees' access to trade secrets, existing products/services, and designs for new product launches and/or mergers and acquisitions (M&A) activity.

A Framework for Individual Companies to Safeguard Trade Secrets and Mitigate Potential Threats

In this context, ABC analyzes the various threat actors that may impact its operating environment and the risk they pose, paying particular attention to the probability and potential severity of a breach. With ABC's leading market position in the industry, it suspects certain threat actors (i.e., malicious insiders, nation states) warrant closer attention and monitoring due to recent data

breaches resulting in the theft of intellectual property at ABC's competitors in locations where ABC also has production facilities. Using Figure 5 as a general guide, ABC researches recent incidents to understand the potential threat actors targeting the company and the likelihood of a malicious action from them.

Figure 5: Potential Threat Actors' Goals, Tools, Vectors and Targets

Threat actor	Goals	Tools and vectors	Trade secrets that could be targeted in your firm
Nation states	<ul style="list-style-type: none"> Technology to support military capabilities Strengthen "national champion" companies 	<ul style="list-style-type: none"> Foreign intelligence and security services Cyber vector Human intelligence operations Technical tools such as electronic eavesdropping, acoustic cryptanalysis, video surveillance and wiretaps Use of insiders Exploitation of open source information concerning companies' executives, vulnerabilities or projects. Co-opted entities such as state-owned enterprises 	<ul style="list-style-type: none"> Items with direct military applications, such as aerospace technologies "Dual-use" products, such as IT technologies and navigational systems, with both civilian and military applications
Malicious Insiders	<ul style="list-style-type: none"> Competitive advantage Financial gain Advance national goals 	<ul style="list-style-type: none"> Access to sensitive company information Manipulation of weak protections, lack of oversight over trade secrets Can access trade secrets on electronic/IT systems or that are hardcopy only 	<ul style="list-style-type: none"> Data that enables your firm to differentiate its services and products in your sector, such as source code or marketing plans "Dual-use" products Sensitive data on customers or suppliers
Competitors	<ul style="list-style-type: none"> Competitive advantage 	<ul style="list-style-type: none"> Cyber vector Technical tools such as electronic eavesdropping, acoustic cryptanalysis, video surveillance and wiretaps Use of insiders Exploitation of open source information concerning companies' executives, vulnerabilities or projects. 	<ul style="list-style-type: none"> Data that enables your firm to differentiate its services and products in your sector, such as source code or marketing plans
Transnational Organized Crime	<ul style="list-style-type: none"> Financial gain PII, other financial data Cybercrime as a service sold to others 	<ul style="list-style-type: none"> Cyber vector Some TOC groups willing to undertake physical attacks against company leadership, personnel and facilities Use of insiders Exploitation of open source information concerning companies' executives, vulnerabilities or projects. 	<ul style="list-style-type: none"> Any trade secret perceived as vulnerable to exploitation
Hacktivists	<ul style="list-style-type: none"> Advance political or social goals by exposing sensitive corporate information 	<ul style="list-style-type: none"> Cyber vector Exploitation of open source information concerning companies' executives, vulnerabilities or projects. 	<ul style="list-style-type: none"> Sensitive data on customers or suppliers Production/distribution technologies

1.2: Vulnerability and Protection Analysis

Threat actors often seek to exploit vulnerabilities in an organization's governance, financial, technology, operational or compliance architecture leading to opportunities for illicit behavior that create economic harm to the company. Accordingly, companies must proactively identify potential internal vulnerabilities in their policies, procedures and controls, as well as their reliance on suppliers and other business partners, and take steps to mitigate any exposure resulting from these weaknesses. These vulnerabilities can range from a lack of training on information security to employees using software without routinely checking for updates, to a highly valuable trade secret stored on an unsecured server with broad access within the company, to a lack of awareness among employees of where trade secrets are kept. Trade secrets can be gauged on a continuum from "fully protected" to "unprotected," and a narrative documenting the type and strength of protection, as well as the remaining vulnerabilities, can be attached to each trade secret. A critical component of the vulnerability assessment is to assess the maturity of the trade secret protection management system.

For each trade secret identified and located during the Level 1 inventory analysis, ABC's Compliance Counsel collaborates with senior executives and corporate functional leaders (e.g., CFO, CIO, CSO, CISO) to review where the information is stored and catalogs the existing protections. ABC also analyzes and documents the design and operation of the existing suite of policies, procedures and internal controls designed to secure and/or limit access to that trade secret. Through this process, ABC's management becomes aware of potential gaps—vulnerabilities—in its existing compliance/security architecture that may require new investment to strengthen and/or enhance efforts to mitigate the risks associated with the combined threat and vulnerabilities. They also identified processes within their trade secret protection management system that were weak and would require improvement. ABC leverages a traditional risk and control matrix to document its analysis, thereby facilitating a discussion with management; an abbreviated example is included as Figure 6

Figure 6: Threat and Vulnerability Matrix

Trade Secret	Threat Actors	Probability of Trade Secret Theft Event (high, medium, low)	Severity of Trade Secret Theft Event (high, medium, low)	Existing Policies, Procedures, Controls, and Mitigating Actions	Severity of Trade Secret Theft Event (high, medium, low)
Source Code	<ul style="list-style-type: none"> • Nation state X • Competitor Y • Competitor Z 	High	High	<ul style="list-style-type: none"> • Information Security policy • Limited access to local development group, November 2013 • Source code located on a secure server • Access control list to source code • Document handling standard 	Medium <ul style="list-style-type: none"> • We lack a consistent training program • We have found instances of source code being circulated • We have not conducted attack and penetration testing against our servers in the past year.

Protecting Trade Secrets: At What Cost to Collaboration?

Companies often raise concerns that taking steps to limit access to trade secrets by implementing stringent security measures has the inadvertent effect of creating “work arounds” in which employees create unofficial processes and means to access trade secrets so as to avoid encountering the security measures—for example, mandating a highly complicated password to access sensitive documents leads to employees writing the password on a note and keeping it in their desks where other staff may find it. While this would be a violation of company policy, employees may be doing so in order to “get the job done”, collaborate, and operate efficiently.

Companies must select the appropriate level of security controls for their unique corporate culture, the amount of time and resources to be invested in training and awareness campaigns. Once these issues are addressed, create clear policies and processes articulating the responsibilities of individual employees. Compliance monitoring and periodic analysis should also be implemented.

For example, since many of ABC's trade secrets relate to its source code, its vulnerability analysis targets the security of its information technology systems and the access controls surrounding the systems. ABC engages in discussions with its CISO, who identifies the security controls that are currently in place for the identified systems. They debate whether these controls are well understood by company employees, and review policies and training programs that support them. The team discusses the potential vulnerabilities of each level of protection given the known and suspected threat actors who may be targeting the company.

The cross-functional team responsible for the overall trade secret protection management system begins to realize the difference between IT security and trade secret protection. This major realization impacts how they proceed to develop a plan that integrates both. At this stage, ABC acknowledges these vulnerabilities and develops recommendations for enhanced mitigation.

Level 3: Trade Secret Portfolio Relative Value Ranking

With only limited resources to implement new safeguards around its most critical assets, how should management decide which trade secrets deserve greater protections? How should management rank its trade secrets based on the insights garnered from the initial analyses performed in Levels 1 and 2?

A Relative Value Ranking analysis provides the company with the means to conduct a qualitative assessment using value-based judgments on the relative importance of a trade secret so that it can perform an initial selection of trade secrets that have the most significant impact on the operations and performance of the business.

Following completion of Level 1 and Level 2, management has new and critical insights into the scope and extent of their trade secret portfolio, including potential areas of vulnerability and threat actors who may seek to inflict economic harm on the company. Depending on the company, these analyses may have provided insights into dozens of trade secrets that the company maintains; some of which are clearly more valuable or create more exposure than others. This value ranking is a critical in developing a return on investment (ROI) proposition that management can use to justify investing more resources in trade secret protection and IT security.

Figure 7 provides an illustrative series of questions to aid management's ability to prioritize those assets among its trade secret portfolio based on the insights from Levels 1 and 2. A related scoring methodology then yields a ranked version of the portfolio based on management's risk assessment of the assets. In order to safeguard the ranked list, companies may consider putting the process and ranked results under attorney client privilege to prevent a defense team from later claiming in court that lower value trade secrets should translate into lower value damages awards.

Following completion of its Level 1 and Level 2 analysis, ABC's Compliance Counsel gathers ABC's executives to evaluate the questions in Figure 7 and rank each asset. For each trade secret, ABC uses these questions to assess the dimensions of the asset's value to the business. In this instance, the relative weights of “Low”,

Figure 7: Establishing the Relative Value Ranking for Company Assets

	High	Medium	Low
How significantly would the company's reputation be impacted if this trade secret were compromised?	We would have devastating reputational impacts.	We would likely have some reputational damage that we would have to respond to and manage.	Not vary, may have some residual effects but we could recover from them.
How critical is this trade secret to the fundamental operation of the business?	It is absolutely critical and there are no viable alternatives.	It is critical but we could find an alternative if absolutely necessary.	It is not critical to our business operations.
How core is this trade secret to our corporate culture that its loss or theft would have a strong emotional impact on the corporate culture?	This is at the core of our culture and would have a devastating impact on morale and our identity.	This is core to our business and its loss would be felt by our employees but we would recover fairly well.	It is not a core component of our corporate culture.
Is this trade secret especially unique to the industry or is a similar product being used/sold?	We are the only company in the industry that makes/sells/uses this.	Other companies make/sell/use it but our version has an exceptional characteristic that makes it unique.	No, many other companies make/sell/use something similar.
Could competitors place a higher value on this trade secret than we do?	Yes, this can be used for many more purposes that we use it for and therefore.	Maybe, but we are unaware of how it may be valued differently.	No, its value is consistent across the market.
How important is this trade secret to current or projected revenue?	It is critical to current and/or future revenue and would be nearly impossible to replace.	It is important but we are sufficiently diverse that we could make up the difference if pressed to do so.	Not very important or we haven't determined its importance.

"Medium" and "High" were calibrated for each category (assessing, for example, the relative reputation cost of a "High" impact in the first column vs. a "Medium" impact) and then the overall asset scores combined. This exercise results in a ranked analysis of ABC's trade secrets by relative value, wherein higher scores are associated with trade secrets that are deemed more important or valuable than other trade secrets in ABC's portfolio. Deciding how appropriately to allocate resources to protect assets is not only dependent upon the relative score, but also an assessment of the economic impact should that trade secret be stolen. Accordingly, ABC's Compliance Counsel decides to proceed to the next level of the framework to assess the economic impact of a trade secret theft event for the ten trade secrets that ranked highest in this exercise.

Level 4: Economic Impact Attributable to Trade Secret Theft

In this Level, management will seek to assess the economic impact of a trade secret theft event for the company's most valuable trade secrets identified in Level 3. Applying both quantitative and qualitative analyses, management will calculate the potential economic losses attributable to theft and, leveraging results from previous Levels, adjust the economic loss analysis based on the perceived threat.

4.1: Impact Assessment

In this step, the company determines the adverse economic impact to the company if an individual trade secret asset is misappropriated. This process enables management to segment the total impact into manageable building blocks and understanding of both direct and indirect impacts helps to establish a complete picture of the economic losses attributable to a trade secret theft event.

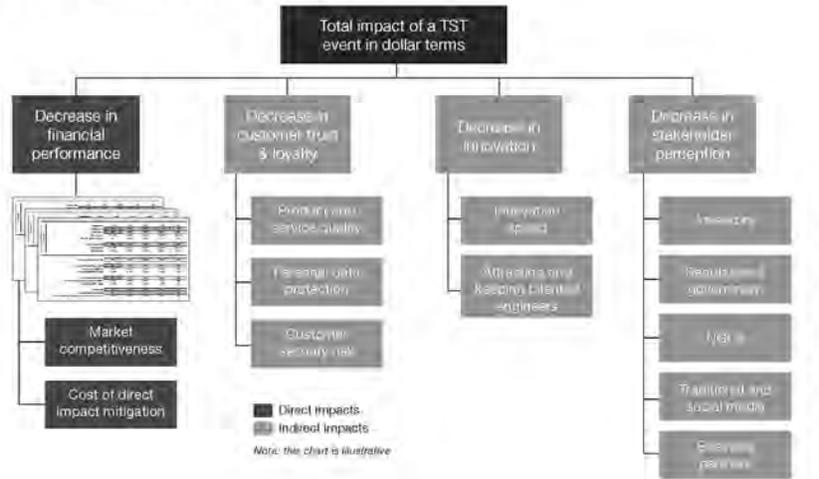
- ▶ **Direct Impact:** A measure of the direct financial and economic losses attributable to a trade secret theft event—i.e., lost sales/revenues, lost market share, lost profits, and/or lost economic opportunity; and
- ▶ **Indirect Impact:** An assessment of the indirect factors impacting a company's short/long-term ability to compete in the marketplace due to the theft of the output of its investment—e.g., reduction in customer trust due to concerns about ongoing relationships or adverse press impacting the company's reputation in the marketplace.

In this context, it is important to consider both the direct and indirect aspects of a trade secret theft event to help companies capture the full range of economic exposure that threat actors' actions may impose on

the organization. The results of the impact assessment provide the basis for establishing a ROI proposition for improving trade secret protection. In most companies, compliance is seen as a cost, not an investment. The valuation is critical to helping companies understand that improving trade secret protection is an investment that has a quantifiable ROI.

In this phase of the framework, ABC's Compliance Counsel may begin by conducting workshops with executives overseeing major subsidiaries or key business units and leaders of core corporate functions (e.g., finance, technology, sales/marketing, human resources) to map areas in which a trade secret theft event could adversely impact the value of the company's operations and business/market environment. A model for these discussions is reflected in Figure 8.

Figure 8: Economic Impact of a Trade Secret Theft (TST) Event



4.1.1: Direct Impact

Estimation of the direct financial impact from the theft of trade secrets is grounded in traditional discounted cash flow analysis that many companies use every day to make business and investment decisions. This estimate typically focuses on various factors including revenues, costs, and profit analysis. It may assess trade secret theft's impact on a company's market competitiveness, or the costs of impact mitigation actions:

- ▶ **Adverse Impact on Market Competitiveness:** Applying traditional discounted cash flow analysis to estimate the reduction in market share, revenue and profitability due to factors such as business interruption and/or dislocation after a trade secret is stolen, loss of potential licensing revenue, or loss of competitive differentiation; and
- ▶ **Cost of Direct Impact Mitigation Actions:** After an event, companies may take action to mitigate negative consequences and restore their competitive position or reputation in the marketplace (e.g., litigation against the responsible party). The costs associated with these actions should be included in this element of the estimate.

ABC's management identifies a range of threats related to potential exposure of particular trade secrets. Examples include, but are not limited to, the following:

- ▶ *A competitor could steal ABC's source code to re-engineer a product, discount its prices and still generate a profit because it would not have to cover the return on R&D efforts. Based on a market analysis, management can estimate what level of market share, revenues and profit would be lost.*
- ▶ *If threat actors compromise the production server for a key service that generates business through continuous micro transactions, the server can go down. Until the company restores operations it would lose revenues. The customer service department would likely work overtime to manage client complaints, and the company might need to prepare and deliver messaging related to the disruption. Management could estimate these lost revenues and additional expenses.*

- ▶ *If threat actors hack ABC's servers and gain access to "sensitive business information" related to ABC's supply chain that compromises the supply chain's ability to compete in the marketplace, suppliers could decide to take legal action against ABC if it appears ABC acted negligently in handling suppliers' trade secrets. Such legal action could contribute to increased legal fees and associated costs for ABC. ABC's legal department could make a reasonable estimate of the nature and amount of these costs.*

Applying these concepts, ABC management estimates the direct financial impacts for the top ten trade secrets in its portfolio identified in the Level 1 exercise.

4.1.2: Indirect Impact

Companies must also consider longer-term, indirect adverse changes to their business environment resulting from trade secret theft. As noted above, these issues typically involve qualitative but nonetheless critical impacts to the organization (e.g., customer relationships, reputational matters) that can be thought of as key drivers of company value. The common element of these indirect impacts is that they are strategically important for the company, but the extent to which they drive financial performance is typically difficult to quantify.

In this context, ABC identified several areas in which a trade secret theft event will adversely impact their business.

- ▶ **Customer Trust and Loyalty:** *ABC believes a trade secret theft event would negatively impact the trust and loyalty the company experiences with certain customers who value the company for product quality and safety. If ABC cannot protect its own assets, customers may doubt that their own confidential information (e.g., design specs) is adequately protected. Customers may express further concerns about a threat actors' ability to access their own systems through the compromised source code. Such factors may decrease customer's willingness to engage with ABC, thereby reducing long-term revenues and profitability.*

- ▶ **Innovation and Talent:** ABC's key competitive advantage lies in its innovative approaches and its ability to develop new alternative energy solutions that provide value to customers. If source code is stolen, the company's pace of innovation may stall as enhanced security measures are adopted, requiring engineers to adapt to new policies and procedures. Key engineers may leave the company, or it could become more difficult to recruit new talent. Further innovation processes may be cut back. Collectively, these factors could lead to decreased innovation and subsequent reductions in long term performance.
- ▶ **Stakeholder Perception:** ABC works with multiple stakeholders who influence markets and customers, so maintaining the trust of the company's stakeholders in ABC's security protocols is essential. For example, investors may assert that the company lacks appropriate controls and protection processes to support sustainable growth, deciding to sell shares despite the absence of direct financial consequences of the theft. Also, if discussion of the theft trends on social media blogs or is covered by traditional media, it can influence long-term customers' buying decisions. Similarly, the theft may erode the trust of the company's key business partners.

Such indirect impact areas all bear upon areas of strategic importance for the long-term performance of companies. To facilitate assessment, companies can consider Key Performance Indicators ("KPI") for each identified indirect impact area and convert them into dollar terms using Multi-Attribute Utility Analysis ("MUA") to measure the economic impact on the business. Specialists familiar with the identified indirect impact areas can inventory existing KPIs and/or create new KPIs to measure performance. While the values generated do not represent accountancy measures, indirect impacts can be converted to economic costs, allowing comparisons of prioritized trade secrets' direct and indirect impacts. This will also help measure the benefits of potential actions companies could take to protect their trade secrets further, as discussed later in the paper.

For example, ABC may convene discussions to identify KPIs across all the identified indirect elements. The company's customer surveys and market surveys targeting future customers include questions that focus on customer trust and loyalty. Management estimates

how these survey results would change in case of a trade secret theft event for each of the prioritized trade secrets. With these measures available, MUA techniques enable ABC management to construct a model expressing the economic costs of each KPI, making it comparable to the direct financial impact estimate.

4.2: Threat Adjusted Economic Impact

The Impact Assessment (Level 4.1), Threat Actor Analysis (Level 2.1), and Vulnerability Analysis (Level 2.2) are aligned to form a total "Threat Adjusted Economic Impact" value for each trade secret and across the portfolio. Collectively, these considerations inform management of the potential threats facing individual trade secrets with a clear view of where the impacts would be, how likely a threat is, and how protected the company is against them. This information enables management to allocate resources across the portfolio to adequately safeguard these important assets – the next level in the framework.

For example, an important trade secret in ABC's portfolio is inherently valuable to the company, but the threat actor analysis indicated that marketplace demand among threat actors for this trade secret was low and the company's existing procedures and internal control were adequate to mitigate potential exposure. Conversely, ABC's management determines its source code is equally valuable, yet its exposure to threat actors would inflict significant economic harm to the company. ABC's analysis further indicates that new working practices and internal controls would enhance ABC's ability to mitigate potential threats in this area.

Level 5: Protective Action Portfolio Management and Allocation of Resources

Analysis of the Threat Adjusted Economic Impact for those trade secrets deemed most important to a company enables management to make informed decisions about how appropriately to use its existing resources to strengthen its ability to mitigate potential threats through advanced protective measures. With insights into the economic costs of a potential trade secret theft event in hand, management can effectively assess the incremental costs of developing and implementing a trade secret protection management system. This can include including new policies,

procedures and/or internal controls against the perceived threat, and the appropriate allocation of resources. For example, the benefit of new protective actions (e.g., impact mitigation, reduced exposure to threat actors, strengthened access controls) can be measured through the reduction in the Threat Adjusted Economic Impact for a single trade secret or across the portfolio, if the benefit extends to multiple trade secrets. Collectively, this approach enables management to effectively analyze its existing resources and efficiently reallocate those resources to safeguard the company's most important assets; in turn, aligning resources with the company's broader strategic priorities and objectives. The cost of developing and implementing a trade secret protection management system can also be established, thus allowing the company to assess the ROI.

ABC, after completing the previous levels of the framework, has a clearer understanding of which trade secrets are at highest risk of exposure, and how exposure would impact its operations. Now, through a series of workshops with subject matter experts, management lists a series of action items that various parts of the organization planned to protect the selected trade secrets. Some of the identified actions focus on the following areas:

- ▶ IT would raise the company's protection level by establishing new servers and firewalls and ensuring all software is routinely updated;
- ▶ The product development teams would develop multiple plans to segregate and limit access to source code in order to mitigate the adverse economic impact if one piece of source code were stolen;
- ▶ The public relations and customer service teams would design "emergency" protocols with which the company can quickly react and communicate to the market and key stakeholders in case of a trade secret theft event. Such a response would help mitigate adverse changes to customer trust and perception of key stakeholders.

In this process, ABC's management team evaluated the recommendations for advanced protective measures around each of the trade secrets and, within its pool of available resources (e.g., budget, talent/personnel, and capabilities of existing information technology systems), targeted mitigation strategies where the enhanced protective measures would lead to the highest reduction to an individual trade secret's Threat Adjusted Economic Impact. This enabled the company to measure the ROI on each action and select the appropriate portfolio of actions to increase the ROI given the company's available budget.

On this basis, management constructed a briefing to senior executives and ABC's Board of Directors to convey their observations of ABC's trade secret portfolio, potential threat actors targeting the company and exposures identified in the vulnerability analysis. The briefing included recommendations to mitigate these emerging threats, including an improved trade secret protection management system, consisting of new policies, more effective procedures and infrastructure-hardening controls. The recommendations were grounded in an economic assessment that balances incremental costs against expected returns. ABC's management plans to perform this analysis annually to help to establish that the company's compliance and security efforts align with the changing market environment and evolving strategic priorities of the company.

This framework addresses the key components of a company's strategy to protect its trade secrets—identification of the secrets, clarification of where and how they are stored or protected, and informing management's ability to make effective and efficient decisions on how to adequately deploy protection measures based on meaningful economic analyses. Applying this framework is a significant undertaking for any company, particularly those approaching these processes for the first time. Stratifying the framework into discrete levels allows companies to take an iterative approach to safeguarding their trade secrets, in order to marshal the necessary resources, obtain buy-in from key stakeholders, evaluate progress, and gain consensus at each level before continuing. Completing each level should be considered significant progress for any company that undertakes this effort.

How do Expectations of Future Trade Secret Loss Impact Private Sector Decision-Making Today? ►

Corporate executives around the world regularly make decisions based on expectations about the future. Choices related to new product launches, expanding strategic business relationships, investment in capital projects, and research and development expenditures are each grounded, in part, on companies' expectations about the future. Effective management of a company's trade secret portfolio requires a similar perspective.

- Will the identified trade secret provide the company with a competitive advantage in the marketplace? For how long? What level of economic returns will these trade secrets provide? Over what period of time? How will the company capitalize on this investment in the marketplace?
- How will the company protect these trade secrets from internal and external threat actors to promote the anticipated competitive advantages and returns in the marketplace are achieved? Are new compliance and security protocols required to safeguard the investment during this phase? What is the plan to improve the maturity of the trade secret protection management system and the information security program? How are those costs factored into the expected economic returns?
- How will expectations involving external factors—regulation, openness of the Internet, cybersecurity threats, emerging threat actors in the marketplace, the pace of innovation—drive the company to evaluate the diversity of threats and incremental costs associated with protecting its trade secrets? How can improved trade secret and IP protection be used as a competitive advantage in the global marketplace in attracting customers, partners and investors?

For years, executives have asked questions like these as part of their internal analysis and due diligence around new investments in R&D projects where the investment's expected time horizon for a return extends for several

years. In today's marketplace, however, these questions are increasingly important given the emerging threat of trade secret theft and the prevalence of other forms of economic crime that can adversely impact the economic analyses upon which these investments are based. Accordingly, corporate executives are increasingly focused on analyzing potential future scenarios and the consequences of acting (or choosing not to act) to further protect the development of their trade secrets; especially for significant capital investments with extended periods before economic returns are generated.

In 2013, the U.S. Intellectual Property Enforcement Coordinator wrote in its strategic plan on IP enforcement that, "As we move forward, we are aware that new technologies, evolving social norms, new business models, and novel global distribution mechanisms will present new challenges and opportunities to combat infringement of American intellectual property rights."³³

New challenges and opportunities form the basis of the following section of the report. We modeled three scenarios focused on trade secret protection-related issues over the next 10-15 years. The scenario models are not predictions; but rather projections of possible outcomes based on a narrow combination of drivers. They are intended to challenge assumptions and provoke new thinking about this issue and where it might go in the future.

As part of this scenario modeling effort, we convened panels of subject matter experts from leading companies, law firms that focus on patents and trade secret protection, and personnel from think tanks and academic institutions that focus on trade secret theft and global change. These subject matter experts provided insights on the challenges and opportunities for companies to consider in each of the three scenarios. They also offered mileposts and indicators that would be observable in the real world that might indicate one scenario or aspects of one scenario could become more likely than others.

Key takeaways from our modeling sessions include:

1. **Trade secret protection must increasingly focus on external threat actors who may have designs on stealing critical trade secrets and IP.** However, in the present world and going forward, the insider threat will continue to be a dangerously rich source of trade secret loss.
2. **Changing social norms, especially a country's cultural expectations of the degree to which companies must disclose confidential and commercially sensitive information, will significantly impact trade secret protection in the years ahead.** When considering countries for expansion or new market entry, companies may factor how the government and the culture generally treat secrets, as well as the extent and nature of protections the company can expect to receive if its trade secrets are misappropriated.
3. **The openness of the Internet will have a significant impact on how companies develop and protect trade secrets.** If separating or walling off from the Internet becomes politically and socially accepted, we may see some trade secrets—built on an assumption of an open and thoroughly interconnected world—decrease in value.
 - ▶ In the latter half of 2013 some multinational corporations and national governments publicly raised the issue of segmenting or walling off parts of their Internet traffic.
4. **Sectors that are able to band together and share threat information concerning trade secret protection will likely fare better than sectors in which participants remain combative and distrustful of peer organizations.**
 - ▶ Intra-sector intelligence sharing already pays dividends in some sectors of the economy; more sectors may pursue this collaborative approach in order to better enable trade secret protection in the coming 10-15 years.

Drivers and Scenarios

Numerous drivers and forces will have an impact on trade secret protection in the coming 10-15 years. For our futures section we selected four drivers that will likely impact these futures and that, in different combinations, offer compelling lessons and different visions for us to consider from our current vantage point.



Driver 1: Regulation for the protection of trade secrets: Enhanced global regulation could take hold to increase protection of trade secrets. Alternatively, a future in which no such regulation emerges could be one of increasing collective and individual vulnerability for companies, individuals, countries and other global players.



Driver 2: Balance between cyber offense and defense: A defense-intensive environment would be characterized by its clear, unambiguous ability for attribution of cyber activities and dramatically improved cyber defense systems. A tilt towards the cyber offense would not only mean that threat actors would have the upper hand technologically, but that individuals and companies may be more willing and able to launch cyber attacks on their own.

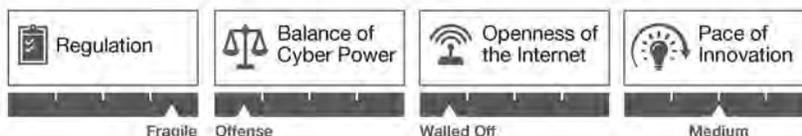


Driver 3: Openness of cyber commons vs. "walled gardens": The openness of the Internet could remain the status quo for the next 10-15 years. An alternative would be the emergence of walled gardens or the creation of IT networks that are separated from the wider Internet. Walled gardens could be used and created by cities, sectors or countries.



Driver 4: Pace of innovation: The final driver considers the rate at which new ideas are developed and spread across the global economy. Innovation is a key foundation of much of what drives the creation of trade secrets. In futures with a faster pace of innovation, there could more trade secrets.

Scenario 1: "Shelter in the Storm"



In this future, the absence of a robust regulatory framework and international consensus on means for trade secret protection—including but not limited to cybersecurity—combines with offensive cyber capabilities having the upper hand.

Fears of intelligence-gathering by governments, dramatically increased data-theft by criminals, and a series of devastating global cyber attacks creates pressure for individuals and corporations to wall their information off from a dangerous world. In addition to this fear there is a definitive tilt in the balance of cyber power towards those who are on the offense, leading to periodic spikes in cybercrime and cyber-enabled economic espionage. This tilt to the offense is a dual-edged sword, as social norms and the lack of regulation make it easier for some companies, individuals and groups to periodically go on the offensive themselves, launching carefully honed cyber attacks at assessed threat actors.

The perceived dangers to trade secrets and Intellectual property on the Internet and connectivity in general lead to new coalitions seeking to increase their security through collective measures. By the end of this 10-15 year period, some companies and sectors have begun to combine forces—sometimes by sector, nation, state or country—behind separate Internet systems that become known as walled gardens.

Information blocs of countries and industries become prevalent. Data centers—formerly globalized—now are owned by groups of countries and hosted in shared locations under the terms of multilateral agreements that exclude non-members.

Eventually, there is some expanded exchange and trade among members of these cyber-blocs. Global commerce decelerates though, and firms with extensive cross-border operations suffer as their ability to conduct data transfers is restricted. Customers prefer to "buy local," reducing firms' need for competition-driven innovation and reducing the value of many trade secrets. Some companies decide to stay outside the walls for a variety of factors.

The observations of many subject matter experts (SMEs) related to this scenario focused on the unique challenge of the walled garden as an active element of this future possibility. SMEs agreed that this could be one of significant adjustment for government, companies, individuals and even threat actors.

Challenges

- ▶ Organizations will face higher costs if they choose to wall off and separate from the open Internet; smaller entities may not be able to survive.
- ▶ Global regulations and standards would suffer and be replaced by limited agreements within walled gardens or between walled gardens.
- ▶ This world will feature high transaction costs and slower advances in technology.
- ▶ Inside the wall, companies will be less agile and will realize fewer gains.
- ▶ The high barrier to investment and cooperation outside the walls may lead to lower levels of investment and loss of trade opportunities.
- ▶ Being in the walled garden would limit companies' choices of suppliers, employees, service providers and customers.

Opportunities:

- ▶ Within the walled gardens, there will be greater security, but at the cost of agility. Those outside the walled gardens will face higher risks, but will also have chances to reap higher rewards.
- ▶ Within the walled gardens, especially larger more diverse gardens, there would be numerous opportunities for some sectors to flourish given the high degree of protection from cyber-enabled economic espionage.
- ▶ The need to abandon the current model of leveraging overseas talent and distributed supply chains can provide new opportunities for companies to do work that is perceived as more secure though perhaps more costly.

- ▶ Companies with a rapid R&D and product development cycle might choose not to wall off, instead remaining in between the walled gardens even if this meant operating at a higher state of risk in order to provide the greatest freedom of movement despite potential increased threats.

Mileposts:

- ▶ Quantum computing capabilities to advance the shift of cyber power towards the offense.
- ▶ A key member of the G8 or G20 walling off parts of its Internet.
- ▶ A series of devastating cyber attacks on trade secrets and IP.
- ▶ Governments and companies are unable to gain the advantage on cyber attackers and are constantly behind the curve.

Scenario 2: "The Roaring 20(20s)"



Open cyber commons, combined with a tilt towards stronger cyber defenses, produces a scenario in which companies are increasingly able to protect trade secrets and consequently undertake collaboration, joint ventures, and investment with greater confidence.

Because of the balance of cyber power towards the defense, the private sector at times becomes complacent about security, discounting emerging threats and short-changing security measures. This results in occasional intense bursts of cyber attacks against entire sectors when threat actors find chinks in the technological armor. Public-private partnerships—partly

the result of more effective and far-thinking regulation on trade secrets and cyber security—and strong intelligence cooperation within sectors limit such outbreaks to manageable proportions. Companies cooperate to drive a culture of compliance into the global supply chain—upstream and downstream. Trade secret protection management systems are implemented and become as common as quality management systems.

Effective regulation in a defense-intensive environment pushes malicious activity to the fringe and reduces the incentive for criminal efforts to steal trade secrets, while not entirely stopping sophisticated efforts by intelligence services and mature organized criminal networks.

How Do Expectations of Future Trade Secret Loss Impact Private Sector Decision-Making Today?

The moderate pace of innovation fosters the creation of new trade secrets and intellectual property. Global trade and commerce steadily progress.

Many SMEs were cautious about the Roaring 20(20s) and were careful to point out that even such a seemingly safe place as the world would come with a cost for many companies.

Challenges:

- ▶ Organizations will seek to abuse a stronger regulatory environment by mounting frivolous lawsuits.
- ▶ Smaller companies without the resources to deal with new regulation or a harsher litigation environment might be challenged to stay in business.
- ▶ The decrease in cyber attacks and a tilt in the balance of cyber power towards the defense may make some companies complacent about security and more vulnerable to attacks from cyber actors and insiders.

Opportunities:

- ▶ If the regulatory regime were truly effective in protecting trade secrets, then the Roaring 20(20s) might witness a golden age of trade secret protection.
- ▶ If cyber systems are more secure, companies can focus on policing negative employee behavior, such as the rise of the insider threat. They can continuously improve their trade secret protection management systems.

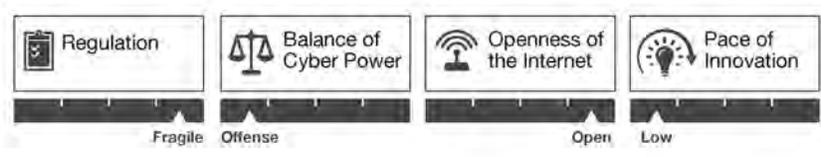
- ▶ Smaller companies may increase their flow of new ideas and trade secrets into larger companies to take advantage of larger companies' regulatory processes and protections.

- ▶ Large companies could cooperate to improve respect for trade secrets in their end-to-end supply chains.

Mileposts:

- ▶ Significantly increased public outcries about trade secret theft leads to the emergence of a regulatory framework—particularly national-level statutes—that would clearly demonstrate an ability to help companies protect trade secrets.
- ▶ Actions by the U.S. Government or other governments to share more clearly defined cyber information and intelligence with the private sector or change laws to enable national-level cyber systems to act as both cyber shield and sword for the private sector, thereby gaining the cyber offensive against threat actors.
- ▶ A consistent string of defensive victories against threat actors known to target trade secrets that would be devastating enough to keep them on their heels for extended periods of time.
- ▶ Signing and enforcement of global agreements curtailing economic espionage.

Scenario 3: "Radical Transparency"



In this world, regulation and norms on trade secret protection break down, leaving it to individuals and companies to decide when to put up fences, when to steal trade secrets, and when to retaliate for cyber intrusions. The balance tilts in favor of cyber offense, resulting in rapidly emerging threats to trade secrets from individuals and small networks.

Governments can offer little protection other than lip service to the mounting losses. Regulations and customer expectations work to keep corporations or countries from creating walled gardens as an option to protect trade secrets and other IP.

The private sector has little choice other than to adopt an open and transparent collaboration model because widely shared innovation-to-market practices are the norm as the only way to meet customers growing expectation of rapid delivery.

Those launching cyber attacks have the consistent edge in the Radical Transparency world and the high cost of protecting trade secrets disincentives private-sector R&D in some sectors. Some governments try to pick up the slack in R&D in goods and services related to defense, pharmaceuticals, and public health. The effects of slackening R&D are evident only towards the end of the period as the flow of new technologies becomes dramatically slower.

Governments and multinationals exert decreasing influence as "radical transparency" accelerates the power of existing societal forces such as WikiLeaks, grass-roots anti-corruption movements, and new "third forces" gain traction. Transparency advocacy groups' cyber and political power grows and provides them with a platform to pressure companies and governments for transparency above protections for trade secrets.

Many subject matter experts felt that the balance of drivers laid out in this scenario would be the "storm" that might precede the future described in our first scenario, "Smile in the Storm." Cyber-SMEs opined that the future is, in some ways, not far off from the status quo. Lastly, some SMEs independently concluded that the world would be welcomed by some of the largest Internet-related products and services companies given their interest in openness and transparency.

Challenges:

- ▶ For businesses this is a hypercompetitive environment for resources, talent and opportunities.
- ▶ Given the hypercompetitive environment smaller firms may not do well in this future.
- ▶ Some organizations may seek to act preemptively against perceived threats, and might feel freer to use cyber weapons against known or suspected threat actors.

Opportunities:

- ▶ Academic institutions and non-profits, which have long emphasized transparency, would become more influential compared to the present day.
- ▶ Given the balance of cyber power and the increasing acceptance of transparency, non-electronic document delivery systems, such as couriers and package delivery companies, might see their services expand for businesses that will not risk electronic networks lest their information might be divulged by those seeking transparency or to steal the information.
- ▶ Some companies can band together to share information face-to-face as some sectors have done. The financial sector's creation of the Financial Services Information Sharing and Analysis Center ("FS-ISAC") is a good example of what we might see more of in this future.

Mileposts:

- ▶ Organizations that champion transparency gain sponsorship from global leaders or G20 countries, or find champions from leaders of similar stature.
- ▶ Use of stolen data becomes more accepted, driven by changes in social norms.
- ▶ National and international regulations and treaties on trade secret protection flounder and fail.
- ▶ A sustained mass movement against trade secrets or corporate secrecy that gains traction beyond the fringes of political circles.

Key observations from scenario modeling exercise:

Companies and industry associations should consider new and innovative ways to come together to think about the road ahead for trade secret theft, and to identify the drivers that will impact trade secret protection in their areas of concern. The drivers used to construct these three scenarios represent only a fraction of the many influences that will shape how trade secrets are protected and misappropriated in the next 10-15 years. Additional forward-looking analyses that consider how threats to trade secrets may evolve may illuminate other critical drivers. Such efforts will spark debate and discussion about which drivers companies, governments and individuals can influence most effectively in order to create more security and stability for their interests and assets.

Please note that the possible opportunities and challenges summarized in our scenario modeling exercise can be replicated or supplemented by individual companies to help them prepare for a variety of future outcomes and to be ready to act decisively to make the appropriate and most secure use of their intellectual property and trade secrets, regardless of what future emerges. By understanding how trade secret misappropriation and other aspects of trade secret protection, including trade secret protection management systems, may develop in the next decade, companies can incorporate these trends into the framework analysis documented earlier in this study.

Conclusion

The trade secret evaluation methodology provided in this report can provide a first step in a larger collective effort to improve trade secret protection, and help companies to better appreciate the importance of proactive protection as an up-front investment. At the company level, firms would benefit from a better understanding the relative value of their trade secrets and the harm that any loss or theft would inflict on them. Understanding the probability and severity of a potential breach can better inform decisions on investments and other critical activities. We hope this also encourages and inspires companies to be more forthcoming in discussing the challenges associated with trade secret protection, thus advancing a broader dialogue on this issue.

This report also provides a glimpse into three possible futures concerning trade secret theft. In addition to demonstrating the breadth of situations that companies must consider and plan for, such a modeling exercise is particularly critical in an era where technology, policy, customer demand and innovation are making trade secrets ever more valuable to those who create them as well as those who wish to steal them. Companies that fail to anticipate the evolution of threats, regulation and other key drivers risk falling behind their competitors and losing market share.

There is increasing convergence between concepts of privacy and data security generally and trade secret protection. The measures that consumers use to protect their personal information overlap significantly with measures that companies take to protect their trade secrets (e.g., consumers and employees not falling victim to spear-phishing scams; not storing sensitive information in the “cloud”). The more that companies can emphasize that their trade secret protection measures can be used to protect personal privacy, the more acceptances may be gained in employee populations. This may occur on a national level as well as a company level.

The challenge of trade secret theft is too large for any one government, company or organization to deal with alone—only a collective focus on this issue will help improve innovators’ ability to secure their most critical information and intellectual property. This cooperative effort will be strongly aided by the investment of individual companies’ time and resources to help to establish they know who threatens their own interests and how to measure the value of their own trade secrets. Replication of this sort of increased self-awareness across entire sectors would produce a detailed understanding of the collective threats and challenges, and the thorough extent of the value of trade secrets. Private sector companies—and other targets of trade secret theft—should approach this issue with a sense of urgency. Threat actors show no signs of slowing their attacks on trade secrets, and each new advance in technology brings new potential vulnerabilities with it.

“An environment where it may be easier to steal a vital intangible asset than it is to value, disclose, or even realize its loss is an inherently risky one.”

—PwC Global Economic Crime Survey, 2014

Acknowledgements

This report represents the analysis and efforts of many individuals within CREATE.org and PwC. This publication was produced under the direction of Pamela Passman and Leslie Benton from CREATE.org and Sanjay Subramanian and George Prokop from PwC. Our report was created and coordinated by Marissa Michel, Craig Stronberg and Peter Geday.

During the drafting of this report, we consulted with numerous subject matter experts in the private and public sectors who participated in our threat modeling workshops and reviewed our final draft. We also would like to thank Roberto Rojas for his assistance.

Endnotes

1 "Economic Espionage Act of 1996" Published by the U.S. Government

2 Article 39 of the World Trade Organization's Agreement on Trade Related Aspects of Intellectual Property Rights ("TRIPS") states: "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or Used by others without their consent in a manner contrary to honest commercial practices so long as such information: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret"

3 The Center for Responsible Ethics And Trade ("CREATE.org"), Trade Secret Theft: Managing the Growing Threat in Supply Chains (May 2012)[please add link]

4 "The 2012 Statistical Abstract/National Data Book, Patents and Trademarks: 1990 to 2010," Census, Bureau, U.S. Department of Commerce, 2013

5 "The Report of the Commission on the Theft of American Intellectual Property", 2013

6 "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods", General Accountability Office, April 2010.

7 Ibid

8 National Science Foundation, National Center for Science and Engineering Statistics. 2013. National Patterns of R&D Resources: 2010–11 Data Update.

- 9 2013 and 2013 Global R&D Funding Forecasts, *Battelle.org* and *R&D Magazine* – December 2012 and December 2013
- 10 The Battelle Foundation, “2013 Global R&D Funding Forecast,” December 2012
- 11 Justin Hicks and Robert D. Atkinson, “Eroding Our Foundation: Sequestration, R&D, Innovation and U.S. Economic Growth,” *The Information Technology & Innovation Foundation*, September 2012
- 12 Association of Certified Fraud Examiners (“ACFE”), “Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study”
- 13 Treasury Inspector General For Tax Administration: Office of Inspections and Evaluations, “The Internal Revenue Service Needs to Improve the Comprehensiveness, Accuracy, Reliability and Timeliness of the Tax Gap Estimate,” August 21, 2013
- 14 Myths and Realities of Governance and Corruption, Daniel Kaufmann, World Bank, October 2005
- 15 Business Software Alliance, 2012, “The Shadow Market: 2011 BSA Global Software Piracy Study: Ninth Edition”
- 16 U.S. Department of Justice: The Economic Impact of Illicit Drug Use on American Society, 2011
- 17 Havocscope: Global Black Market Information; “World Black Market Value”, December 2013.
- 18 Illicit Financial Flows from Developing Countries: 2002–2011. Dev Kar and Brian LeBlanc. Ford Foundation, December 2013
- 19 Office of the National Counterintelligence Executive (“ONCIX”), “Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011”, October 2011, published by the Office of the Director of National Intelligence
- 20 Office of the National Counterintelligence Executive (“ONCIX”), “Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011”, October 2011, published by the Office of the Director of National Intelligence
- 21 *Ibid*
- 22 *Ibid*
- 23 “Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets,” U.S. Department of Justice, December 21, 2011.
- 24 *RJGG v Director General of Security* [2013] FCA 269 (Federal Court of Australia, Foster J, 27 Marcy 2013)
- 25 PwC, State of Cybercrime Survey 2013; State of Cybercrime Survey 2012
- 26 Office of the President of the United States, “Administration Strategy on Mitigating the Theft of U.S. Trade Secrets,” February 2013
- 27 Office of the President of the United States, “Administration Strategy on Mitigating the Theft of U.S. Trade Secrets,” February 2013
- 28 *Ibid*
- 29 Katherine Herbig, “Allegiance in a Time of Globalization,” Defense Personnel Security Research Center, December 2008.
- 30 Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, February 2013
- 31 Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, February 2013
- 32 “White House Strategy to Combat Transnational Organized Crime”, The White House, July 19, 2011
- 33 Organized Crime and Cyber-Crime: Implications for Business, Phil Williams, CERT@ Coordination Center
- 34 Office of the Director of National Intelligence, “Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence,” March 12, 2013
- 35 Raj Samant and Francois Paget, “Cybercrime Exposed: Cybercrime-as-a-service,” McAfee.
- 36 Dr. Mike McGuire and Samantha Dowling, “Cyber crime: A review of the evidences, Research Report 75. Chapter 1: Cyber-dependent crimes,” Published by the United Kingdom Home Office, October 2013
- 37 Office of the Director of National Intelligence, “Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence,” March 12, 2013
- 38 Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases, U.S. Attorneys’ Bulletin, November 2009
- 39 U.S. Intellectual Property Enforcement Coordinator, 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT, June 2013, Published by the U.S. Government

www.create.org
www.pwc.com

© 2014 DREAtE.org. All Rights Reserved.

© 2014 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the U.S. member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisers.

Mr. COLLINS. Mr. Burns, could you elaborate further on why both a strong patent system and a Federal civil right of—private right of action are important for the continued dominance basically of the U.S. IP industry?

Mr. BURNS. Absolutely. You know, patents and trade secrets are complimentary forms of intellectual property, and there is this constant interplay within enterprises, within members of IPO asking the question, is this something that is better classified as a trade secret or as a patent.

They deliver tremendous value for our enterprises in just a countless number of ways. You know, obviously patents, although they have limited duration, are exclusive rights, and that means that they have a certain kind of value that is different from trade secrets.

Trade secrets are oftentimes the manufacturing techniques, the what we call the special sauce—

Mr. COLLINS. Okay.

Mr. BURNS [continuing]. That is linked to the patented right. Used together, they are a very powerful tool for generating revenue flows, for allowing our business leaders to make intelligent capital allocation decisions about where to invest within our companies, and they create certainty that we are going to be able to reap some kind of benefit from that R&D investment that in and of itself is so risky.

But if it actually leads to patented subject matter and a panoply of trade secrets that accompany it, it is much more likely that that is going to be a successful technology business enterprise, so—

Mr. COLLINS. And I think that is true, and I think one of the things that I wanted to add to it, I think one of our discussions that we enter into is we take the property right ownership, we take thus in what I call “esoteric terms.” We talk about intellectual property, patentable items, trade secrets, and really the bottom line is whether you are talking across the board from manufacturing to music to wherever.

We have taken it away from actually there is an ownership interest in here, and I think that is something that we lose and we’ve got to get back to talking about it being the building block of folks’ dreams, ideas that are actually tangible as—just as tangible as this phone sitting on this desk, and if we don’t do that, then both Democrats, Republicans, all of us are going to be hurting because people are going to tune out to what we are talking about.

Very quickly, a lot of different groups support this Federal right of—civil right of private action, but at the same point had two very different approaches to patent reform. Very quickly, anyone that wants to—to Mr. Moore or anyone, is there—why is there a consensus over trade secret legislation more so than IP or the intellectual property or patentable items?

Mr. MOORE. Thank you, Congressman. We are one of the organizations that did not take a position on the patent reform bill, in part, because we had members on very different sides of that issue.

We have a very broad membership, lots of different business models and approaches, but I am here, and I am here because our members agree on this issue. They all have trade secrets, they all are seeing a rising threat both at home and abroad, and they all

want to make sure that those trade secrets are effectively protected.

Mr. COLLINS. Well, I appreciate that, and Mr. Chairman, I know I am out of time, but I think it goes back to this issue that as my friend from California put it, the “nerd caucus” is here, and we appreciate this because in the end, a lot of those nerds have great ideas and dreams and hopes that we want to protect for future generations, and I think this is a great part of this hearing for that.

And Mr. Chairman, with that, I yield back.

Mr. COBLE. I think, folks, in all candor, truth in advertising, I am not sure I am qualified to be a member of the “nerd caucus” but—

Mr. COLLINS. All Ernest Tubb fans can be classified as in a “nerd caucus.” You and I—bluegrass will get us there, Mr. Chairman.

Mr. COBLE. I thank you for that.

The distinguished gentleman from New York, Mr. Jeffries is recognized

Mr. JEFFRIES. Thank you, Mr. Chairman.

Mr. Burns, there was reference made to General Alexander’s observation as it relates to the nature of and scope of the problem that we confront in this area, and I just wanted to get some clarification. I gather it was in a 2012 speech he stated that IP theft due to cyber espionage is the greatest transfer of wealth and history, estimating that U.S. companies lose 250 billion per year due to IP theft.

Are you aware as to whether he was speaking specifically about trade secret theft or is that \$250 billion number all encompassing and inclusive of patent infringement, copyright infringement, counterfeit and/or piracy, as well as trade secret theft?

Mr. BURNS. It is my belief, sir, that he is referring specifically to trade secret theft.

Mr. JEFFRIES. Okay. And that would be consistent with other studies that have been done in this area in terms of that particular amount?

Mr. BURNS. Absolutely. Those numbers fall within the range that was put forward in the CREATE study of between 180- and \$400 billion in losses, yes.

Mr. JEFFRIES. And I think everyone has testified either explicitly or implied in their remarks that there has sort of been a recent explosion of trade theft activity and it is become more sophisticated over time. What accounts for that phenomenon? And if anyone else on the panel wants to weigh in, that would be fine as well.

Mr. MOORE. Well, just to share with you some of the things that we hear from our member companies. I think part of the issue is the greater mobility of our workforce.

One of our member companies, a small business from Maryland, testified in the other chamber last month and said, “look, you know, I have six international airports within 100 miles of my facility in Baltimore, and you know, by the time I realized what has happened and take action in my home state and in the other States where these other airports, the five other airports are located, these can be long gone and so the mobility of our workforce, the ability of people to get on a plane and be out of the country quickly, I think, is big challenge.”

Second, we certainly face a technological challenge. As I pointed out in my prepared testimony, what might have taken a moving truck to move out of a company in terms of documents, records, different types of information kept secret, can now go out the door on a thumb drive, can stick it in the back of your pocket, nobody knows you have it, and that is, I think, enabling some of the challenges as well.

Mr. JEFFRIES. Thank you.

Mr. Hertling, as you understand it, does the Department of Justice civil division currently have any authority under law to address the trade secret issue?

Mr. HERTLING. The Economic Espionage Act provides to the Attorney General an injunctive remedy to go into Federal court. I don't know whether that right, whether that ability is exercised by the Civil Division. I suspect, because the nature of getting the department involved in these sorts of instances, that you are probably actually looking at the Criminal Division or, of course, typically the U.S. Attorney's Office actually being the entity that would enforce that right rather than the Civil Division, but I don't honestly know.

Mr. JEFFRIES. Okay. Right. And most U.S. Attorneys' Offices, certainly the ones that are located in the City of New York, have both a criminal division and a civil division present in the same office. Perhaps that is an issue in terms of greater enforcement relative to that injunctive provision that this Committee could also look at.

And I think all four of you have indicated that you support a private right of action in the trade secret area, it certainly is something that I look forward to working with my colleagues on both sides of the aisle on.

If one is created, when would it be appropriate for a company to go into Federal court, and in what instances would you envision companies taking advantage of the State court remedies that will remain on the books?

Mr. HERTLING. Well, I think obviously for a company to get into Federal court in the first instance, there would have to be at a minimum an interstate nexus, an effect on interstate commerce and certainly an effect with—instances in which there is an international nexus.

Otherwise it would be left to the—the choice of forum would be left typically to the plaintiff, and I think it would depend on the particular circumstances if there is—in an interstate or international case, if the concern is the thief absconding with the information physically, it probably is a benefit to file in Federal court, because the process that would be issued by Federal court could be enforced by a U.S. Marshal anywhere, whereas if you go into the State court, the process issued by a justice of Kings County Supreme Court, for example, doesn't mean anything to a sheriff executing a process in California.

So whereas the U.S. Marshal in San Francisco would enforce an order of a Federal District Judge from the Eastern District of New York, just as he would process issued by a Judge of the U.S. District Court for the Northern District of California, but if the matter is one in which the mis-appropriator absconds from Brooklyn to Staten Island, you probably wouldn't need to go to Federal court. It is a question whether you could. If he absconds to New Jersey,

it would be up to the plaintiff to decide what the best forum is, and the factors would be the ease of relief, the comfort with the judiciary in the location.

So there would be nothing in a Federal civil remedy that would preempt state law or preclude the plaintiff in choosing the forum in which to file.

Mr. JEFFRIES. Thank you.

I yield back.

Mr. COBLE. I thank the gentleman.

The distinguished gentleman from Pennsylvania, Mr. Marino, is recognized.

Mr. MARINO. Thank you, Chairman.

Gentlemen, I am pretty much a States rights guy and the less Federal Government in my life, the better. Tell me what, and anyone can speak to this. Tell me what requires fixing? Why do we need the Federalization here?

Mr. HERTLING. Well, I think initially, as I mentioned to Mr. Jeffries, one of the things that needs fixing is, of course, each State enforces the judicial process issued by the judges of that particular State, and process issued by a judge in Pennsylvania is typically not going to be enforced by a sheriff in California. So if you have a big company in Harrisburg and somebody walks out with a thumb drive with some important trade secrets and drives from the facility, gets on a plane and flies to San Francisco, and from San Francisco, he is going to abscond to Beijing, if the owner of that business finds out that the person has walked out with a trade secret, he runs to common pleas court in Gotham County, the judge is going to issue process.

You get that process out to the San Francisco sheriff, and the sheriff in San Francisco who's going to—because you are looking to seize the thumb drive.

Mr. MARINO. I was reading some cases preliminarily just before I got here. And let's take, for example, the international court of justice gets involved. I think there was a case that—a case, a preliminary case that started out in one of the States here in the U.S. and it involved Canada, and I am—are you familiar with this case that I am talking about? And—

Mr. HERTLING. I am not. I was under the impression that the ICJ only heard cases between sovereigns, so I—but I am not an expert in international law.

Mr. MARINO. Also the U.S. Federal court stepped in and raised an issue about a State having a right to hand down the decision that pertained to another country, and I am thinking it was Canada. Have you heard of that? I am trying to get more information on that explanation.

Mr. HERTLING. I am—

Mr. MARINO. Is anyone else familiar with it?

Mr. HERTLING. I am not—

Mr. MARINO. I will do some research on it, then.

Mr. HERTLING. I am not familiar with it, but again, I think it is important that nothing—obviously there is no House bill that has been introduced yet, a broader bill, Ms. Lofgren, of course, has a barebones bill. So this would be something that the House would take and create, but nothing, say, in the bill that has been intro-

duced in the Senate would preempt State law, foreclose the ability to go into State Court. This is a—a Federal remedy would be a complement to the existing State Court remedies, but not a replacement for them.

Mr. MARINO. Do you only get one bite at either or—or a venue? If you lose in one, can you go to the other?

Mr. HERTLING. Well, typically, obviously, unless it is a criminal case where you have—you know, the dual sovereign doctrine applies, but in the civil litigation context, you would generally have claim preclusion so that if you lose in—if you lose on those issues or issues that you could have raised in a previous suit, and you go to a different court, whether State or Federal, you are precluded if there is identity of parties between the two suits.

Mr. MARINO. Mr. Simon, you have raised an issue, but I am sorry, I have been going in and out meeting with people, on seizure. Could you repeat that again for my benefit that I may not have heard concerning your concern with seizure?

Mr. SIMON. Sure. I would be happy to. So we have a lot of people's data in our systems. That data, because of the way our security algorithms and others mix, work, the data between the customers is mixed together. There is no one disk drive for any one customer, generally speaking. There are some exceptions, to be clear.

The point being that under the current—some of the current proposals, the ability to come in and seize physical property would permit somebody to say, we think there is a mis-appropriator's information here, go get that physical drive. That is the issue that we are concerned about.

Mr. MARINO. All right. Thank you.

I see my time has expired and I yield back. Thank you.

Mr. COBLE. I thank the gentleman.

This concludes today's hearing. I appreciate those of you in the audience who stayed with us. Particularly appreciate the panelists for your contributions.

Without objection, all Members will have 5 legislative days to submit a written—additional written questions for the witnesses or additional materials for the record. This hearing stands adjourned.

[Whereupon, at 4:38 p.m., the Subcommittee was adjourned.]