INVESTIGATING AND PROSECUTING 21ST CENTURY CYBER THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MARCH 13, 2013

Serial No. 113–14

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

79–878 PDF WASHINGTON : 2013

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
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVE CHABOT, Ohio
SPENCER BACHUS, Alabama
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
MARK AMODEI, Nevada
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
GEORGE HOLDING, North Carolina
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
KEITH ROTHFUS, Pennsylvania

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
JOE GARCIA, Florida
HAKEEM JEFFRIES, New York

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

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

HOWARD COBLE, North Carolina
SPENCER BACHUS, Alabama
J. RANDY FORBES, Virginia
TRENT FRANKS, Arizona
JASON CHAFFETZ, Utah
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho

ROBERT C. "BOBBY" SCOTT, Virginia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MARCH 13, 2013

INVESTIGATING AND PROSECUTING 21ST CENTURY CYBER THREATS

WEDNESDAY, MARCH 13, 2013

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Subcommittee met, pursuant to call, at 11:35 a.m., in room 2237, Rayburn Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee), presiding.

Present: Representatives Sensenbrenner, Goodlatte, Gohmert, Coble, Forbes, Franks, Chaffetz, Gowdy, Scott, Conyers, Chu, and Richmond.

Staff present: (Majority) Caroline Lynch, Chief Counsel; Sam Ramer, Counsel; Alicia Church, Clerk; (Minority) Bobby Vassar, Minority Counsel, and Joe Graupensperger, Counsel.

Mr. SENSENBRENNER. Because the President is coming to address the Republican Conference of the House, this hearing will end at 1:00 sharp. So would everybody please make note of that and judge their time accordingly?

I would like to welcome everybody to the first hearing of the Subcommittee, acknowledge the Ranking Member, the gentleman from Virginia, Mr. Scott, and also welcome the full Committee Chair, Mr. Goodlatte.

Today's hearing will investigate our focus on how America investigates and prosecutes 21st century cyber threats. The United States has been the subject of the most coordinated and sustained computer attacks the world has ever seen. Rival nations, particularly China, have been invading corporate computer systems and stealing intellectual property at an increasing rate.

Spying between governments has always been a fact of life, but in the digital age the spying is more pervasive and harder to guard against. The systematic and strategic theft of intellectual property by foreign governments threatens one of America's most valuable commodities, our innovation and hard work.

In 2011, the American Superconductor Corporation supplied sophisticated software for wind turbines to Sinovel, a giant Chinese wind turbine corporation. When American engineers went to China to repair a wind turbine, they discovered that Chinese wind turbines were already using a stolen version of the American software.

Worse, the Chinese company had complete access to the American company's proprietary source code. Because they possessed this important code, the Chinese did not need the American Superconductor Corporation anymore.

A few months later, Sinovel abruptly began turning away shipments. On April 5, 2011, the American Superconductor Corporation had no choice but to announce that Sinovel, its biggest customer, accounting for more than two-thirds of the company's $315 million in revenue in 2010, had stopped making purchases. The result for the American company: investors fled, erasing 40 percent of the company's value in a single day, and 84 percent of its value by September 2011.

This week, the Obama Administration has finally increased public pressure on Chinese cyber spying. On Monday, the President's national security advisor announced what the media has called the White House's most aggressive response to a series of military-style hacks of American corporations. Describing the problem as a key point of concern in discussion at all levels of government, Mr. Donilon said Beijing should take serious steps to investigate and put a stop to these activities. I agree.

The fact that such mild comments have been termed the Administration's most aggressive ever may be part of the problem. When one country decides to advance its economy by stealing our intellectual property, we must do more than simply ask Beijing to investigate. Make no mistake. Sinovel stole hundreds of millions of dollars from the American Superconductor Corporation. This is a company that received over $20 million in stimulus money from U.S. taxpayers. But far from demanding our $20 million, the Administration's strongest rebuke has been to ask that Beijing take serious steps to investigate.

We simply cannot outsource the fight against cybercrime to international diplomacy. The theft of valuable intellectual property is a serious strategic threat to the American economy, and it must be treated as such by U.S. law enforcement.

Congress has repeatedly addressed the issue of cybercrime. In 2000 or in 1986, Congress implemented the Computer Fraud and Abuse Act as a tool for law enforcement to combat computer crimes. As computer crimes continue to evolve, so, too, has the CFAA, which Congress has amended eight times since its enactment. It may be time for Congress to augment and approve the CFAA and other criminal statutes to enable law enforcement to combat international criminal enterprises.

The Administration has taken initial steps to address the growing cyber threat. We applaud the Administration for its efforts, but it remains to be seen whether these steps will actually work.

Today the Committee will look at the criminal laws and investigative tools to combat cybercrime. We will determine what changes can be made to our criminal laws to more effectively combat and deter the cyberattacks we are enduring. We will discuss what protection can be provided for the privacy of Americans through data breach notification laws, and we will discuss what steps can be taken by this Committee to protect the intellectual property and sensitive government information that hackers in foreign governments seek to obtain.

As we saw from China's cyberattack on Google and other companies, America's edge in innovation and technical superiority can be compromised by competing countries that make theft of intellectual property a national strategy. I look forward to hearing more about this issue and thank all of our witnesses for participating in today's hearing.

It is now my pleasure to recognize for his opening statement the Ranking Member of the Subcommittee, the gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Chairman, because of our growing reliance on Internet and computer networks, I welcome today's hearing to examine the cyber threats we face and to discuss how we can better protect ourselves against them.

This hearing comes at a time when there's a rise in the disparity of cyber threats, and so an update of our computer crime statutes may have to be considered. It is critical that we work together on this effort with the Members of Congress, Administration, with the business community, and with private advocates to find ways to enhance the security of our government information systems, business computer systems, and our personal use of the Internet.

And while it is the job of Congress to evaluate and update our laws in response to changing circumstances, we have to be careful that any changes we make will actually improve the law, and not just ratchet up penalties in an exercise of sound bite politics. Often the problem is a lack of enforcement, investigation, and prosecution, and so penalties become irrelevant if a case is not even investigated in the first place.

This is particularly important in the case of the Computer Fraud and Abuse Act, a law whose breadth of scope and sometimes questionable application has already generated concern by citizens and narrowing by the courts. In the last Congress, we met to discuss many of these same issues, and the cyber threats of course remain an urgent issue of national economic and personal security. At that time, I raised concerns about one provision in the proposed law, and that was the mandatory minimum sentencing for certain crimes of damaging political critical infrastructure computers.

This Committee has heard a lot of testimony on mandatory minimums. They have been found to waste the taxpayers' money, do nothing about crime, and often result in sentences that are violative of common sense. This Committee has recently also focused on the issue of federalism, so we have to be concerned about whether the Computer Fraud and Abuse Act appropriately focuses on behavior that we all believe rises to the level of Federal criminal liability.

That statute was originally enacted to deal with intrusions into computers, what we now call hacking, and since that time we have extended the scope of the law on several occasions, which has led to expansive use in recent years, which have generated concerns on both sides of the aisle. I hope we can work together to address those concerns.

Mr. Chairman, we know that criminals target computers and cyber networks of individual companies and our government. That is why we have to enhance the protective measures that we take

at every level to prevent cyber intrusions. I applaud the President's resolve to work with industry to better resolve our critical infrastructure. His executive order will improve the sharing of information with industry and establish a framework for best practices to help companies step up cyber protection.

As in every area of crime policy, public safety demands that we engage in level-headed efforts to identify and implement comprehensive evidence-based solutions, and I hope we can do that in this case.

Before I close, Mr. Chairman, I ask unanimous consent that a letter signed by 20 Internet companies expressing their concerns about the scope of the current Computer Fraud and Abuse Act be entered into the record.

Mr. SENSENBRENNER. Without objection.

[The information referred to follows:]

March 12, 2013

Chairman Jim Sensenbrenner
House Subcommittee on Crime, Terrorism, and Homeland Security
Rayburn House Office Building B-370B
Washington, DC 20515

Ranking Member Bobby Scott
House Subcommittee on Crime, Terrorism, and Homeland Security
Rayburn House Office Building B-351
Washington, DC 20515

Dear Subcommittee Chairmen Sensenbrenner, Ranking Member Scott, and Members of the Committee,

We, a wide array of Internet innovators, write to support efforts led by Representative Lofgren to reform the Computer Fraud and Abuse Act. This issue is important to us not just because of the tragic death of Aaron Swartz, but because the CFAA chills innovation and economic growth by threatening developers and entrepreneurs who create groundbreaking technology.

We strongly believe in protecting our users' data from unauthorized access. We recognize that computer criminals and cyber-spies pose a serious threat to American companies, their property, and our national security. It is therefore crucial that federal laws deter and punish those who would maliciously attack U.S. computers and networks. But deterring digital criminals can be done without criminalizing harmless contractual breaches and imposing felony liability on developers of innovative technologies. In the nearly three decades since the CFAA's enactment, the law has lost its way.

This is primarily because the CFAA makes it illegal—a felony, potentially—to "obtain information" from virtually any computer "without" or "in excess of" authorization, but fails to explain what that means. Several prosecutors and courts have interpreted this vague language to render mere breaches of contractual agreements or policies, like website's terms of service, or legal duties, like those between employer and employee, a violation of the CFAA.[1] And at least one other court has found that taking minimal technological steps taken to ensure interoperability of web sites violates the CFAA.[2]

These interpretations of the CFAA give incumbent companies a dangerous and unfair weapon to wield against competitors and developers of innovations that build on existing services. And

[1] *See, e.g., EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001) (holding that breach of an employment-related confidentiality agreement exceeded authorized access under the CFAA); *United States v. Rodriguez*, 628 F.3d 1258, 1260-65 (11th Cir. 2010) (holding that defendant had exceeded authorized access under the CFAA when he accessed information in a Social Security Administration database in violation of SSA employee policy); *United States v. Drew*, 259 F.R.D. 449, 452-53, 467 (C.D. Cal. 2009) (rejecting prosecution argument that a defendant who violated a website's terms of service exceeded authorized access under the CFAA).
[2] https://www.eff.org/cases/facebook-v-power-ventures.

because the statute contains criminal penalties as well as civil remedies, prosecutors have the discretion to bring the full weight of harsh criminal penalties against innovators, too.

Some examples of where the CFAA has been, or could be, used to thwart innovation include:

- A large social networking company sued the creators of a tool that let users view, manage, and use multiple social networks on one screen, claiming the tools violated the CFAA and a similar California computer crime law. The tool allowed users to exchange private messages with any of their social networking friends through a single interface of their choice, rather than having to separately check their messages on Gmail, Twitter, and Facebook.[3]

- A major website used the CFAA to sue developers of a tool that let users automatically place apartment ads from numerous classified ad websites onto a mapping website and added content such as the price range for apartments in that area.[4]

- The CFAA threatens tools that help mobile users automatically fill out forms and otherwise interact with websites without having to type out their information on a tiny keyboard, when a website prevents this automated access either through terms of service or technically blocking the service. This threat can especially hurt the millions of Americans who have only mobile devices yet increasingly must use the Internet to seek employment and services.

Of course, the greatest loss for consumers may be unseen: the innovations that quietly died when their creators were threatened with CFAA claims by more established competitors, or innovations that never emerged because developers or investors feared potential CFAA liability. Nothing chills ingenuity like the shadow of felony charges for tools that harm no one.

Other existing laws recognize the importance of permitting reverse-engineering and interoperability. For instance, U.S. copyright law has long considered the copying of computer code necessary to build an interoperable computer program to be fair use. This change arose out of attempts by companies like Sony and Sega to stop competitors from building interoperable games and consoles.[5] Similarly, the Digital Millennium Copyright Act's anti-circumvention provisions contain a specific exception that allows reverse engineering to achieve interoperability even if it circumvents a technological protection measure protecting a copyrighted work.[6] The DMCA is not perfect, but this exception reflects Congress's recognition that technological barriers can be misused as anticompetitive barriers to entry by incumbents threatened by innovative ideas.

Many of today's best-known innovators—from Steve Jobs and Steve Wozniak to Paul Allen and Bill Gates to Mark Zuckerberg—could have likely been prosecuted under overly broad computer

---

[3] https://www.eff.org/cases/facebook-v-power-ventures. The case was civil, not criminal, but the CFAA ties the two together so that, had a prosecutor wished to do so, he could bring a criminal case for the same activity.
[4] http://gigaom.com/2012/07/24/craigslist-sues-competitor-padmapper-over-listings/
[5] *See Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992).
[6] 17 U.S.C. § 1201(f).

crime laws like the CFAA when they were young, simply for doing what innovators do: pushing boundaries.[7] The point is not that everything they might have done should necessarily be legal, but that stepping over the line should not trigger the draconian penalties that the CFAA currently carries. We therefore urge Congress to amend the CFAA to ensure it does not chill the development of innovative and interoperable software and services. We believe that this should be accomplished by:

1) ensuring that violation of terms of service, contractual agreements or other legal duties do not violate the statute;

2) protecting technical steps necessary for interoperability and innovative means of access and;

3) fixing the statute's penalty scheme so that the punishment better fits the crime, including making sure that prosecutors can't double-charge for the same conduct and ensuring that felony punishments only apply to most egregious behavior.

Sincerely,

Internet Infrastructure Coalition (i2Coalition)
Engine Advocacy
O'Reilly Media
Reddit
OpenDNS
Stack Exchange
PadMapper
heyzap
Agile Learning Labs
Vuze
#sfbeta
ZeroCater
Vidmaker
4Chan and Canvas
Notcot Inc.
The Lewis Charitable Foundation
Get Satisfaction
VigLink
Zemamai
American Library Association

cc: Members of the House Committee on the Judiciary

[7] Jobs and Wozniak: http://www.kottke.org/10/09/woz-and-jobs-phone-phreaks; Allen and Gates: http://www.v3.co.uk/v3-uk/news/2044825/paul-allen-spills-beans-gates-criminal-past; Zuckerberg: http://www.businessinsider.com/how-mark-zuckerberg-hacked-into-the-harvard-crimson-2010-3; generally: http://www.newyorker.com/online/blogs/newsdesk/2013/01/everyone-interesting-is-a-felon.html.

Mr. SENSENBRENNER. And it is now my pleasure to recognize for his opening statement the Chairman of the full Committee, the gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman. I very much appreciate your holding this hearing, and I will submit my full statement for the record in order to save a little time for our witnesses. But I do want to make a few points.

First of all, yesterday, and I would submit these for the record, the Secret Service launched an investigation of the alleged hacking of private information of Vice President Joe Biden, First Lady Michelle Obama, FBI Director Robert Mueller, Attorney General Eric Holder, and many others. And the President yesterday also acknowledged that hacking of personal data is a big problem.

Mr. SENSENBRENNER. Without objection, the material will be entered.

[The information referred to follows:]

POLITICO

Obama on hacking of personal data: 'It is a big problem'

By JENNIFER EPSTEIN |
3/12/13 6:48 PM EDT

President Obama wouldn't confirm Tuesday whether hackers had accessed his wife's credit records, but did acknowledge that online tampering is a serious problem.

"I'm not confirming that that's what happened," he told ABC News hours after federal investigators began probing **an alleged hacking (http://www.politico.com/politico44/2013/03/feds-launch-investigation-of-alleged-hacking-of-joe-159116.html)** that may have compromised credit reports of first lady Michelle Obama, Vice President Joe Biden and other high-profile government officials – plus some big-name celebrities.

"We should not be surprised that if you've got hackers who want to dig in and devote a lot of resources, that they can access peoples' private information," he said. "It is a big problem."

He added: "You've got websites out there right now that sell peoples' credit cards that have been stolen."

POLITICO

Feds launch investigation of alleged hacking of Joe Biden, Michelle Obama financial info

By DONOVAN SLACK and JENNIFER EPSTEIN |
3/12/13 2:59 PM EDT

The Secret Service has launched an investigation of the alleged hacking of private information for Vice President Joe Biden, first lady Michelle Obama, FBI Director Robert Mueller and Attorney General Eric Holder, along with a dozen big-name stars from Hollywood and the music world.

Hackers posted what they claim to be personal information, such as credit reports, home addresses and telephone numbers on what appears to be a Russian web site.

"We will confirm Secret Service is investigating the matter," spokesman Brian Leahy told POLITICO. "We cannot comment further as it is an ongoing investigation."

Credit agency Equifax launched an internal investigation Tuesday after determining that four accounts on AnnualCreditReport.com had been accessed through "fraudulent and unauthorized" activity. The firm didn't release the names of the people whose accounts had been hacked.

The hackers claimed to have posted information about 17 people, including Kim Kardashian, Hillary Clinton, LAPD Chief Charlie Beck, Mel Gibson, Ashton Kutcher, Jay-Z, Beyoncé, Paris Hilton, Britney Spears, Sarah Palin, Hulk Hogan, Donald Trump, Arnold Schwarzenegger, and Al Gore.

Some of the information is very limited. The file on Trump, for example, shows only home addresses, while those for Obama, Holder and Mueller purport to show their full credit reports with addresses, accounts, phone numbers and social security numbers. Biden's includes a social security number, phone number and home addresses. It's unclear how much, if any, of the information is real.

Mr. GOODLATTE. Thank you. But that is just the beginning of this problem. Cyber intrusions are just the tip of the iceberg. In November 2011, the National Counterintelligence Executive, the agency responsible for countering foreign spying on the U.S. government, issued a report that hackers and illicit programmers in China and Russia are pursuing American technology in industrial secrets jeopardizing an estimated $400 billion dollars in U.S. research spending.

According to the report, China and Russia view themselves as strategic competitors of the United States, and are the most aggressive collectors of U.S. economic information and technology.

Further, in January of this year, the New York Times reported it is has been the victim of a sustained cyberattack by Chinese hackers. Shortly afterward, the Wall Street Journal and Washington Post also reported they, too, had been breached by similar sources. The Times commissioned a report from Mandiant, a private investigative agency which traced the cyberattacks to a unit of the Chinese People's Liberation Army. According to the report, the Chinese are engaged in massive cyber spying on the American industrial base and in areas the Chinese are trying to develop for their own national purposes.

Earlier this year, the Administration issued a cybersecurity executive order and presidential directive aimed at helping secure America's cyber networks. The executive order is a first step toward protecting our public and private networks from attack, but Congress can and must do more. The Judiciary Committee is responsible for ensuring that our Federal criminal laws keep pace with the ever-evolving cyber landscape. Our challenge is to create a legal structure that protects the invaluable government and private information that hackers seek to exploit while allowing the freedom of thought and expression that made this country great.

I would submit the rest of my statement for the record, and I thank the Chairman.

[The prepared statement of Mr. Goodlatte follows:]

Prepared Statement of the Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary

Thank you, Chairman Sensenbrenner.

The 21st century has brought us a more connected, inter-dependent world. The Internet and portable computer systems make it possible for people, businesses and governments to interact on a global level never seen before.

The United States, with its bounty of personal freedom and free enterprise, is a leader in advancing the technology that enables us to stay in touch almost everywhere with almost everyone.

However, our technological advancement also makes the United States increasingly vulnerable to cyber attacks—from routine cyber crimes to nation-state espionage. Earlier this week, we all heard about the high profile cyber breach that exposed sensitive personal and financial information about high-ranking government officials and celebrities from FBI Director Mueller and Attorney General Holder to Beyonce and Donald Trump. The truth is that all citizens are vulnerable to these kinds of cyber attacks.

We are also currently experiencing a profound cyber-spying conflict on the nation-state level. Most Americans are familiar with the Wikileaks case, which resulted in the public disclosure of hundreds of thousands of secret State Department cables. And many of us are familiar with the cyber attack on the Chamber of Commerce, in which Chinese hackers gained access to the files on the Chamber's 3 million member companies.

But these cyber intrusions are just the tip of the iceberg. In November, 2011, the National Counterintelligence Executive, the agency responsible for countering foreign spying on the U.S. government, issued a report that hackers and illicit programmers in China and Russia are pursuing American technology and industrial secrets, jeopardizing an estimated $398 billion in U.S. research spending. According to the report, "China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of U.S. economic information

and technology." The report drew on 2009–2011 data from at least 13 agencies, including the Central Intelligence Agency and the Federal Bureau of Investigation.

And in January of this year, the New York Times reported it has been the victim of a sustained cyber attack by Chinese hackers. Shortly afterward, the Wall Street Journal and the Washington Post also reported they too had been breached by similar sources. The Times commissioned a report from Mandiant, a private investigative agency, which traced the cyber attacks to a unit of the Chinese People's Liberation Army. According to the report, the Chinese are engaged in massive cyber spying on the American industrial base and in areas the Chinese are trying to develop for their own national purposes.

Earlier this year, the Administration issued a cyber security Executive Order and Presidential Directive aimed at helping secure America's cyber networks. The Executive Order is a first step towards protecting our public and private networks from attack. But Congress can and must do more. The Judiciary Committee is responsible for ensuring that our federal criminal laws keep pace with the ever-evolving cyber landscape.

Our challenge is to create a legal structure that protects the invaluable government and private information that hackers seek to exploit, while allowing the freedom of thought and expression that made this country great. One thing is clear: cyber attacks can have devastating consequences for citizens, private industry and America's national security and should be treated just as seriously as more traditional crimes by our criminal justice system.

The risks to our national infrastructure, our national wealth, and our citizens are profound, and we must protect them. We must not allow cyber crime to continue to grow and threaten our economy, safety and prosperity.

Mr. SENSENBRENNER. Without objection, the Ranking Member and Chairman Emeritus of the Committee, the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Sensenbrenner.

I would like to welcome the witnesses and note that I am reintroducing today a bill that I introduced in 2012, July or August, the Cyber Privacy Fortification Act, which will create a strong standard for data breach notification, which does not exist now, and is a great reason for us to be conducting this hearing. It requires a data breach activity to be made public, notified to us so that we can measure just what is going on.

Cyberattacks have increased, according to the National Security Agency, by 44 percent. And many of these attacks are perpetrated by criminals operating beyond our national boundaries, intent on stealing our intellectual property, assessing financial accounts, and compromising our critical infrastructure.

And so, we have got a problem here, and it is one that I think this Committee is perfectly suited to handle. And I would recommend, and I will be looking for discussion on this, the increasing collaboration necessary between the government and the private sector on cybersecurity, but not at the expense of the privacy of innocent citizens. We must not toss aside existing privacy restrictions to grant the government and law enforcement unwarranted access to private communications.

The Administration and others have called for private sector companies to be allowed to share communications in their possession for the purpose of protecting against cyber threats. We must require that any additional sharing only be allowed to occur if information is removed that can be used to identify persons unrelated to the cybersecurity threat itself.

And then in addressing a recent cybersecurity conference, FBI Director Mueller emphasized the law enforcement-focused need for this information is limited to threats and attacks, not other sensitive information about company secrets or customers. This must be the condition for enhancing collaboration between the government and the private sector to better secure our computer networks.

And finally, the Internet has made the world a smaller place, and because cyberattacks are often launched outside of our borders, now more than ever, we need a diplomatic engagement to increase cooperation between nations and cybersecurity issues. In other words, diplomacy is going to have a larger role in this activity.

I submit the rest of my statement, and I yield back to the Chairman.

Mr. SENSENBRENNER. Without objection, the rest of the statement will be included in the record.

[The prepared statement of Mr. Conyers follows:]

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary

Good morning. This hearing focuses on a topic that is very important to the country and this Committee.

Last year, the head of the National Security Agency warned that cyber attacks had increased by 44%. With the proliferation of these attacks, especially those perpetrated by criminals operating beyond our national boundaries intent on stealing our intellectual property, accessing financial accounts, and compromising our critical infrastructure, we must take additional steps to protect our cyber networks.

To start with, we need a strong national requirement for reporting data breaches. When a company has suffered a cyber attack that has resulted in the compromise of sensitive information of consumers, they should report the attack to law enforcement and notify affected consumers.

As it stands now, there are 47 different state laws with different data breach notice requirements. This often makes compliance more complex and difficult than it should be. A national standard should be strong enough to provide appropriate notice so that individuals may be on guard against any subsequent identity theft and law enforcement is able to investigate these intrusions.

That is why I am reintroducing my Cyber Privacy Fortification Act, which will accomplish this.

Next, we must increase collaboration between the government and the private sector on cyber security, but not at the expense of the privacy of innocent citizens. We must not toss aside existing privacy restrictions to grant the government and law enforcement unwarranted access to private communications. The Administration and others have called for private sector companies to be allowed to share communications in their possession for the purpose of protecting against cyber threats.

We must require that any additional sharing only be allowed to occur if information is removed that can be used to identify persons unrelated to the cyber security threat.

In addressing a recent cyber security conference, FBI Director Mueller emphasized that law enforcement's focused need for this information is limited to the threats and attacks, not other sensitive information about company secrets or customers. This must be the condition for enhancing collaboration between government and the private sector to better secure our computer networks.

Finally, now more than ever, we need diplomatic engagement to strengthen cooperation between nations on cyber security because the Internet has made the world a smaller place, and because cyber attacks are often launched from outside our borders. The interconnected nature of the Internet allows for communication

across all borders, but also allows some cyber criminals to hide from prosecution behind international boundaries.

Even if we improve our domestic computer crime laws, those laws are only as effective against international criminals as our ability to find, investigate, and prosecute them.

The State Department and our federal law enforcement agencies must take steps to reinforce international relationships so that their foreign colleagues enhance their capabilities to find and preserve evidence of cyber crime, extradite criminals to the United States, and prosecute these criminals in their own courts when extradition is not possible.

I commend the Crime Subcommittee for discussing this issue, and with these thoughts in mind, we can better protect our cyber networks from intrusion while protecting our civil liberties and preserving the openness of the Internet.

Mr. SENSENBRENNER. And without objection, all Members' opening statements will be included in the record.

We have a very distinguished panel today, and I will begin by recognizing the gentlewoman from Washington, Ms. DelBene, who will introduce the first witness.

Ms. DELBENE. Thank you, Mr. Chair. It is my pleasure to introduce Jenny Durkan. Ms. Durkan currently serves as the United States attorney for the Western District of Washington, where my district is located. She is the top Federal law enforcement officer of 19 counties in western Washington. She was nominated by President Obama in May of 2009 and was confirmed by unanimous vote of the U.S. Senate on September 29 of 2009.

Ms. Durkan chairs the Attorney General's Advisory Subcommittee on Cybercrime and Intellectual Property Enforcement. She is also a member of three other subcommittees: Terrorism and National Security, Civil Rights, and Native American Issues.

Ms. Durkan is a Seattle area native who grew up in Issaquah, Washington, graduated from the University of Notre Dame, and received her law degree from the University of Washington.

Thank you, Mr. Chair.

Mr. SENSENBRENNER. Before recognizing you, Ms. Durkan, let me introduce the rest of the members of the panel.

Mr. Boles currently serves as the deputy assistant director for the cyber division of the FBI, where he oversees FBI cyber operations and investigations.

He entered on duty with the FBI in Sacramento in 1995, where he successfully investigated an Internet Ponzi scheme that defrauded 15,000 victims in 57 countries. In 2009, as assistant special agent in charge of the San Diego Division, he oversaw six investigative squads over cyber and white-collar crime matters, as well as directing the administrative program from the office.

Mr. Boles was a legal attaché? to Kiev, Ukraine in 2003, where he successfully facilitated the first extradition from Ukraine to the United States. He served as the special assistant director, national security branch, and in 2011 was selected as the special agent in charge of the Norfolk FBI office.

He is a graduate of the University of Georgia.

Mr. Robert Holleyman serves as president and CEO of BSA, the Software the Alliance. He was also appointed by President Barack Obama to serve on the Advisory Commission for Trade Policy and

Negotiations, the principle advisory Commission for the U.S. government on trade matters. He oversaw an innovative study of cloud computing-related policies around the world, and is an advocate for breaking down barriers that cloud providers face when they do business internationally. He also was an early proponent for policies that promote the widespread deployment of security technologies and to build public trust and confidence in cyber space.

He has testified before Congress, the European Commission, the World Intellectual Property Organization, and other governing bodies on technology, trade, and economic matters. He previously served as a counselor and legislative advisor in the Senate, an attorney in private practice, then a judicial clerk in the U.S. District Court.

He holds a bachelor's degree from Trinity University in San Antonio, where he was named distinguished alumnus in 2012, and received his law degree from Louisiana State University. He completed the Stanford Executive Program at the Stanford Graduate School of Business.

Professor Orrin Kerr is a professor law at George Washington University, where he teaches criminal law, criminal procedure, and computer crime law. Before joining the faculty in 2001, Professor Kerr was an honors program trial attorney in the Computer, Crime, and Intellectual Property section of the criminal division at the Department of Justice, as well as the special assistant U.S. attorney for the Eastern District of Virginia.

He is a former law clerk for Justice Anthony Kennedy of the U.S. Supreme Court and Judge Leonard Garth of the U.S. Court of Appeals for the 3rd Circuit. In the summer of 2009 and '10, he served as special counsel for the Supreme Court nominations to Senator John Cornyn and the Senate Judiciary Committee. He has also been a visiting professor at the University of Chicago Law School and the University of Pennsylvania Law School.

He received his bachelor of science degree in engineering from Princeton, master of science from Stanford, and earned his juris doctor from Harvard Law School.

Now, each of the witnesses' written testimony will be entered into the record in its entirety, and I ask that each witness summarize his or her testimony in 5 minutes or less. And I am going to be kind of like the chief justice given the time constraints that we have with the President coming. So when the little red light appears before you, time is up.

So we will start with you, Ms. Durkan.

TESTIMONY OF JENNY S. DURKAN, UNITED STATES ATTORNEY, WESTERN DISTRICT OF WASHINGTON, U.S. DEPARTMENT OF JUSTICE

Ms. DURKAN. Thank you. Good afternoon, Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee. Thank you for the opportunity to testify before you this afternoon regarding the investigation and prosecution of cyber threats to our Nation. I want to thank Congresswoman DelBene for the introduction and for her service to our district.

As United States attorney, I see the full range of threats to our communities and to our Nation. Few things are as sobering as the daily cyber threat briefing I receive.

Technology is changing our economy and our daily lives. We have witnessed the rapid growth of wonderful companies, lifesaving technologies, and the way we connect with others. Unfortunately, the good guys are not the only innovators. We have also seen growth in the number and the sophistication of bad actors exploiting the new technology. Financially motivated international rings have stolen large quantities of personal data. Criminal groups develop tools and techniques to disrupt and damage computer systems. State actors and organized criminals have demonstrated the desire and the capability to steal sensitive data, trade secrets, and intellectual property.

One particular area of concern is computer crime that invades the privacy of individual Americans. Every day, criminals hunt for our personal and financial data, which they use to commit fraud or to sell to other criminals. Hackers perpetrate large-scale data breaches that leave hundreds of thousands, if not millions, susceptible to identity theft.

The national security landscape has evolved dramatically in recent years. Although we have not yet experienced a devastating cyberattack against our critical infrastructure, we have been victim to a range of malicious cyber activities that siphon off valuable economic assets and threaten our Nation's security. There can be doubt. Cyber threat actors pose significant risks to our national security and our economic interests.

Addressing those complex threats requires a unified approach that incorporates criminal investigative and prosecutorial tools, civil and national security authorities, diplomatic tools, public-private partnerships, and international cooperation. Criminal prosecution, whether here in the United States or by a partner country plays a central and critical role in this collaborative effort. We need to ensure that throughout the country members of the Department of Justice who are actively working on these threats have the investigative resources and forensic capabilities to deal with these challenges, and we appreciate the support this Committee has given in this regard.

To meet these challenges, the Department has organized itself to ensure that we are in a position to aggressively investigate and prosecute cybercrime wherever it occurs. The criminal division's Computer Crime and Intellectual Property Section works with a nationwide network of over 300 Assistant United States Attorneys designated as our computer hacking and intellectual property prosecutors. They lead our efforts in this area.

Similarly, the Department's National Security Division is organized to ensure that we are aggressively investigating national security cyber threats through a variety of means. These include counterespionage and counterterrorism investigations and prosecutions.

Recognizing the diversity of the national security cyber threats and the need for a coordinated approach, the Department established last year a National Security Cyber Specialist Network. It brings together the Department's full range of expertise on national

security-related cyber matters, drawing on experts from the National Security Division, the Criminal Division, U.S. attorney offices, and other department components to make sure that we have a centralized resource for prosecutors and agents around the country.

Our efforts have led to a number of enforcement successes, two of which I will highlight later. But I will say that in our district we have been able to bring these prosecutions very successfully, and have made a difference for our citizens and for our businesses.

Thank you.

[The prepared statement of Ms. Durkan follows:]

Department of Justice

STATEMENT OF
JENNY S. DURKAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF WASHINGTON

BEFORE THE
COMMITTEE ON JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED:
"INVESTIGATING AND PROSECUTING 21ST CENTURY CYBER THREATS"

PRESENTED
MARCH 13, 2013

Statement of
Jenny S. Durkan
United States Attorney
Western District of Washington

Committee on Judiciary
Subcommittee on Crime, Terrorism, Homeland Security, and Investigations
United States House of Representatives

"Investigating and Prosecuting 21st Century Cyber Threats"
March 13, 2013

Good afternoon, Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee. It is an honor to appear before you to testify about investigating and prosecuting cyber threats to our nation. I am pleased to share with the Subcommittee an overview of the Department of Justice's role in the U.S. Government's overall investigative strategy and enforcement efforts as it relates to cyber. The Department also has some legislative concepts that would enhance our ability to address these threats. I will provide more detail later in my remarks. The Department's approach on cybercrime is rooted in three interests: 1) deterring, disrupting, and dismantling the threat; 2) holding bad actors accountable; and 3) protecting our national security, economic interests, and individual privacy.

As United States Attorney, I see the full range of threats our communities and nation face. Few things are as sobering as the daily cyber threat briefing I receive. Cyberspace is the new frontier. We have witnessed the rapid creation of incredible businesses, lifesaving technologies, and new ways to connect society. Unfortunately, the "good guys" are not the only innovators. We have seen a significant growth in the number and nature of bad actors exploiting new technology. As Attorney General Holder has noted, "[f]rom criminal syndicates, to terrorist organizations, to foreign intelligence groups, to disgruntled employees and other malicious intruders, the range of entities that stand ready to execute and exploit cyber attacks has never been greater." Threats to the nation's computer networks and cyber systems continue to evolve, as the nature and capabilities of those responsible for the threats evolve. Over the last several years, investigators and prosecutors have seen significant increases in the skills of threat actors and the complexity of their organizations. These actors have a variety of aims and motivations. For instance:

- Financially motivated groups working closely and easily across national boundaries have stolen large quantities of personal data. These criminals coalesce in forums where they barter individual skills to create ad hoc criminal networks with a power and reach sometimes approaching that of traditional transnational organized crime networks.

- Criminal groups have also developed tools and techniques for disrupting and sometimes damaging computer systems. Motivations run from profit to politics, but their motivations do not change the damage incurred by users and our economy.

- State actors and organized criminal groups have demonstrated the desire and the capability to steal sensitive data, trade secrets, and intellectual property for military and competitive advantage. Whether through remote attacks or insider threats, such thefts pose significant risk to our national security and economic interests.

- Malicious actors are now seeking to exploit the computer networks that control our critical infrastructure.

Responding to these threats requires a multi-faceted approach, including diplomacy and public-private partnerships. The Department, acting with its law enforcement components and in partnership with other agencies, plays a critical role by identifying the offenders, seizing their hardware and assets, and deterring their conduct through, among other things, indictment, arrest, prosecution, and appropriate punishment. In doing so, the Department works closely with other agencies and private sector entities to reduce vulnerabilities. Stated another way, we need to develop better locks, but when those locks are broken—as they inevitably will be—the Department responds to bring the offenders to justice.

Our reliance on technology requires that we take action to protect not only the information infrastructure itself, but the data it carries and activity that it supports. The Administration is committed to integrating and organizing the government's cybersecurity efforts to better ensure that we have a comprehensive framework in place that will allow us to bring all of our collective tools to bear in the fight against cyber criminals, terrorists, and other adversaries. The Department of Justice plays a key role in that fight.

Nature of the Threat

Ten years ago, many of the threats to the burgeoning Internet came from solo hackers, writing viruses like "I love you" or "Melissa," or crafting denial of service attacks on fledgling Internet companies. As bothersome as those attacks were, the threats today are much more significant. We face the challenges of organized crime, botnets (i.e., a collection of compromised computers under the remote command and control of a criminal or foreign adversary), identity theft, and carding, to name just a few. Many of these threats originate overseas.

However, we face significant challenges in attributing the origin of these threats. The tools used to commit serious cyber theft and damage are not only wielded by those with large-scale development resources. Instead, using widely available tools, individuals or small groups can steal huge quantities of sensitive data, damage key computer systems, or silence those who disagree. Financial gains from these crimes can, in turn, be used to build larger networks and buy protection from foreign government officials. As a result, U.S. investigators working to determine the source and nature of a cyber threat often do not know at the outset whether an

attack was mounted by an individual acting alone, an organized criminal or terrorist group, or a hostile nation.

Every day, criminals hunt for our personal and financial data so that they can use it to commit fraud or sell it to other criminals. The technology revolution has facilitated these activities, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Skilled hackers are now able to perpetrate large-scale data breaches that leave hundreds of thousands—and in many cases, tens of millions—of individuals at risk of identity theft. Today's criminals can remotely access the computer systems of universities, merchants, financial institutions, credit card companies, and data processors to steal large volumes of personal information—including financial information. As I explain below, we are working hard to address these threats to personal information.

The most significant threats are continuing to evolve, and now increasingly include threats to corporate data. A 2011 report from McAfee and Science Applications International Corporation confirms this trend in cybercrime. According to this report, which was based on a survey of more than 1,000 senior IT decision makers in several countries, "high-end" cyber criminals have shifted from targeting credit cards and other personal data to the intellectual capital of large corporations. This includes extremely valuable trade secrets and product-planning documents.

These threats come both from outside hackers as well as insiders who gain access to critical information from within companies and government agencies. Trusted insiders pose particular risks. Those inside U.S. corporations and agencies may exploit their access to funnel information to foreign nation states. And once the enemy is inside the gates, external defense can only provide limited protection. The Justice Department has successfully prosecuted corporate insiders and others who have obtained trade secrets or technical data from major U.S. companies and routed them to other nations via cyberspace.

The massive proceeds from these online crimes create another troubling issue. It is too soon to say where that money ends up, but the risk that it is being used to influence foreign governments, distort foreign justice systems, and fund terrorists cannot be ignored.

The national security cyber threat picture has similarly undergone a dramatic evolution in recent years. Although we have not yet experienced a devastating cyber attack against our critical infrastructure, we have been victim to a range of malicious cyber activities that are siphoning off our valuable economic assets and threatening our nation's security. Nevertheless, these cyber threats are growing, and make the threat of cyber-generated physical attacks, like those that might disrupt the power grid, appear no longer to be the stuff of science fiction. Leaders in our national security community have discussed the cyber threat we face, predicting that it "will pose the number one threat to our country" in "the not too distant future." Accordingly, just as the Department realigned its counterterrorism efforts after 9/11, we are realigning our cyber efforts to meet this challenge.

The national security cyber threats we face are as varied as the actors who carry them out. While details about most of the state-sponsored intrusions remain classified, the Intelligence Community has publicly noted that "entities within China and Russia are responsible for extensive illicit intrusions into US computer networks and theft of US intellectual property." Indeed, "Chinese actors are," according to a 2011 public report of our top counterintelligence officials, "the world's most active and persistent perpetrators of economic espionage." Secretary of Defense Panetta has stated that "Iran has also undertaken a concerted effort to use cyberspace to its advantage."

Cyber-enabled terrorism poses another major national security cyber threat. While terrorists have not yet used the Internet to launch a full-scale cyber attack against the United States, they have exhorted their followers to engage in cyber attacks on America. Last year, an al-Qaeda video released publicly by the Senate Homeland Security Committee encouraged al-Qaeda followers to engage in "electronic jihad" by carrying out cyber attacks against the West.
Terrorists have already gone beyond using cyberspace to spread propaganda and recruit followers. They have used cyberspace to facilitate operations. The individuals who planned the attempted Times Square bombing in May 2010, for instance, used public web cameras for reconnaissance, file sharing sites to share operational details, and remote conferencing software to communicate.

Addressing these complex threats requires a unified approach, one that incorporates criminal investigative and prosecutorial tools, civil and national security authorities, diplomatic tools, public-private partnerships, and international cooperation. Criminal prosecution, whether in the United States or a partner country, plays a central and critical role in this collaborative effort. While prosecution is not the appropriate approach for every threat that affects the United States, identifying and understanding the threat will very often involve the use of criminal investigative tools and methods.

Role of the Department of Justice

A key part of the nation's overall cybersecurity effort is the investigation and prosecution of cyber criminals – be they financially motivated actors, hackers, terrorists, or state actors. Our goal is to stop or deter these actors before they can complete an attack on our networks, or to punish and deter similar acts in the future if a successful intrusion has already occurred. Many Department of Justice components—including the Criminal and National Security Divisions and United States Attorneys offices across the country—are actively working to counter these threats.

These cases can be complex to investigate and prosecute. We need to ensure we have the investigative expertise and forensic capabilities needed to meet the challenge. We appreciate the support this committee has given in this regard. Almost every federal case prosecuted now involves an increasing volume of digital evidence, sometime scattered over numerous devices and multiple online services. For example, in one recent case in our District, the target carried as many as 15 cell phones. Gathering, sifting, and analyzing digital evidence is an increasing challenge. Bad actors know how to hide their cyber tracks: evidence can disappear with a few

key strokes, or through malicious code set as a booby trap. Moreover, large cyber cases frequently involve multiple players in multiple states and countries. One significant case can require multiple agents several years to investigate. Obtaining evidence from foreign countries – even those that are strong allies – can take time, delay, and require translating voluminous foreign language evidence.

To meet these challenges, the Department has organized itself to ensure that we are in a position to aggressively investigate and prosecute cybercrime wherever it occurs. The Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and a nationwide network of Assistant United States Attorneys (AUSAs), including nearly 300 AUSAs designated as Computer Hacking and Intellectual Property (CHIP) prosecutors lead our efforts to investigate and prosecute cybercrime offenses. These prosecutors, as well as other Assistant United States Attorneys (AUSAs) working cybercrime cases throughout the country, work closely with our law enforcement partners, including the FBI, the Secret Service, and the U.S. Postal Inspection Service. In addition, we have a strong partnership with the FBI's National Cyber Investigative Joint Task Force (NCIJTF), which brings together law enforcement, intelligence, and defense agencies to focus on high-priority cyber threats.

Other sections of the Criminal Division also play important roles in cybersecurity. The Fraud Section focuses on large-scale fraud cases involving identity theft. The Office of International Affairs (OIA) supports and enhances international cooperation efforts by expediting the sharing of critical electronic evidence with foreign law enforcement partners and by marshaling efforts to secure the extradition of international fugitives. Increasingly, large scale cyber cases involve actors from any number of foreign countries. International cooperation is critical and the work of OIA a key component of our success.

The Department's National Security Division (NSD) pursues national security cyber threats through a variety of means, including through counterespionage and counterterrorism investigations and prosecutions. The Counterespionage Section (CES) prosecutes, among other offenses, misappropriation of intellectual property to benefit a foreign government, as provided by the Economic Espionage Act of 1996 (18 U.S.C. § 1831), and obtaining national defense, foreign relations, or restricted data by accessing a computer without authorization, as provided by the Computer Fraud and Abuse Act (18 U.S.C. § 1030). The Counterterrorism Section (CTS)—leveraging the capabilities and expertise of CCIPS, the Anti-Terrorism Advisory Council, Joint Terrorism Task Forces, and others—would play a pivotal role in addressing any potential cybersecurity attack by terrorists or associated groups or individuals. NSD also provides the FBI, and the intelligence community in general, with extensive legal support on cyber issues.

Recognizing the diversity of national security cyber threats and the need for a coordinated approach to them, the Department established last year a nationwide network of National Security Cyber Specialists (referred to as the "NSCS network"). The network brings together the Department's full range of expertise on national security-related cyber matters, drawing on experts from NSD, the U.S. Attorney's Offices, CCIPS, and other DOJ components. This

network seeks to build on the successes of existing initiatives, including the CHIP network and the Anti-Terrorism Advisory Council. Each U.S. Attorney's office around the country has designated a point of contact for the National Security Cyber Specialists network. Last year, approximately 120 Assistant U.S. Attorneys and presenters convened in Washington, D.C. for a cyber training program to kick off the NSCS program.

The NSCS network now serves as a centralized resource for prosecutors and agents around the country. It is a one-stop shop within the Department for national security cyber intrusion activity. The network has focused the Department nationwide on opening more national security cyber investigations with an eye toward criminal prosecution. Through this network, we are bringing our best resources to bear against the problem—to enhance information sharing, ensure coordination, and leverage the Department's expertise in legal authorities and advice relating to national security cyber threats. Finally, we are using this network to do more outreach to the private sector and to enhance our joint work with the NCIJTF.

In addition to these efforts, the Department works closely with our partners throughout the government—including law enforcement agencies, the Intelligence Community, the Department of Homeland Security (DHS), Department of Commerce, and the Department of Defense—to provide legal support to cybersecurity efforts and inform policy discussions. The intersection between laws and technology can require complicated analysis and multidisciplinary training. That is why the Department has lawyers in the Criminal and National Security Divisions who are specially trained to handle cyber issues, ranging from the use of existing legal tools and authorities, the legality of cybersecurity programs like the EINSTEIN program, and the ways in which we can vigorously protect privacy, confidentiality, and civil liberties while still achieving our goal of securing the Nation's networks. Partnering with the National Science Foundation (NSF), through NSF's CyberCorps Scholarship for Service (SFS) program - which seeks to increase the number of qualified students entering the fields of information assurance computer security and to increase the capacity of the U.S. higher education enterprise to continue to produce professionals in these fields to meet the needs our increasingly technological society – the Department currently employees more than 40 SFS CyberCorps graduates, including 17 working for the Federal Bureau of Investigation.

For example, the Department is currently providing legal and policy support to the Department of Homeland Security in support of its cybersecurity mission and to the National Security Agency in support of its information assurance efforts. We are participating in government-wide planning and preparedness efforts, such as the development of the National Cyber Incident Response Plan and the associated Cyber Unified Coordination Group, which assists the Secretary of DHS in coordinating responsive measures to significant cyber incidents. We also participate in cyber exercises, such as 2012's National Level Exercise, and, along with other governmental partners, in reviewing the national security implications and vulnerabilities of certain foreign acquisitions of U.S. companies, including those with cyber-related capabilities.

Our work does not stop at our shores. Due to the global nature of the Internet, many of our cases involve computers and electronic evidence located in other countries. Many times the offenders are located in another country. But even U.S. criminals will use computers located in another country to hide their tracks. Often it is impossible to identify, arrest, and prosecute offenders without the assistance of foreign governments.

To assist us in preserving and obtaining data from other nations, the Department, with funding support from the Department of State Bureau for International Narcotics and Law Enforcement Affairs, has engaged in numerous efforts to enhance the ability of foreign governments to fight cybercrime, including:

- promoting the Council of Europe Convention on Cybercrime (2001);
- providing technical expertise to countries developing their legal frameworks relating to computer crime and electronic evidence;
- providing capacity building assistance for foreign law enforcement agencies; and
- promoting the 24/7 High-Tech Crimes Network of the G8, which is a network of points of contact designed to facilitate rapid law enforcement coordination across borders.

The profusion and diversity of cyber threats, and the challenges inherent in identifying and addressing them, highlight the need for a whole-of-government approach—an all-tools approach—to combating cyber threats. As Director Mueller has said, "We must be willing to use whatever legal means are available and appropriate—civil, criminal, or other means—to disrupt a particular threat—whether it be a terrorist threat or a cyber threat." Just as law enforcement and other legal tools have been critical in our efforts to combat organized crime, terrorist threats, and espionage, so too will they be critical to the deterrence and disruption of cyber threats.

Operational Successes

The relationships between the Department's prosecuting components and the federal investigative agencies, such as the U.S. Secret Service and the Federal Bureau of Investigation, and the robust cooperation and information sharing that they support, have led to a number of enforcement successes—just a few of which I would like to highlight here.

International, Multi-state Carding Ring – In my District, we prosecuted participants at all levels of an international credit card skimming ring from a Secret Service investigation. Christopher A. Schroebel, 21, of Keedysville, Maryland, obtained credit card information by hacking into vulnerable point of sale computers in small business operations across the country, including one in the Seattle area. Tens of thousands of people were victimized, and the investigation indicated that over 100,000 credit cards were compromised. David Benjamin Schrooten, 22, a Dutch citizen living in Romania sold the card numbers for a profit by advertising them on "carding websites." Charles Tony Williamson, 33, of Torrance, California, has also been charged with buying the card

numbers for his criminal group to use in multiple frauds. Schroebel was sentenced to seven years in prison, Schrooten received a twelve year sentence, and Williamson is awaiting trial.

Prolific Identity Thief and Hacker Sentenced. Following a complex Secret Service investigation, on July 18, 2012, a court in the Eastern District of New York sentenced Aleksandr Suvorov to seven years in prison following his 2009 plea to conspiracy to commit wire fraud and his 2011 plea to trafficking in unauthorized access devices. Suvorov, an Estonian, was extradited from Germany in 2009. Along with Albert Gonzalez and Maksym Yastremskiy, he participated in a massive hacking scheme involving retail merchants. The May 2009 pleas, for example, involved a hack into the Dave & Buster's restaurant chain in which the group stole names and account numbers for approximately 110,000 credit card accounts. Gonzalez, arguably the most prolific identity thief in American history, had already pled guilty and was sentenced in March 2010 to 20 years in prison. Yastremskiy earlier received a 30-year prison term in Turkey for identity theft and related crimes.

Coreflood Botnet Takedown. In April 2011, the government filed a civil complaint against 13 "John Doe" defendants, alleging that they ran the Coreflood Botnet in order to engage in wire fraud, bank fraud, and illegal interception of electronic communications. At its peak, the group had control over several million computers infected with the Coreflood malware. Search warrants were obtained for computer servers throughout the country, and a seizure warrant was obtained for 29 domain names. The government also obtained a temporary restraining order (later followed by a preliminary and permanent injunction), authorizing the government to respond to signals sent from infected computers in the U.S. in order to stop the Coreflood software from running, thereby preventing further harm to hundreds of thousands of unsuspecting users of infected computers in the United States. Over the next month, the Coreflood Botnet was effectively eliminated.

Charges Brought Against Six Leaders of Anonymous and Related Hacktivist Collectives. In March 2012, charges were unsealed in five districts against Hector Xavier Monsegur, aka "Sabu," the former head of Anonymous and LulzSec who had been cooperating with the FBI since his arrest in the Southern District of New York (SDNY) in June 2011. Monsegur participated in hacks of HBGary Inc. and HBGary Federal LLC (Eastern District of California); Sony Pictures Entertainment and Fox Broadcasting Company (Central District of California); Infragard Members Alliance (Northern District of Georgia); and the Public Broadcasting Service (Eastern District of Virginia). SDNY also unsealed an Indictment charging Ryan Ackroyd, aka "kayla"; Jake Davis, aka "topiary,"; Darren Martyn, aka "pwnsauce,"; and Donncha O'Cearrbhail, aka "palladium," who identified themselves as members of Anonymous, Internet Feds and/or LulzSec, with a computer hacking conspiracy involving the hacks of Fox Broadcasting Company, Sony Pictures Entertainment and PBS. Lastly, FBI agents in Chicago arrested Jeremy Hammond, aka "Anarchaos," who identified himself as a member of a related

hacking group called "AntiSec."

Notorious Hacker and Identity Thief Surrendered by France to the U.S. On June 6, 2012, France surrendered a Russian citizen, Vladislav Anatolievich Horohorin, a/k/a "BadB," to United States authorities to face charges in two separate federal districts for aggravated identity theft, access device fraud, wire fraud, and conspiracy, based on a Secret Service operation. French authorities had provisionally arrested Horohorin on August 8, 2010, in Nice. Horohorin is alleged to be a notorious dealer in stolen credit and debit card information. The D.C. charges relate to Horohorin's operation of a website where he advertised the sale of stolen credit and debit card information. The Northern District of Georgia charges relate to his lead role in an international criminal group that completed more than 15,000 fraudulent transactions at over 2,100 ATMs in at least 280 cities worldwide in a 12-hour period in November 2008, causing more than $9.4 million in losses.

Romanian "Point-of-Sales" Hackers Lured and Extradited to U.S. Following an extensive Secret Service investigation, on May 4, 2011, a federal grand jury in Concord, New Hampshire, returned an indictment charging Adrian-Tiberiu Oprea, Cezar Iulian Butu, Iulian Dolan, and Florin Radu, all residents of Romania, with conspiracy to commit computer intrusions, wire fraud, and access device fraud. The defendants were part of a group that, beginning in 2008, remotely hacked into Subways' and other merchants' "checkout" or "point-of-sales" computer systems by using password-cracking and other tools; surreptitiously installed "keystroke logging" software, which in turn recorded and stored customers' credit, debit, and gift card data; electronically transferred the stolen card data to several U.S.-based computer servers ("dump sites") and from there to a server in Cyprus, for temporary storage; and then made unauthorized charges on the compromised accounts and sold stolen card data to other co-conspirators. Members of the conspiracy have compromised over 50,000 accounts and have made unauthorized charges in excess of $10,000,000 on these compromised accounts. Dolan and Butu, lured to the United States, were arrested upon their entry in August 2011, and remain in United States custody. Adrian-Tiberiu Oprea, 28, of Constanta, Romania, was extradited from Romania to the United States and appeared in federal court in New Hampshire on May 29, 2012. Radu is currently at large.

Operator of Worldwide Spam Botnet Convicted. On February 27, 2013, Oleg Nikolaenko, 25, a citizen of Russia who entered the United States on a tourist visa, was sentenced to time served (just over 27 months) in the Eastern District of Wisconsin following an earlier guilty plea. According to court documents, Nikolaenko operated and controlled the Mega-D botnet, which was at one time the world's largest spam botnet, accounting for approximately 32% of all spam worldwide. A network security company estimates that approximately 509,000 computers worldwide were infected with Mega-D botnet malware.

Operation Trident Tribunal Takes Down International Crime Rings Distributing Scareware. Operation Trident Tribunal is a coordinated international enforcement action targeting a cybercrime ring that caused over $71 million in losses to more than one million computer users by operating a "scareware" scheme. Scareware is malicious software that cybercriminals plant on victim computers through a variety of computer exploits including the use of botnets, "drive-by" downloads, and criminal search engine manipulation. The scheme uses a variety of ruses, including web pages featuring fake computer scans, to trick consumers into purchasing fake anti-virus software products at a cost of up to $129. In June 2011, DOJ coordinated the efforts of law enforcement in over a dozen countries to seize dozens of servers that were being used to orchestrate this scheme. At that time, the Department also announced the indictment of two Latvian nationals, and the freezing of five foreign bank accounts. More recently, the Department has announced additional indictments including four Ukrainian nationals and a Swedish national responsible for operating the scheme.

On January 19, 2012, defendant Mikael Patrick Sallnert, a citizen of Sweden, was arrested in Denmark and extradited to the United States. Sallnert was a trusted payments processor for the scareware ring, responsible for processing a substantial portion of the funds fraudulently obtained from U.S. victims.

These cases illustrate the broad scope of the Department's efforts to pursue cyber criminals. While the Department is proud of these cases and all of our efforts to tackle the growing and evolving cybersecurity problem, we recognize that there is much more to be done, and we will continue to work with our law enforcement and private sector partners to meet that challenge. Because of the global nature of the Internet and the related crimes it can facilitate, continued close coordination and cooperation with foreign law enforcement is critical to our collective success. Because our prosecutors understand the severe damage that computer crimes can have upon a victim, we continue to pursue appropriate cases, both large and small.

Legislation to Enhance the Department's Ability to Combat Cyber Threats

As the threat increases and evolves, so must our legal tools to combat the threat. In May 2011, as part of the Administration's Cybersecurity Proposal, the Department proposed some needed, moderate updates to the computer crime laws.1 These proposals were also explored in testimony before this committee in November, 2012.2 We continue to believe that many of these proposals would enhance our ability to combat cyber threats, including:

- A proposal to update the Racketeering Influenced and Corrupt Organizations Act ("RICO") to make the Computer Fraud and Abuse Act ("CFAA") offenses subject to

1 *See* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security.pdf.
2 *See* http://judiciary.house.gov/hearings/pdf/Downing%2011152011.pdf .

RICO. The CFAA is the primary statute used to prosecute hacking crimes. Computer technology has become a key tool of organized crime. Indeed, criminal organizations are operating today around the world to: hack into public and private computer systems, including systems key to national security and defense; hijack computers for the purpose of stealing identity and financial information; extort lawful businesses with threats to disrupt computers; and commit a range of other cybercrimes. Many of these criminal organizations are similarly tied to traditional Asian and Eastern European organized crime organizations.

- A proposal to clarify and update the forfeiture provision of the CFAA. This proposal would allow for civil forfeiture and clarify the rules governing criminal forfeiture under the statute.
- A proposal to update the CFAA's sentencing provisions. The goal of these changes is to eliminate overly complex, confusing provisions; simplify the sentencing scheme; and enhance penalties in certain areas where the statutory maximums no longer reflect the severity of these crimes. For example, 18 U.S.C. § 1030(a)(4) prohibits unauthorized access to a computer in the course of committing a fraud, such as where a hacker breaks into a database and steals 100,000 credit card numbers, but the maximum sentence is five years in prison. Because criminals can obtain many millions of dollars through fraud, other federal fraud crimes -- such as section 1343 (Wire Fraud) -- have maximum penalties of 20 years in prison. This disparity makes little sense. These changes will empower federal judges to appropriately punish offenders who commit extremely serious crimes, ones that result in widespread damage, or both. Judges would still, of course, make sentencing decisions on a case-by-case basis.

We look forward to working with the Committee on these important issues.

* * *

The Department of Justice stands ready to work with the Committee as it examines these important issues. We appreciate the opportunity to testify today, and we look forward to continuing to work with you.

This concludes my remarks. I would be pleased to answer your questions.

Mr. SENSENBRENNER. Thank you very much.
Mr. Boles.

TESTIMONY OF JOHN BOLES, DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. BOLES. Good morning, Chairman Sensenbrenner and distinguished Members of the Subcommittee. I appreciate the oppor-

tunity to be here today to talk to you about the cyber threat and how we are going about it with our partners to combat it.

As the Subcommittee is aware, the number and sophistication of cyberattacks against our Nation's private sector and the government networks has increased dramatically over the recent years, and it expected to continue.

We see four primary adversaries in the cyber world: spies who seek to steal our secrets and our intellectual property, organized criminals who want to steal our identities and our money, terrorists who would like to attack our critical infrastructure, and hacktivist groups who are trying to make a political or a social statement through the use of the Internet. The bottom line here is that we are losing data, money, ideas, and innovation to a wide range of cyber adversaries.

FBI Director Mueller has stated that he expects the cyber threat to surpass the terrorism threat in our Nation in the coming years. That is why we are strengthening our cyber capabilities, much in the same way that we enhanced our intelligence and our national security capabilities in the wake of 9/11.

The FBI recognized the significance of the cyber threat more than a decade ago, and in response the FBI developed a number of techniques to go after a strategy for responding to it. We created the Cyber Division. We elevated the cyber threat to our number three national priority behind only counter intelligence counterterrorism. We significantly increased our hiring of technically-trained agents, analysts, and forensic specialists, and we have expanded our partnerships with law enforcement, private industry, and academia.

We have made progress since the cyber division was first created in 2002. Back then, we viewed it as a success when we were able to recognize that networks were being attacked. Just the fact that we saw it and recognized it was part of our success. So the next 8 or 9 years, attribution, which is knowing who is responsible for the attack on our computers and our networks, was considered the level of success, and we got very good tracking the Internet protocol address or the IP addresses back to their source to determine who was responsible.

Now, we can often tell when the networks are being breached and are able to determine who is doing it. So the question now becomes as we move forward in this, is what are we going to do about it, or, how are we going to take action on this information that we have gathered.

The perpetrators of these attacks are often overseas, and in the past tracking an IP back to a source in a foreign country, it usually led to a dead end investigatively. Since then we have imbedded cyber agents with law enforcement and several key countries, including Estonia, Ukraine, the Netherlands, and Romania. And we have worked with some of these countries to extradite subjects from their countries to stand trial in the United States.

As I described in my written statement, the prime example of international collaboration came in the 2011 take down of Rove Digital, as company that was founded by a ring of Estonian and Russian criminals to commit a massive Internet fraud scheme. Seven of these have since been indicted in the Southern District of

New York, two of which have been extradited to the United States now and are in U.S. custody, and one pled guilty last month.

While we are proud of this and our other successes, we are continuing to push ourselves so that we can respond more rapidly and prevent attacks before they occur. Over the past year, under our current legal authorities and with our government partners, we successfully warned potential victims before an attack has occurred. They were then able to use that information to shore up their network defenses and combat the attack.

As we go into now our next move here will be the next generation of cyber, and these have all come apart as our initiative to drive forward in the next gen. Next gen cyber entails a wide range of measures, including focusing the cyber division specifically on computer intrusion networks as opposed to crimes committed with the computers being the modality, hiring additional computer scientists to assist with the technical investigations at FBI field offices, and expanding our partnerships in collaboration with the National Cyber Investigative Joint Task Force, or the NCIJTF.

Briefly, the NCIJTF is a compendium of 19 agencies who work together in a collaborative and information sharing environment so that we can almost in real time share information back and forth across the cyber threat.

So the next step of that, of course, is our private sector outreach. We consider that as an important and as our next step for our whole of government team approach in combatting cybercrime. Now, we have reached into the industry, developed expertise with them, and are sharing as rapidly at unseen rates than we have seen in the past. We now realize that the information flow must go both ways, where in the past we have taken information and not necessarily given them back actionable intelligence. We have now actionable intelligence. We have now rectified that, and in developing our partnership, we are able to make that information flow go in both directions.

So in conclusion, Mr. Chairman, to counter the threats that we face, we are engaging in an unprecedented level of collaboration within the U.S. government, with the private sector, and with international law enforcement. We look forward to continuing these partnerships and expanding them with the Committee and with Congress.

And thank you very much. I look forward to your questions.

[The prepared statement of Mr. Boles follows:]

Department of Justice

STATEMENT OF

JOHN BOLES
DEPUTY ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED

"INVESTIGATING AND PROSECUTING 21ST CENTURY CYBER THREATS"

PRESENTED

MARCH 13, 2013

Statement of
John Boles
Deputy Assistant Director
Cyber Division
Federal Bureau of Investigation

Before the
Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

At a Hearing Entitled
"Investigating and Prosecuting 21st Century Cyber Threats"

March 13, 2013

Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee, I am pleased to appear before you today to discuss the nature of the cyber threat, how the FBI has responded to it, and how we are marshaling our resources and strengthening our partnerships to more effectively combat the increasingly sophisticated adversaries we face in cyberspace.

The Cyber Threat

Some of the most critical threats facing our nation today emanate from the cyber realm. Intrusions into our corporate networks, personal computers, and government systems are occurring every single day by the thousands.

We see four malicious primary actors in the cyber world: foreign intelligence services, terrorist groups, organized crime enterprises, and hacktivists.

Dozens of countries have offensive cyber capabilities, and these foreign cyber spies have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate government and military secrets, as well as valuable intellectual property—information that can improve the competitive advantage of state-owned entities and foreign companies.

Terrorist groups would like nothing better than to digitally sabotage our power grid or water supply. Some say they do not currently have the capability to do it themselves. But the reality is that the capability is readily available on the open market.

Organized crime groups, meanwhile, are increasingly migrating their traditional criminal activity from the physical world to computer networks. They no longer need guns to rob a bank; they use a computer to breach corporate and financial institution networks to steal credentials, account numbers, and personal information they can use to make money.

These criminal syndicates, often made up of individuals living in disparate places around the world, have stolen billions of dollars from the financial services sector and its customers. Their crimes increase the cost of doing business, put companies at a competitive disadvantage, and create a significant drain on our economy.

Hacktivist groups such as Anonymous and LulzSec are pioneering their own forms of digital anarchy by illegally accessing computers or networks for a variety of reasons including politically or socially motivated goals.

With these diverse threats, we anticipate that cyber security may well become our highest priority in the years to come. Computer intrusions and network attacks are the greatest cyber threat to our national security. That is why we are strengthening our cyber capabilities, in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11th attacks.

FBI Response 2002-2012

The FBI recognized the significance of the cyber threat more than a decade ago and, in response, created the Cyber Division in 2002; elevated the cyber threat as our number three national priority (only after counterterrorism and counterintelligence); significantly increased our hiring of technically trained agents, analysts, and forensic specialists; and expanded our partnerships with law enforcement, private industry, and academia, through initiatives like InfraGard—a public-private coalition of 55,000 members to protect critical infrastructure—and the National Cyber-Forensics and Training Alliance, a proven model for sharing private sector intelligence in collaboration with law enforcement.

We have made great progress in the interim. Ten years ago, if you were an agent conducting a cyber investigation and the Internet Protocol (IP) address tracked back to a foreign country, that was effectively the end of your investigation. Although you could send a lead to one of the FBI's overseas Legal Attaché Offices, the likelihood that you would discover who was behind the keyboard was small.

Since then, we have embedded cyber agents with law enforcement in several key countries: Estonia, Ukraine, the Netherlands, and Romania. Some countries in cyber hot spots also enhanced their domestic laws and agreed to allow extraditions to the United States.

Those changes, along with improvements in our ability to track IP addresses back to their source, have led to a recognition in the underground economy that there are fewer safe hiding places around the globe. Building on the success of our international outreach, we are currently expanding our Cyber Assistant Legal Attaché program to additional countries.

A prime example of how our investigations have progressed in the 10 years since the Cyber Division was created is the 2011 takedown of Rove Digital, a company founded by a ring of Estonian and Russian hackers to commit a massive Internet fraud scheme.

The scheme infected with malware more than four million computers located in more than 100 countries. The malware secretly altered the settings on infected computers, enabling the hackers

to digitally hijack Internet searches using rogue servers for Domain Name System (DNS) routers and re-routing computers to certain websites and ads. The company received fees each time these web sites or ads were clicked on or viewed by users. This scheme generated $14 million in illegitimate income for the operators of Rove Digital.

Because Estonia has improved its domestic laws, we were able to work with our law enforcement counterparts and our private industry partners to execute a takedown of this criminal organization. Following the arrest of several co-conspirators in Estonia, teams of FBI agents, linguists, and forensic examiners assisted Estonian authorities in retrieving and analyzing data that linked the co-conspirators to the Internet fraud scheme. At the same time, we obtained a court order in the United States to replace the rogue DNS servers with court-ordered clean servers.

In this case, we not only took down the criminal organization, but worked with our partners in DHS and other agencies to mitigate the damage. Seven individuals have been indicted in the Southern District of New York in this case: six in Estonia and one in Russia. The United States has sought extradition of all six Estonian subjects. To date, two of them have been remanded to U.S. custody. One pleaded guilty on February 1, 2013.

We are also employing novel ways of combating the threat. In Operation Coreflood, the FBI worked with our private sector and law enforcement partners to disable a botnet that had infected an estimated two million computers with malicious software.

The malware on this Coreflood botnet allowed infected computers to be controlled remotely by criminals to steal private personal and financial information from unsuspecting users. In an unprecedented move, the FBI obtained a court order to seize domain names, re-route the botnet to FBI-controlled servers, and respond to commands sent from infected computers in the United States, telling the zombies to stop the Coreflood software from running. The success of this innovative operation will help pave the way for future cyber mitigation efforts and the development of new "outside the box" techniques.

While we're proud of these investigative successes and our progress against the threat, we are continuing to push ourselves to respond more rapidly and prevent attacks before they occur.

Last month, President Obama released the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets. As part of the Strategy, the FBI is expanding its efforts to fight computer intrusions that involve the theft of trade secrets by individuals, foreign corporations, and nation-state cyber hackers.

Over the past year, under our legal authorities and in conjunction with our government partners, we have successfully warned some potential victims ahead of time that Computer Network Exploitation (CNE) or Computer Network Attacks (CNA) were about to happen. They were able to use that information to shore up their defenses.

Another area in which we've had success recently is in targeting infrastructure we believe has been used in Distributed Denial of Service (DDOS) attacks, and preventing it from being used for future attacks.

Since October, the FBI and the Department of Homeland Security (DHS) have released nearly 130,000 IP addresses that were believed to be infected with DDOS malware. We have released this information through Joint Intelligence Bulletins (JIBs) to 129 countries. These JIBs are released by both the DHS' Computer Emergency Readiness Team (CERT) mechanisms as well as by our Legal Attachés to our foreign partners.

These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDOS attacks.

Next Generation Cyber

The need to prevent attacks before they occur is a key reason we have redoubled our efforts to strengthen our cyber capabilities while protecting privacy, confidentiality, and civil liberties. The FBI's Next Generation Cyber Initiative, which we launched in 2012, entails a wide range of measures, including focusing our Cyber Division on intrusions; hiring additional computer scientists; creating Cyber Task Forces focused on intrusions in each of our 56 Field Offices; and expanding partnerships and collaboration at the National Cyber Investigative Joint Task Force (NCIJTF).

The nature and severity of the cyber threat have led the government agencies with a role in cyber security to recognize that we must work together more efficiently than ever to keep pace with and surpass our adversaries in this realm.

To that end, FBI Director Robert Mueller, DHS Secretary Janet Napolitano, and National Security Agency (NSA) Director Keith Alexander recently held a series of meetings to clarify the lanes in the road in cyber jurisdiction. The group mutually agreed on their respective roles and responsibilities related to a cyber incident. The FBI's role is to investigate, attribute, and disrupt cybercrimes affecting the United States. DHS' role is to protect our critical infrastructure and our networks, coordinate mitigation and recovery from cyber incidents, and to disseminate threat information across various sectors. NSA's role is to gather intelligence on foreign cyber threats and to protect national security systems.

We are coordinating at an unprecedented level, including rapid, real-time exchanges from FBI investigative activities to DHS, allowing the Department to push out information to help safeguard other networks from similar attacks.

A key part of the intergovernmental effort is the FBI-operated National Cyber Investigative Joint Task Force (NCIJTF), which serves as the deconfliction center on cyber investigations among 19 agencies. The NCIJTF involves senior personnel from key agencies, including Deputy Directors from NSA, DHS, the Central Intelligence Agency, and U.S. Secret Service. A fifth deputy will soon be appointed by U.S. Cyber Command. NCIJTF brings together a partnership of agencies focused on addressing cyber threats through investigations and intelligence sharing.

Not only have we recognized that the cyber threat warrants considerably strengthening our intergovernmental partnerships, but it also warrants significantly enhancing our collaboration with the private sector.

Today, the private sector is the essential partner if we are to succeed in defeating the cyber threat. The private sector is a primary victim of cyber intrusions—and its networks contain the evidence of countless such attacks. Our nation's companies and businesses possess the information, the expertise, and the knowledge we need to combat the threat. They also build the components of cyber security—the hardware, the software, and the networks—and drive future technology.

In the past, industry has provided us information about attacks that have occurred, and we've investigated the attacks. Our adversaries have taken advantage of the fact that we have been limited in the kind of information we exchange with the private sector. We now realize this can no longer be a one-way flow of information.

As part of our enhanced private sector outreach efforts, we're providing industry with tools, including information, to help repel intruders. In fact, in line with a strategic government-wide shift, we have recently begun to provide classified threat briefings to key industry partners and work with them to exchange information. InfraGard, NCFTA, and our other partnerships are a step in the right direction. But we must build on these initiatives, in conjunction with our federal partners, to expand the channels of information sharing and collaboration. We recognize that there are many considerations to take into account when considering the level of public-private collaboration we believe is necessary, including industry concerns about the protection of their proprietary information and questions about how best to share classified information. We are committed, however, to engaging in this collaboration in a way that fully protects privacy, confidentiality, and civil liberties.

Conclusion

In conclusion, Mr. Chairman, to counter the cyber threats we face, we are engaging in an unprecedented level of intergovernmental collaboration and cooperation with the private sector.

We look forward to continuing to expand on those partnerships and working with the Committee and Congress as a whole to determine a successful course forward for the nation to combat the cyber threat while protecting privacy, confidentiality, and civil liberties.

Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.

Mr. SENSENBRENNER. Thank you.
Mr. Holleyman.

TESTIMONY OF ROBERT HOLLEYMAN, PRESIDENT AND CEO, BSA, THE SOFTWARE ALLIANCE

Mr. HOLLEYMAN. Mr. Chairman, Ranking Member Scott, Members of the Subcommittee, there are more than 400 million strains of malicious computer code in the world today, and their most frequent targets are here in the United States. And this costs American citizens and businesses well over $100 billion a year, and the losses are mounting.

So I would like to recommend and outline a policy approach that BSA believes can help us address the nature of the threats that we face. It has three principle elements: first, promoting real time information sharing; second, strengthening law enforcement tools and resources; and third, supporting cybersecurity research and development.

On the issue of promoting real time information sharing, we know that to prevent cyberattacks, we need to be able to identify threats in real time, and the best way to do that is to let IT professionals share information. And when companies and government agencies detect threats, they need to tell each other.

Unfortunately there are legal barriers and commercial disincentives that stand in the way when the private sector tries to information with the government. First, there are liability concerns whenever you share commercial data, and, second, there is a risk of exposing trade secrets. And BSA believes that we need legislation that promotes information sharing by addressing these issues, and we need to do that in a way that carefully balances privacy and civil liberties concerns.

Secondly, we believe that we need to strengthen law enforcement tools and resources. Identifying emerging threats is important, but it is not nearly enough. We also need to enhance our ability to deter criminal behavior with effective law enforcement. We should not be over zealous in prosecuting people for innocent mistakes or minor infractions, but we in the government need tools and resources that send a strong message that there will be appropriate punishment for serious cybercrimes.

Third, the last element we need to do is to create something that is really fundamental that is elemental. We need to recognize that technology innovation is the best tool to combat long-term cyber threats, and BSA believes that we need a robust national R&D plan that involves technology companies, involve technologists within the governments, to develop the resources to take our technologies and our practices and improve our country's overall cybersecurity policy.

Now, the issue of data breach notification has come up as well, and we appreciate Mr. Conyers' statement this morning. We know that we will never be completely risk-free or eliminate all the risks of cyberattacks. But as a separate, but related, matter to cybersecurity legislation, we also believe we should clarify how and when to notify people when a breach compromises their personal information.

Today there are 47 States that have their own laws, and BSA supports replacing that patchwork with a well-crafted Federal law that simplifies compliance for businesses, but also ensures the proper notices when there is a breach of sensitive personal information.

And lastly, when Congress is working on cybersecurity legislation, we also do that knowing that the Administration is beginning to implement the President's recent executive order. And we are encouraged by the emphasis that order places on innovation, and we welcome the Administration's plan to improve coordination of cybersecurity policy and increased information sharing from the government to industry. And these measures must embody principles that everyone can embrace.

But it will take congressional oversight to ensure that the order is implemented effectively. And as the Administration develops the framework it envisions for protecting critical infrastructure, it will be especially important to forge a close partnership with industry. We believe that NIST should have a lead role in that, and done well, there is an opportunity for the framework to serve as a model for best practices that can be extended beyond just critical infrastructure.

So I appreciate the opportunity to testify today. BSA looks forward to working with this Committee and Congress to upgrade America's cyber readiness. Thank you.

[The prepared statement of Mr. Holleyman follows:]

Testimony

Bolstering US Cybersecurity

Robert Holleyman, President and CEO, BSA | The Software Alliance

Testimony before the US House of Representatives, Committee on the Judiciary, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations

Hearing: Investigating and Prosecuting 21st Century Cyber Threats

March 13, 2013

Mr. Chairman, Ranking Member Scott and distinguished members of the Subcommittee, thank you for convening this hearing and for drawing attention to the issue of cybersecurity.

My name is Robert Holleyman. I am president and CEO of BSA | The Software Alliance, an association of the world's leading software companies. They operate on the front lines of the digital economy, investing heavily in research and development to provide software solutions and security tools to consumers and enterprises in all sectors of the economy. BSA member companies understand better than anyone the nature of the cybersecurity threats America faces today — and what we can do to confront them.

The Growing Threat Landscape

BSA member company Symantec publishes an annual *Internet Security Threat Report*. The most recent edition found more than 400 million unique variants of malicious computer code present in the global IT ecosystem. And only a few years ago, BSA member company McAfee identified a new piece of malware every 15 minutes. Today it's one per second, and McAfee's Fort Detrick-like vault of dangerous digital viruses contains more than 100 million specimens. Moreover, hack attacks on mobile devices are up over 700 percent in one year.

Cybercrimes and attacks carry enormous economic costs and security risks. For example, Symantec has calculated that cybercrimes perpetrated on consumers alone account for $110 billion in damages. This does not take into account harm done to government computers or the value of intellectual property stolen from businesses.

There are increasing numbers and varieties of advanced, determined, and persistent threats targeting businesses and government. Recent attacks on major US Banks were one

alarming example. Another was the attack on Saudi Aramco, the world's largest oil producer. Its entire computer network — at least 30,000 computers — were shut down. Employees were forced to run oil production processes with telephones and fax machines.

The important lesson we should take from these attacks is that cybersecurity threats are becoming bigger and more sophisticated. We need to respond by bolstering America's cybersecurity posture for what will be an ongoing fight.

BSA Recommendations

- **Promote real-time sharing of cyber-threat information.**

Legislation is needed to promote increased sharing of cyber-threat information. First and foremost, we need to ensure that government shares a greater quantity of actionable information with the private sector. Information should be categorized according to its actual level of sensitivity, not deemed "Top Secret" by default. This will ensure that frontline IT professionals have access to essential cyber threat information. BSA also believes that applications for security clearances for cybersecurity professionals should be expedited.

There should also be more sharing among and between private companies and the government. Legislation can help by eliminate unnecessary legal barriers that serve to deter the timely sharing of threat information with those who are actually positioned to act on it. The legal changes should include safeguarding of trade secrets and ensuring that there are adequate liability protections, while also carefully balancing privacy and civil-liberties concerns. This includes ensuring that any new liability-protected channel for information sharing by industry with the government is run by a civilian agency.

- **Strengthen law enforcement tools and resources.**

Despite concerted efforts by authorities at all levels, budget constraints and gaps in existing law make it harder than it should be to effectively investigate and prosecute of cybercrime. If we reach a point where criminals can act with virtual impunity, it would threaten online consumer confidence in the security of ecommerce. To ensure this doesn't happen, Congress should close loopholes in criminal statutes and stiffen penalties and sanctions to provide more effective deterrence. It also should provide more resources to law-enforcement authorities so they can keep pace with evolving threats. FBI Director Robert Mueller previously testified that cybercrime is a top priority for the FBI. This is as it should be. However, we must make sure he has the resources to back that commitment up.

It is important for laws and law enforcement to be strengthened in appropriate proportions — so that innocent and minor infractions are not over-penalized, but serious crimes are effectively deterred.

Finally, legislation should strengthen and support federal authorities' ability to coordinate and collaborate with their counterparts internationally. BSA member Microsoft has studied infection rates of computers around the world. The company found that countries with the lowest malware infection rates were significantly more likely to have signed one or more international treaties on cybercrime. For this reason, BSA believes that giving the federal government greater authority to improve the quality of legal frameworks around the world would be a positive step.

- **Support cybersecurity research and development.**

Technological innovation is our best tool against cyber-criminals. Comprehensive cyber-legislation should contain a robust R&D plan and give researchers more resources to develop new technologies and practices that will improve the country's cybersecurity posture.

- **Reform FISMA.**

There is overwhelming agreement that the Federal Information Security Management Act of 2002 (FISMA) needs to be reformed. The Act was an important step in improving our nation's cybersecurity, but its effectiveness in today's world is questionable. FISMA serves as a reminder that legislation should be written with the understanding that the future is unpredictable and that the cyber-landscape will undoubtedly change faster legislation can be updated. To make FISMA more "future-proof" — and to support important work being done by the Administration to move toward more dynamic models of risk management — the law should be reformed to encourage agencies to engage in continuous, real-time monitoring instead of conducting rigid, "check-the-box" exercises. This shift in tactics will make federal IT systems more adaptive and reliable.

- **Pass a uniform data-breach notification law.**

A separate, but related cybersecurity issue is how and when to notify people when a data breach has compromised their personal information.

First, BSA believes organizations should adopt security measures that are appropriate for the level of sensitivity of the data and information they are holding. If, despite those security measures, a breach occurs that poses significant risk of serious harm, then there should be consistent national policies to ensure that customers and consumers are notified in an appropriate manner.

Today, 47 states have data-breach notification laws. And while we have managed to adapt to these various laws, a properly defined data-breach notification standard would go a long way to guide organizations on how to address cyber threats in their risk management policies. It also would help prevent breaches and give guidance on how best to respond if

an organization should fall victim to a breach caused by an attack. It would be particularly helpful for smaller businesses. Because of the Internet, they are able to do business in every state, but many cannot afford teams of lawyers to navigate 47 data breach standards should something bad actually happen.

National data-breach legislation should be carefully crafted, and in particular be technology-neutral, to help organizations prevent and respond to security incidents while avoiding costly, burdensome rules that would not provide any real protection to consumers and freeze security innovation. Such legislation will provide much-needed regulatory relief to companies facing conflicting legal obligations under today's patchwork of state laws.

Effectively Implementing the Executive Order on Critical Infrastructure

While Congress works on cybersecurity legislation, the Administration has begun implementing the President's recent Executive Order on protecting critical infrastructure. Implementing the Administration's policy effectively should be one of our biggest priorities. The Executive Order attempts to:

1. Improve the coordination of cybersecurity policy within the federal government;
2. Increase and accelerate "government-to-industry" information sharing efforts while at the same time protecting privacy and civil liberties;
3. Establish a "framework" to reduce cyber threats to critical infrastructure through a voluntary program with industry; and
4. Use of market-based incentives to encourage adoption of industry-led standards and widely accepted business practices beyond just critical infrastructure.
5. Make the preservation of innovation a central principle of our country's efforts to strengthen cybersecurity.

BSA welcomes the Order's emphasis on innovation and applauds the measures to improve coordination and increase information sharing. But we believe it will be important to develop the framework on critical infrastructure protection in careful partnership with industry. Even more important is ensuring that this work continues to be led by NIST, which has an admirable track record of working with industry to identify and foster the development of consensus-based guidance that leverages globally recognized standards and widely accepted business practices. Done well, there is an opportunity for it to serve as a model for best practices beyond just infrastructure that is deemed critical. It also can serve as a formula for other countries that tend to favor strict, command-and-control regulations that are ill-suited to the modern cybersecurity environment because of their inflexibility.

Conclusion

There will be no silver bullet to effectively combat cybercrimes and attacks. Instead, the public and private sectors need to have a variety of tools at their disposal. I appreciate the opportunity to testify today. BSA looks forward to working with Congress to bring these urgently needed policy solutions to fruition.

Mr. SENSENBRENNER. Thank you, Mr. Holleyman.
Professor Kerr.

TESTIMONY OF ORIN S. KERR, FRED C. STEVENSON RESEARCH PROFESSOR, GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

Mr. KERR. Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee, thank you for the invitation to testify this morning.

The Computer Fraud and Abuse Act is the primary Federal computer crimes statute, and its main prohibition is on unauthorized access to a computer. A year and a half ago, the Subcommittee had a relatively similar hearing to that today, and at that time I testified about some of the recent court decisions which had adopted a very broad interpretation of the Computer Fraud and Abuse Act, not only punishing what we would think of as hacking, breaking into a system, but also violating the terms of use on a computer, doing something contrary to an employer's interest while using a computer, and the like.

And I warned about the implications of that broad interpretation of the Computer Fraud and Abuse Act. Everyone agrees that the law should punish serious computer crimes, but I hope we would also agree that the law should not punish completely innocent activity, the kind of innocent activity that most Americans engage in every day might be violating terms of use on a Web site. That is that little language that nobody reads off to the corner that everybody blows by when they go to use a Web site or an Internet service. It should not be that violating those terms of service is a crime. Some Federal circuits have, in fact, indicated that that is the case.

And a lot has changed, though, in the last 18 months since the last hearing. In the 9th Circuit, the en banc 9th Circuit in *United States v. Nozol*, concluded that the Computer Fraud and Abuse Act does not apply to breach of employer restrictions on access to a computer, and is relegated only to sort of classic breaking into a machine, what we might call hacking or we think of as hacking, what the court called circumventing a technological access barrier.

Also in 2012, the 4th Circuit decided a case, concluding that an employee that acts in a way disloyal to an employer while using the employer's network is not violating the Computer Fraud and Abuse Act, creating a disagreement between the decision of the 4th Circuit and another decision of the 7th Circuit, which it indicated that that would be a Federal crime.

So right now, the state of the law in the lower courts interpreting this critical phrase of this critical statute, the Computer Fraud and Abuse Act, is essentially in disarray. There are circuits that are all over the map in terms of just figuring out what this prohibition means, what is this statute that has been on the books for 25 years.

So I think this Committee basically has two choices. One is to do nothing and let the Supreme Court figure it out. There is a circuit split. That means usually the Supreme Court at some point will step in and resolve the uncertainty and either pick the narrow view of the statute, or the broad view of the statute, or something

in between, or Congress could act and actually clarify which interpretation of the statute is the right one.

I think this Congress should act. This is a question ultimately of what Congress wants to prohibit, and I think the best approach is for Congress to enact the narrow view of the Computer Fraud and Abuse Act, essentially codifying the rule of the 9th Circuit, *United States v. Nozol*, that what this statute does is prohibit breaking into a computer.

We are not meeting here because we are worried about individuals breaching terms of service. We are not worried about employees of companies checking Facebook on company time. We are worried about people hacking into critical infrastructure, people accessing United States' secrets that are stored on computers from abroad. Those are problems which would be prosecuted and criminalized under any interpretation of the Computer Fraud and Abuse Act. But I think it is essential that Congress narrow the statute and expressly adopt this narrow view rather than just wait for the Supreme Court to try to figure it out.

We do not know what would happen if the Supreme Court took this case, and in all likelihood, no matter what the Supreme Court would do, we would probably be back here to try to figure out what the laws should look because there are hard cases to be dealt with on either side.

In particular, imagine the Supreme Court adopts the narrow view of the statute and says that the Computer Fraud and Abuse Act only prohibits classic hacking into a network. In that case, there is the problem of insiders. They are given access to the network, but they essentially steal secrets and then send them to somebody else or use them in some nefarious way or maybe give them to a foreign government. We of course need to make sure that that is prohibited as well.

And there are statutory authorities that can do that, for example, the Theft of Trade Secrets Statute is available in those situations. But also we could amend the Interstate Transportation of Stolen Property Act, which is used to deal with the transferring of stolen property in the case of physical property. The Justice Department has tried unsuccessfully to use that statute to prosecute stolen information. The 2nd Circuit has said that is not a fair interpretation of the statute, and that could be amended to make sure the insider threat is dealt with.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Kerr follows:]

United States House of Representatives
Subcommittee on Crime, Terrorism, Homeland Security and Investigations

"Investigating and Prosecuting 21st Century Cyber Threats"
Wednesday, March 13, 2013
2237 Rayburn House Office Building, 11:30 a.m.

WRITTEN STATEMENT OF ORIN S. KERR
FRED C. STEVENSON RESEARCH PROFESSOR
GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

The federal computer crime law known as the Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. § 1030, must strike a vital balance. On one hand, the law must allow the government to criminally prosecute and appropriately punish those who break into vital computer networks and cause significant harms. On the other hand, the law must not allow the government to criminally prosecute and punish innocent computer users who engage in routine harmless activity such as violating Terms of Service or visiting public websites.

In order to achieve both goals at once, the law must be clear. The law must specify what it prohibits and what it does not prohibit, what is a felony and what is a misdemeanor. When the law is clear, courts can easily interpret it to both ensure that the government has the power it needs to prosecute wrongdoers and also that the government does not have the power to prosecute innocent Americans who engage in common and innocuous online activity.

Unfortunately, the CFAA is remarkably vague. Congress has largely given up the task of explaining what the law covers, leaving the courts to grapple with what the statute means. The lower courts are deeply divided on the statute's scope, with some courts concluding that the law is remarkably broad. As a result of this confusion, the meaning of the law presently varies depending on which part of the country you happen to be in. This situation is intolerable. Congress should step in and state clearly what harmful conduct Congress wants to prohibit with the force of federal criminal law.

Clarity will ensure that both of the essential goals of the CFAA can be satisfied at once: The law should both punish what should be punished and ensure that innocent conduct is not criminalized.

In my written testimony, I will begin by briefly addressing my experience with the CFAA. I will then explain the broadest and most important provision of the CFAA, and then will then explain how courts have interpreted the most important aspects of the statute. I will conclude by offering my views on how the CFAA should be amended.

I. My Experience With the CFAA

Before I begin, let me briefly explain my experience with the CFAA. I have worked with the CFAA at various times in the capacity of prosecutor, legal scholar, and defense attorney. I first began studying the Computer Fraud and Abuse Act in 1998, when I joined the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. From 1998 to 2001, I assisted in the investigation and prosecution of many CFAA cases as a Justice Department Trial Attorney and as a Special Assistant U.S. Attorney in the Eastern District of Virginia.

In 2001, I joined the faculty at George Washington University Law School. Since that time, I have authored a chapter of a law school casebook on the CFAA, and I have taught the law of the CFAA in a course on computer crime law. *See* Orin S. Kerr, Computer Crime Law (Thomson-West 3nd ed. 2013). I have also written two law review articles about the Act. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010); *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes,* 78 NYU L. Rev. 1596 (2003).

Finally, I have worked and continue to work as a defense attorney in CFAA cases on a *pro bono* basis to try to block the expansive readings of the Act that are the subject of my testimony. My written testimony draws from all of these experiences, although of course it is made entirely in my personal capacity.

II. The Broadest Section of the CFAA, 18 U.S.C. § 1030(a)(2)(C).

The CFAA is essentially a computer trespass statute. It prohibits trespassing on to a computer much like a trespass statute punishes trespassing onto physical land. The CFAA contains a number of different crimes, but the best way to understand the statute is to focus on its broadest section, 18 U.S.C. § 1030(a)(2)(C). This provision punishes whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." We can break this federal crime into its three elements as follows:

(1) Intentionally accesses a computer without authorization or exceeds authorized access
(2) Obtains information
(3) From a protected computer

Critically, elements (2) and (3) will be satisfied in most instances of routine computer usage. Element (2), the requirement that a person "obtains information," is satisfied by merely observing information. *See, e.g., United States v. Tolliver*, 2009 WL 2342639 (E.D. Pa. 2009) (citing S. Rep. No. 99-432 at 2484 (1986)). The statute does not require that the information be valuable or private. *Any* information of *any* kind is enough. Routine and entirely innocent conduct such as visiting a website, clicking on a hyperlink, or opening an e-mail generally will suffice.

Element (3) is easily satisfied because almost everything with a microchip counts as a protected computer. The device doesn't need to be what most people think of as a "computer," and it doesn't need to be connected to the Internet. Consider the relevant definitions. Under 18 U.S.C. § 1030(e)(1), a "computer" is defined as:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.]

This definition "captures any device that makes use of a electronic data processor." *United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011). Indeed, the Justice Department has argued that any "electronic, magnetic, optical, [and] electrochemical" data processing device is included, whether or not it is "high speed." *Id.* at n.3. Given that many everyday items include electronic data processors, the definition might plausibly include everything from many children's toys to some of today's toasters and coffeemakers.

The statutory requirement that the computer must be a "protected" computer does not provide an additional limit. In 2008, Congress amended the definition of "protected" computer to include any computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). In federal law, regulation that "affects interstate or foreign commerce" is a term of art: It means that the regulation shall extend as far as the Commerce Clause allows. *See Russell v. United States*, 471 U.S. 858, 849 (1985). Under the aggregation principle of *Gonzales v. Raich*, 545 U.S. 1 (2005), this appears to include all computers, period. As a result, every computer is a "protected" computer.

Because elements (2) and (3) are so extraordinarily broad, liability for federal crimes under 18 U.S.C. § 1030(a)(2)(C) hinges largely on the first element: What does it mean to access a computer without authorization or to exceed authorized access? Unfortunately, courts have not settled on clear answers to these questions. The terms "access" and "without authorization" are not defined by the CFAA. The phrase "exceeds authorized access" is a defined term, but the definition is largely circular. That phrase is defined in 18 U.S.C. § 1030(e)(6):

> the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

Under this definition, conduct exceeds authorization if it exceeds entitlement. But this merely restates the problem: What determines entitlement? Unfortunately, the statute doesn't say. Because these key phrases are either undefined or defined poorly, judicial interpretations of "access without authorization" and "exceeds authorization" are

surprisingly murky. The next two sections will focus on how courts have interpreted these two terms.

II. The Meaning of "Access Without Authorization"

The two most important precedents on the meaning of "access without authorization" are *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), and *Pulte Homes, Inc. v. Laborers' International Union Of North America*, 648 F.3d 295 (6th Cir. 2011). These two cases indicate that a person accesses a computer without authorization when that person bypasses some kind of password gate or code-based restriction to gain access to a computer.

In *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), the Second Circuit held that sending out an Internet "worm" had accessed victim computers without authorization by gaining access to them in unauthorized ways. The Second Circuit identified two specific ways that accessing the victim computers was without authorization. The first way was gaining access to a computer by guessing a password that controlled accessed to that computer. This makes sense: Guessing a password is something like picking a physical lock, and using a stolen password is something like making a copy of the key and using it without the owner's permission. The second way identified by the *Morris* court to access a computer without authorization is by exploiting a security flaw in a program to gain access in a way contrary to the program's "intended function." The basic idea is that if a program has a security flaw that enables an outsider to gain access to the computer based on an unintended effect of that program, then the access is not authorized. For a physical analogy, imagine a burglar breaks in to a home by finding a window that has accidentally been left open. The entrance would be without authorization because the homeowner did not intend to allow individuals to enter his home through the window.

The second case, *Pulte Homes, Inc. v. Laborers' International Union Of North America*, 648 F.3d 295 (6th Cir. 2011), provides a helpful bookend to *Morris*. *Pulte Homes* was a civil case involving a lawsuit by a company involved in a labor dispute against a union. According to the complaint, the union hired an auto-dialing service to place thousands of calls to clog access to the phone system of the company. The

company claimed that this constituted an "access without authorization" of the company's computers. The Sixth Circuit disagreed. According to the Sixth Circuit, the difference between access without authorization and exceeds authorized access is that a person who accesses a computer without authorization has no rights at all to access that computer. The company's communications system could not have been accessed without authorization, the court held, because it was an unprotected public means of communications. The company "allows all members of the public to contact its offices and executives," and does not require "a password or code to call or e-mail its business." "[L]ike an unprotected website," the Sixth Circuit explained, the company's "phone and e-mail systems were open to the public, so [everyone] was authorized to use them." *Id.* at 303-04.

Morris and *Pulte Homes* thus offer a relatively clear answer to the meaning of "access without authorization," at least in the networked setting when a user accesses a computer over a remote network. Under those two cases, a person accesses a computer without authorization when that person bypasses some kind of password gate or code-based restriction to gain access to the computer.

Importantly, however, even this relatively clear standard does not answer how the concept of "access without authorization" applies outside the network setting. For example, imagine a person has a laptop computer in a locked room, and someone breaks the lock and enters the room to use the computer. Alternatively, imagine *A* borrows *B*'s laptop with *B*'s permission; later on *B* changes his mind and tells *A* that *A* can no longer use it; and *A* uses it anyway. Are these acts "access without authorization" prohibited by the CFAA? At this point, the answer is unclear. *Cf. Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (concluding that an employee who accesses his employer's laptop computer while breaching the employee's duty of loyalty accesses the computer "without authorization.")

III. The Meaning of "Exceeds Authorized Access"

If the meaning of "access without authorization" is relatively clear, the same cannot be said for the meaning of "exceeds authorized access." Courts have struggled to understand the meaning of "exceeds authorized access" under the CFAA. The issue is

presently the subject of massive confusion in the lower courts, with the federal courts of appeals sharply divided. Much of the problem is the circular definition of "exceeds authorized access," which is defined in 18 U.S.C. § 1030(e)(6) to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." Courts have divided on what conduct "exceeds authorized access" means because they disagree on what controls "entitlement."

Some courts have held that a written statement as to what the owner of the computer allows controls entitlement. Under this view, if a computer owner announces a written rule that governs how users must access the computer, then using the computer in a way inconsistent with that written rule "exceeds authorized access." For example, in *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010), the Eleventh Circuit held that an employee of the Social Security Administration exceeded his authorized access under § 1030(a)(2) when he used a SSA database for personal reasons. SSA policy limited access to the database for official business: By breaching that policy and accessing the database for non-business reasons, the defendant had exceeded authorized access. *See id.* at 1263-64.

Other courts have taken a narrower view. For example, in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), the en banc Ninth Circuit held that written restrictions do not govern access. According to the Ninth Circuit, a person "exceeds authorized access" when they have some rights to access a computer but nonetheless circumvent technological access barriers to access other information o the computer that they are not entitled to access. *See id.* at 858, 863. Put another way, under the Ninth Circuit view the CFAA only punishes hackers. Hackers who have no rights to access a network "access without authorization," while hackers have some rights to access a network "exceed[] authorized access. *See id.* at 858. *Accord* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 NYU L. Rev. 1596, 1662-63 (2003).

Courts have also divided on whether conduct "exceeds authorized access" absent explicit written conditions from the computer owner. For example, some courts contend that an employee acts without authorization by accessing his employer's computer with

an intent to further acts contrary to the employer's interests. Under this agency theory, a employee violates criminal law by using the employer's computer outside of the scope of agency. *See Citrin*, 440 F.3d at 420–21. On the other hand, other courts have rejected the agency approach and held that an employee does not exceed authorized access by accessing the employer's computer with an intent to act contrary to the employer's interests. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) ("Such a rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems.")

To add to the confusion, the Justice Department has taken the view that "exceeds authorized access" includes violating a written restriction on computer access such as the Terms of Use of a website. *See United States v. Drew*, 259 F.R.D. 449 (C.D.Cal.2009). This interpretation has the effect of prohibiting an extraordinary amount of routine computer usage. It is common for computers and computer services to be governed by Terms of Use or Terms of Service that are written extraordinarily broadly. Companies write those conditions broadly in part to avoid civil liability if a user of the computer engages in wrongdoing. If Terms of Use are written to cover everything slightly bad about using a computer, the thinking goes, then the company can't be sued for wrongful conduct by an individual user. Those terms are not designed to carry the weight of criminal liability. As a result, the Justice Department's view that such written Terms should define criminal liability – thus delegating the scope of criminal law online to the drafting of Terms by computer owners – would make criminals out of most computer users.

IV. What Should Be Prohibited By the CFAA?

The underlying question raised by the difficulties courts have in interpreting the CFAA is what kind of conduct Congress intended to prohibit. And since this Congress has the power to amend the statute, the more important question is prospective: What kind of conduct should be prohibited under the CFAA?

I urge Congress to expressly adopt the *Nosal* rule. The CFAA should only apply to those who circumvent technological access barriers. The law should apply only to those who break in to computers – to use the common term, it should apply only to "hackers." In my view, this is the best reading of existing law. Further, Congress should expressly codify it to make clear the appropriate scope of the CFAA.

To be sure, there are some situations in which people do very bad things that happen to involve a violation of a written access restriction. If an individual commits a crime and happens to violate Terms of Service along the way, then the individual should be prosecuted for the crime committed. But the CFAA should not be a catch-all statute that always gives the federal government another ground on which to charge a wrongdoer who violated some other crime that happened to involve a computer.

The problem with a broader approach is that it inevitably ends up covering a great deal of innocent activity. Consider a few examples:

A. A political blog announces a new rule that readers only are allowed to visit the blog if they plan to vote Republican in the next Presidential election. A reader who plans to vote for the Democratic nominee visits the blog in violation of the rule.
B. A law student who is forbidden by law school policy to access the law school network during class intentionally violates the rule by checking his e-mail during a particularly boring lecture.
C. You receive an e-mail from a friend that a new website, www.dontvisitme.com, has some incredible pictures posted that you must see. But there's a catch: The Terms of Service of the website clearly and unambiguously say that no one is allowed to visit the website. You want to see the pictures anyway and visit the website from your home Internet connection.

If violating an express condition on computer usage is a crime, then all three of the individuals in these scenarios above have committed a federal offense.

Such a law would be intolerable because Terms of Service are essentially arbitrary. Anyone can set up a website and announce whatever Terms of Use they like.

Perhaps the Terms of Use will declare that only people who have been to Alaska can visit the website; or only people named "Frank" can visit. Under the Justice Department's interpretation of the statute, all of these Terms of Use can be criminally enforced. It is true that the statute requires that the exceeding of authorized access be "intentional," but this is a very modest requirement because the element itself is so easily satisfied. Presumably, any user who knows that the Terms of Use exist, and who intends to do the conduct that violated the Term of Use, will have "intentionally" exceeded authorized access.

I do not see any serious argument why such conduct should be criminal. Computer owners and operators are free to place contractual restrictions on the use of their computers. If they believe that users have entered into a binding contract with them, and the users have violated the contract, the owners and operators can sue in state court under a breach of contract theory. But breaching a contract should not be a federal crime. The fact that persons have violated an express term on computer usage simply says nothing about whether their conduct is harmful and culpable enough to justify criminal punishment. There may be cases in which harmful conduct happens to violate Terms of Use, and if so, those individuals should be punished under criminal statutes specifically prohibiting that harmful conduct. But the act of violating Terms of Service alone should not be criminalized.

In my view, the answer is to codify the *Nosal* rule. Instead of prohibiting two different acts, "access without authorization" and "exceed[ing] authorized access," the law should simply prohibit "access without authorization" defined in the following simple way: "the term 'access without authorization' means to circumvent technological access barriers to a computer or data without the express or implied permission of the owner or operator of the computer." This rule would codify *Nosal* and result in a simple rule that would allow the government to prosecute real intruders in networks but not go after those who simply breach terms of service.

V. Additional Thoughts About the Future of CFAA Reform

My written testimony only scratches the surface of the changes to the CFAA that I think are necessary. In addition to adopting the *Nosal* rule, I think Congress needs to better define and narrow the felony provisions of the statute to ensure that the statute accurately distinguishes minor offenses from major ones. I have posted statutory language that I suggest for CFAA reform here: http://www.volokh.com/wp-content/uploads/2013/01/Amended10302.pdf I would be happy to discuss any of the changes I recommend in that draft during your questioning.

I want to conclude with four points about the future of CFAA reform:

1) *Congress can do this.* The CFAA dates back to the 1980s, and the major questions raised as to its scope are decades old. As a result, Congress should not be afraid to step in and better define the coverage of the statute. Although computer technologies can change quickly, the scope of authorization is a timeless issue. Federal criminal statutes are purely a creature of Congress: There are no federal common law crimes. As a result, Congress should feel not only the ability but the responsibility to explain with clarity what kind of conduct the criminal laws prohibit.

2) *A narrow but clear CFAA will serve both government interests and civil liberties interests.* The major ambiguity over the scope of the CFAA is an obvious problem from the standpoint of civil liberties. But it is also a problem for law enforcement. Significant statutory vagueness in a criminal statute invites courts to narrow or even invalidate the statute under the "void for vagueness" doctrine. As long as the CFAA retains its existing text, vagueness challenges will continue. *See generally* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010). Prosecutors need to rely on the CFAA when prosecuting important cases with real harms. A clear and specific statute will be better serve government interests than a vague and opaque one.

3) *Insider threats can be covered under a different statute.* Under the *Nosal* rule, insider threats can still be punished under some sections of the CFAA, such as 18 U.S.C. § 1030(a)(5)(A). But if Congress wishes to punish insiders beyond 18 U.S.C. § 1030(a)(5)(A), the answer is to punish insider threats using a different statute. To some extent, other criminal laws will apply already. For example, many insider threats can be punished under the federal theft of trade secrets statute, 18 U.S.C. § 1832. But Congress

can easily address the insider threat through other statutes such as the Interstate Transportation of Stolen Property Act, 18 U.S.C. § 2314.

4) *The CFAA is only becoming more important.* A final reason to focus attention on CFAA reform is that the statute will only become more important over time. Every year, the American public uses computers for more hours and for more tasks. The recent public uproar over the tragic death of Internet activist Aaron Swartz has brought new attention to the scope of the CFAA. Swartz was facing felony charges under the CFAA, and many believe that those charges show that the CFAA is overly broad and overly punitive. *See, e.g., Lessig on 'Aaron's Laws - Law and Justice in a Digital Age'*, available at http://www.youtube.com/watch?v=9HAw1i4gOU4. But whether inspired by recent events or simply by the need to address the scope of a statute that has become ever more important in our Internet age, Congress should take this opportunity to revisit the CFAA to make sure that it both provides appropriate tools for law enforcement but does not end up prohibiting innocent activity.

Thank you for this opportunity to testify. I look forward to your questions.

Mr. SENSENBRENNER. Thank you very much. Because of the time constraints, the Chair will withhold his questions until the end if there is time remaining.

And the Chair recognizes the gentleman from Arizona, Mr. Franks, to start the questions.

Mr. FRANKS. Well, thank you, Mr. Chairman. And thank all of you for being here today. I do not envy your jobs. It is difficult when you are trying to marry highly esoteric technological issues with very precise legal enforcement and prosecution issues. So it is a difficult challenge.

And it so happens that I am new on this Committee, so my primary familiarity with cybersecurity issues is on the Strategic Forces Committee where there is a national security component. And of course, it is an issue of the first magnitude.

So my first question is to you, Mr. Boles. Given that some type of commercial cyber intrusion carries with it one set of concerns, and national security carries with it a whole different set of concerns.

Are there different protocols or more latitude in existing law when you are doing what is necessary to protect our critical systems from national security threats or threats that have a national security nexus as opposed to the commercial intrusions?

Mr. BOLES. Thank you, sir. That leads right into why I spoke briefly about the next generation of cyber initiative. And one of the things that we have seen, that we have implemented in the change of that initiative is putting all tools in the toolbox. We recognize that in the cyber world, crimes are essentially without borders, as one of the gentlemen said, that the world has gotten smaller, crimes without borders. And it is often difficult to tell at the outset is it criminal or is it national security oriented.

So one of the things that we, working with the DoJ partners and with our other law enforcement partners, is how do we bring all the tools to the toolbox to combat the threat? So, for example, if it is a nation-state actor who is attempting economic espionage and stealing trade secrets, that then may enhance their national economy and/or structure. Is that criminal? Is it national security? I would say that it is both, and we have both sets of tools that we can bring to it.

So it gives us a wide latitude. It makes us a much more nimble law enforcement community to go after and combat these threats by being able to put the appropriate tool against the appropriate threat.

Mr. FRANKS. But once you identify whether it is a national security threat or it is simply a commercial threat, do you have a different set of criteria in the law as it is now to combat those, or are they treated essentially the same as far as your tools to respond?

Mr. BOLES. Again, I will tell you it sounds a little bit like I am going to hedge on you, but I am not. The fact of the matter is that by having both sides in the toolbox, we have kind of melded the two protocols together.

So what that means is, let us say, for example, we determine that is, in fact, a straight national security, you know, intrusion or theft, you know. How can we go about disrupting that? Part of the next generation cyber initiative is to identify the hands on the key-

board, you know, the skin behind the screen, and how do we go after them and disrupt that? So that is through criminal prosecution? Is that through working with our intelligence partners and our foreign partners overseas to disrupt in other manner or shutting off access?

It is a multitude of options that are open to us by doing that. So I would tell you that the protocols, by going to the all tools approach, actually gives us access to both protocols through the entirety of the investigation.

Mr. FRANKS. What would you suggest to this Committee, if we were to apportion our concern for each of those two things I mentioned, commercial intrusion as opposed to those threats that have a national security nexus.

When you identify these threats, what would you suggest would be the proportion, I mean, how much under attack from your point of view, and we are familiar with it in some of the security committees. But from your point of view in the FBI, what would you suggest is the state of the union here as far as our protection from national security cyber threats? Do you think that we are facing pretty significant challenges?

Mr. BOLES. We are absolutely facing significant challenges.

Mr. FRANKS. That was a leading question.

Mr. BOLES. Yes, it was. [Laughter.]

Mr. FRANKS. I am very familiar with just how serious they are in some ways. And I guess I would like to put something on your radar. It is not really in the form of a question, but I am concerned, and we are concerned on some of the security committees that intentional electromagnetic interference may someday be or EMP may be our ultimate cybersecurity threat in terms of a national security destructive to try to disrupt our systems. And I would hope that we would have that on the radar. I realize that is a little ways down the road, but perhaps not as far as it should be.

And I appreciate all of you for what you are doing. You are kind of the front line of freedom, even though people do not see you and appreciate it.

Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman. And I would like to follow through on that same line of questioning, but I would like Ms. Durkan to respond with the various levels of seriousness. First, will the Administration have a recommendation to address the concerns that Professor Kerr pointed out that there is split in the circuits on interpretation. Do we have a recommendation on how to deal with that split in the circuits?

Ms. DURKAN. Thank you, Ranking Member Scott. As we have said in other forums, we believe that there needs to be some clarification to the law in terms of particularly what exceeds authorized access is. But we think that what we need to make sure is that there are a number of insiders who have access to very valuable and confidential information, and we have to make sure that we still have the law enforcement necessary to protect against that threat.

Mr. SCOTT. Well, do you have a legislative recommendation?

Ms. DURKAN. We do not have a specific legislation recommendation, but we are willing to work with your staff and provide technical assistant to reach those goals.

Mr. SCOTT. Are there any other elements of the crime that need clarification?

Mr. SCOTT. There are additional ones we need clarification. I think that in our last year's proposal, we had how the difference between felonies, and misdemeanors, and previous offenses. And so, I think we can look at those issues.

But I think that you are right, and it has been said before is the nature of the threat is evolving rapidly, and it ranges everything from the consumers whose private data is threatened by hackers to the national security threats. We at the Department of Justice have to deal with that full range of threats, and so the important thing for us right now is not to create greater gaps in the law, but to ensure we have the tools that we need.

Mr. SCOTT. In your statement, you mentioned that judges would still, of course, make sentencing decisions on a case by case basis. Should we infer from that that the Administration will not have any mandatory minimums in its recommendations?

Ms. DURKAN. We are not recommending mandatory minimums in these recommendations. The judicial discretion, as you know, is very important for the judge to be able to determine what level of penalty is important.

I want to emphasize the Department does that at each stage of prosecutions as well, whether an investigation is merited in the first place, whether charges should be brought, and then what plea or what sentence is appropriate.

Mr. SCOTT. Well, we do not have to scour the recommendations for mandatory minimums, so we will assume that they are not there. Is that a fair assumption?

Ms. DURKAN. Yes, sir.

Mr. SCOTT. And a lot of these crimes, there are overseas connections to some of these crimes. Does that create jurisdictional problems that we need to address legislatively?

Ms. DURKAN. There may be some legislative fix. We need to do that. The Department has already taken some steps on the international front. It is more and more important, more of these cyber cases. For example, in my district we recently prosecuted a case where a case where a small business in Seattle was hacked by someone who was in Maryland, who traded the card information he got to a Dutch citizen living in Romania, who then sold them to someone in Los Angeles.

We were able to bring the person in Maryland, who has been prosecuted and convicted, as well as extradite the person from Romania charges pending against Los Angeles.

So international cooperation is key, and we are working on many fronts to make sure we have the most robust system possible.

Mr. SCOTT. Are any legislative changes needed to help you in that regard?

Ms. DURKAN. There may be some. There was one proposal that we had that was approved in the previous budget that gave us additional resources abroad, what we call our iChip Center, national cyber prosecutors, who can assist our foreign partners to make sure

that we gather the evidence we need to bring the people an extradite them to America.

Mr. SCOTT. Well, that brings me to my next question. A lot of this is resources and investigation. You have got these things in a statute. It is just a matter of priorities. This Committee has looked at things like ID theft where consumer ID theft cases are not brought because you just do not have the resources, organized retail theft for those cases are not investigated because of resources or funding. And somebody fails a background check on a gun purchase, nothing is done because you do not have the resources.

I guess, Mr. Boles, if you focus more on cybercrime, do you have enough resources to do the other things you need to do? And as part of that, what effect will the sequester have on your ability to continue doing your work?

Mr. BOLES. I keep going back to the net gen cyber, and that was one of our functions and one of our driving forces in that.

So the Cyber Division focuses entirely on intrusions and pushing forward for the high tech solution, but part of that was that we have also added impact and emphasis on the traditional cyber—I am sorry.

Mr. SENSENBRENNER. You can continue your sentence. [Laughter.]

Mr. BOLES. Okay. Under traditional cybercrime, much like on the ID theft, sir.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you very much. Members of the panel, most of our serious computer hacking threats come from other countries. Can any of you discuss with me and make a point about how we can better identify, stop, and prosecute these attacks?

Your recollection of what happened in another case is very compelling because we want to improve the law protecting against cybercrime. And the whole idea of this hearing is to identify where we should be going.

I think I have about the only general law on cyber privacy, which I introduced last year and will reintroduce today. And so I would appreciate, and the comments that have been made and any that may be added to this discussion.

Who would like to volunteer?

Ms. DURKAN. I can address some of that, Congressman.

First, I want to be clear. While the international cyber threat is growing and complex, we have a lot of homegrown cyber actors as well. In my district, we regularly prosecute people who are located right in our district who are able to do a significant amount of damage to both individual consumers and to businesses.

With regards to your privacy legislation, obviously we have not had the opportunity to review it yet. We look forward to doing so and working with the staff of the Committee. I will say that it has always been the position of the Department of Justice that all legislative proposals should carefully balance both the need to deter and hold accountable the bad actors with consumer privacy and civil rights, as well as making sure we have the adequate public-private partnerships. And so we look forward to working with you on that bill.

Mr. CONYERS. Well, you have the kind of a Subcommittee here that is going to take this seriously. There have been so many things going on, especially in the Judiciary Committee, that it is easy for this to slip through the cracks. And I think this hearing is extremely important for focusing in on that.

Mr. HOLLEYMAN. Mr. Conyers, let me say I think it is going to take a complement of laws and a mix like criminal statutes. I think the corollary around data breach notification can be very important, particularly if it also encourages the kind of incentives for companies to build in security practices so that if there is a breach of consumer data, that that data will be essentially useless because it is has been protected in the first instance.

So I think as the Federal Government, we can do more to protect our citizens. I think the private sector can do more. And it is going to take a mix of civil and criminal statutes to effectively deal with this.

Mr. CONYERS. Professor Kerr?

Mr. KERR. Yeah, just one brief comment. So the substantive law, the Computer Fraud and Abuse Act, already jurisdictionally covers the world. It covers everything. In fact, the Computer Fraud and Abuse Act covers every computer that the United States government can regulate around the world under the Constitution, under the foreign commerce clause and under the interstate commerce clause. So it will certainly apply to a foreign hacker who hacks into U.S. computers, the U.S. hacker that hacks into foreign computers, or even a foreign person that hacks into other foreign computers through the U.S.

So the substantive criminal law is very broad. The difficulty is always if somebody is outside the U.S., if the foreign government is going to cooperate with the U.S., then that is a way that the U.S. can have the person extradited and brought to the United States for prosecution. But if they are not a cooperative government, that is where the problem is going to be.

Mr. CONYERS. Well, you know, I think that we are going to have to put increased emphasis on our diplomacy aspect. I think the sooner, Chairman Sensenbrenner, that we begin to look at this part of this problem, the better off we are going to be in terms of getting as much cooperation as we can. Now, we know that is going to vary from country to country, but it is still very important.

Mr. SENSENBRENNER. The time of the gentleman has expired, and I agree with the last point that the gentleman from Michigan has made since the Internet is completely internationalized and knows no boundaries, either for doing good or breaking the law.

The gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman, and thank you to all the witnesses for your research, for your concerns, and for your testimony here today.

It is my understanding that under 18 U.S.C. 1030, that it is a violation, a criminal violation, of our law to do anything that helps take control of another computer even for a moment. Is that your understanding? Some general nods.

Mr. KERR. It depends exactly what you mean by take control, but certainly if taking control includes gaining access to the computer in order to take—assuming a network, you are not supposed to

take control of, then, yes, that would clearly be prohibited by the statute.

Mr. GOHMERT. All right. For example, my understanding is there was a recent example where someone had inserted malware on their own computer such that when their computer was hacked and the data downloaded, it took the malware into the hacker's computer, such that when it was activated, it allowed the person whose computer was hacked to get a picture of the person looking at the screen. So they had the person that did the hacking and actually did damage to all the data that was in the computer.

Now some of us would think that is terrific. That helps you get at the bad guys. But my understanding is that since that allowed the hackee to momentarily take over the computer and destroy information in that computer, and to see who was using that computer, then actually that person would have been in violation, in the United States would have been in violation of 18 U.S.C. 1030.

So I am wondering if perhaps one of the potential helps or solutions for us would be to amend 18 U.S.C. 1030 to make an exception such that if the malware or the software that allows someone to take over a computer, is taking over a hacker's computer, than it is not a violation. Perhaps it would be like we do for, say, assaultive offenses, you have a self-defense. If this is part of a self-defense protection system, then it would be a defense that you violated 1030.

Anybody see any problem with helping people by amending our criminal code to allow such exceptions or have any suggestions along those lines?

Mr. KERR. Mr. Gohmert, I think it is a great question and one that is very much debated in computer security circles because from what I hear, there is a lot of this sort of hacking back, as they refer to it. But at least under current law, it is mostly illegal to do that.

There is a limited necessity defense that some courts have recognized to say basically if you are a victim of a crime, you have a certain amount of ability to act to try to stop that crime. But it is not really clear how the necessity defense, as it is recognized in current Federal law, would apply in those circumstances.

I think the idea of saying there is some ability to counterhack back, however you want to describe it, is a sound one. The real difficulty is in the details of how do you do it. What circumstances do you allow somebody to counterhack how broadly, how broadly are they allowed to counterhack, how far can they go?

The difficulty, I think, is once you open that door as a matter of law, it can be something that is difficult to cabin. So I think if there is such an exception, it should be a quite narrow one to avoid it from sort of becoming the exception that swallows the rule.

Mr. GOHMERT. Well, I am not sure that I would care if it destroyed a hacker's computer completely, as long as it was confined to that hacker. Are you saying we need to afford the hacker protection so that we do not hurt him too bad?

Mr. KERR. No. The difficulty is that you do not know who the hacker is, so it might be that you think the hacker is one person. Let us say you think you are being hacked from a French company or even a company in the United States.

Mr. GOHMERT. Oh, and it might be the United States government, and we do not want to hurt them if they are snooping on our people. I do not really understand why you are wanting to be protective of the hacker.

Mr. KERR. The difficulty is first identifying who is the hacker. You do not know when somebody is intruding into your network who is behind it. So all you will know is that there is an IP address that seems to back to a specific computer, but you will not know who it is that is behind the attack. That is the difficulty.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The gentleman from Louisiana, Mr. Richmond.

Mr. RICHMOND. Thank you, Mr. Chairman. I guess my first question, maybe first two questions, will go to Mr. Holleyman.

You talked about information sharing, you talked about security, and you talked about oversight over critical networks. And we had that bill last year in Homeland Security, which was the PRECISE Act, which when it came up, the interesting thing about it, it was a pretty decent bill at the time that shared bipartisan support. But when it came up for markup, it was gutted by the author, which was a strange thing, but that is because he could not get leadership to move on the issue and bring it up to a floor vote if that was that comprehensive.

So I guess I am asking you your thoughts on the PRECISE Act, and was that going in the right direction.

Mr. HOLLEYMAN. Thank you for that question. I know that in the last Congress there were a number of pieces of legislation that were considered, several of which were approved. We believe it is important for Congress to supplement what the President did in his executive order with not only oversight, but with additional legislation.

I think the executive order has tried to do—yeah, I would need to look back at the elements of the PRECISE Act to be able to comment further. But I think the President's executive order has tried to address many of the elements that would have been outlined in the PRECISE Act. So whether or not that act would be needed at this point in time, I cannot comment on. I would be happy to look at that for the record.

Mr. RICHMOND. If anyone else wanted to comment on it, that is fine.

My next question would be, you mentioned one of the elements and one of the things we should be doing is continuing or creating a robust R&D for cybersecurity. And I guess my question would be, would that be in the term of maybe an R&D tax credit, or are you thinking of something like NIH and grants to people who want to do that type of research for cybersecurity?

Mr. HOLLEYMAN. Well, I think there are really three elements of it. One is that we do not have enough students who are being trained as professionals to be able to work in cybersecurity for the future, and that is a problem for the private sector and for the government. So we need to have the right education and the right training. Secondly, I think we need the right cooperative agreements between private sector and government to allow that research to happen, including with university research. And certainly, finally there is research that goes on at the Federal Govern-

ment about the level and the nature in evolving threats, and that research needs to be properly funded, and there needs to be proper oversight. So I think it takes all three of those.

Mr. RICHMOND. And I guess I have a third question for you or Mr. Kerr. I think that Ms. Durkan and Mr. Demers will probably know the answer to it. But part of it is from your organization's standpoint and from your experience, the level of cooperation, and information sharing, and assistance that our security agencies provide now. And sometimes we get the benefit of hearings that are not public. But I am interested in knowing from your perspective the interaction between FBI, CIA, Department of Justice, and those in terms of helping either avert or on the back end, find the perpetrators. So how has that been with you all?

Mr. HOLLEYMAN. Well, I will start by saying I think the nature of that is critical, and they are certainly very good relationships. What we need is to be able to share more real time threat information, not simply after the fact, but real time threat information. That is part of what the President has tried to do in his executive order and part of what we think Congress can supplement that would make it even easier and better for industry to share information with the government, too.

Mr. RICHMOND. And I understand the barriers for industry. What is the biggest barrier, or if you want to do it comprehensively, what are the biggest barriers to doing it? Is it just permission and law for real time information sharing?

Mr. HOLLEYMAN. Yeah, I think some of it is sort of the existing laws that private sector companies feel like they must, and appropriately, adhere to, which in some cases makes it difficult, if not impossible, to share real time threat information. So you can only do something about it after the fact. That is not in anyone's interest to do that, so we need the appropriate way to be able to share that with the Federal Government.

Mr. RICHMOND. Mr. Chairman, for the sake of time, I yield back.

Mr. SENSENBRENNER. The time of the gentleman had expired. [Laughter.]

The gentlewoman from California, Ms. Chu.

Ms. CHU. Thank you, Mr. Chair.

I wanted to ask about economic espionage and the stealing of intellectual property, of trade secrets, customer lists, future plans and contracts. And, Mr. Holleyman, I wanted to ask you, you said that Semantic estimated that it lost $110 billion through economic espionage and the stealing of IP through these means.

What do you think is the overall cost to the corporations that you represent?

Mr. HOLLEYMAN. Well, the Semantic number came from their Internet security threat report, and it really related to the total amount of losses. It was not sort of referring to their company losses. And so the figure of $110 billion of damages on consumers is what they cited.

I think that all of the data shows, and certainly the information that is being very public and that the Chairman spoke of in his opening remarks, shows that the nature of the threat is increasing and it is increasing substantially. McAfee, one of our members, estimated that it used to be that a new piece of malware was identi-

fied and put into action about 15 minutes, and now they estimate it is one per second.

So the pace at which this is occurring is huge. The consequence of losses are growing. And this is exactly the kind of hearing this Committee and other Committees should be focused on because we are all in this together.

Ms. CHU. And what is the private sector doing to minimize these intrusions and to protect intellectual property throughout all these layers?

Mr. HOLLEYMAN. Well, I think the Attorney General, the IP enforcement coordinator, the Homeland Security Secretary, about three weeks ago had a major discussion about theft of trade secrets. And I know Members of this Committee were a part of that process.

One, I think it is sort of building awareness. Two, it is building best practices. Three, is security companies. We are working to create faster, more effective ways of preventing these intrusions to share information about the threats when they occur. And it is a race. I mean, it is a race, and we are in the business of trying to help prepare us. But a lot of it is going to take education on the part of businesses, and consumers, and the Federal Government, who is the biggest source of attacks, against the Federal Government. The Federal has to be using the strongest security to try to limit those attacks.

So, I mean, we are all in this together. Our companies want to do more things, particularly in small or medium enterprises and others, build in security procedures, so that if there are breaches of their information, and there will be from time to time, that that information is rendered useless so that the hacker or the perpetrator cannot do anything with it because it is has been secured through encryption or other means. And those additional incentives will be helpful to a long-term solution.

Ms. CHU. I wanted to make sure law enforcement has the tools that it needs to prosecute these cases and investigate them. And Ms. Durkan and Mr. Boles, I want to know, Ms. Durkan, I note that the DoJ leads vigorous prosecutions in cyber theft and economic espionage. I am curious to know how frequently a case regarding intellectual property appears in your case load and if you feel like you have the appropriate tools, like training and funding, to effectively prosecute these cases.

Ms. DURKAN. Thank you. It is a very significant part of our district's work. We have some small mom and pop corporations, like Boeing, Amazon, Microsoft, and the like, where the proprietary information, as the Chairman said, is their most valuable commodity. So we consistently work with those corporations to make sure that we are getting the appropriate referrals.

We have specially trained prosecutors. We will say we always take more resources because the threat is evolving, but we appreciate the resources this Committee has given to us.

Ms. CHU. And, Mr. Boles, do you have the adequate training and funding to carry on your investigations?

Mr. BOLES. Like my partner, Ms. Durkan, said, we will always take more. It is important. It is a high tech and evolving thing.

And just to give you a feel for it, we currently have about 1,100 cases ongoing in the FBI that involve intellectual property theft, and it cuts across all of our programs whether it be cyber, counter intelligence, and in the traditional criminal. So it is a wide-ranging need that we have. And part of our drive is to make sure that all the investigators, and the analysts, and the support folks have the training that they need as we push that out and go forward in the computer world.

But, you know, that is a need that we constantly reassess and try to address.

Mr. SENSENBRENNER. The gentlewoman's time has expired.

The Chair will recognize himself for a couple of questions.

Ms. Durkan, in response to Mr. Scott's question, you said in the Administration's proposal, there are no mandatory minimum sentences. My understanding is the bill the Administration sent us up in the last Congress had mandatory minimums. What made them change their mind?

Ms. DURKAN. We assess a variety of factors, and at this time we are not supporting that. But we would be happy to work with your staff to answer any further questions that the Chairman may have.

Mr. SENSENBRENNER. Well, what factors were those?

Ms. DURKAN. We will look at the number of factors we have to as to what our priorities are in addressing the statute. And right now we see that as the threat is evolving, what we really need are tools that can address some of the gaps we see in the law to make sure that we disrupt, deter crimes in the first instance and hold people accountable.

Mr. SENSENBRENNER. Well, you know, there are two separate things, you know. When we are talking about mandatory minimums, we are talking about after a conviction when the judge pronounces a sentence. There certainly is not a lot of effort and a lot of money that is required to go into that, particularly with a mandatory minimum giving the judge little or no discretion. I think you are trying to confuse apples with oranges and not get into the fact.

Does the Administration oppose mandatory mininums as a matter of principle, or do they not think that the crimes that we are talking about here deserve a mandatory minimum?

Ms. DURKAN. I think what you are getting at, Chairman, is what is the appropriate sanction for these activities, and we agree that we must assess and make sure that these bad actors are held accountable under the law. It is one reason why we support increasing the statutory maximum in the fraud scenario to bring that on par because there are some cases where that is the only statute available, but yet a judge would not be able to assess the nature of the crime that occurred and assess the appropriate penalty.

And so the Department of Justice is always going to look at the factors present in a case and make sure that we are recommending to a judge what the appropriate sanction is. And then, of course, the judge needs to have the discretion and the ability to make sure that that sanction can be imposed so that we both deter the crime in the first instance and hold the people when it occurs.

Mr. SENSENBRENNER. I think we are going to be talking about this issue a lot more as legislation is developed. I disagree with that conclusion.

I do want to spend some time asking two questions of Professor Kerr.

I am a little bit concerned, Professor Kerr, about your idea that there should be certain things that are currently criminal that should not be criminal anymore. And let me pose a hypothetical view. Say that there is a foreign agent that is employed by a U.S. tech company, and he was ordered to check to see that the company was not working on a certain project, using process of elimination to see who is working on that project. The spy exceeds the authorized access and determines that the company really is not working on the project.

Now, in this example, nothing was taken or damaged, but should the Justice Department not have a tool to be able to do something about that, even though another crime was not committed?

Mr. KERR. In that situation, I would imagine there would be another crime committed. I am thinking in terms of attempt liability for attempted—I gather the goal was to ultimately determine confidential information relating to the company as to what the company was or was not doing. So it would be either an attempted theft of that information. I am not sure of the criminal statutes governing spying, for example.

I think the key idea is that it is not a computer-related offense. It just so happens that that offense involves computer-related conduct. But it should be treated under the law just as it would be if the spy were going were going into a locked closet instead of locked computer. It does not make any difference as to whether it is a physical or a computer crime.

So my approach would be just to resolve the circuit split by adopting the 9th Circuit standard, which is treating hacking like hacking and treating computer crime offenses like the physical world analysis.

Mr. SENSENBRENNER. Okay. Well, let me go into the trespass issue that you talked about. Now, it is obvious if somebody got into the mechanical room at Space Mountain at Disneyworld and then pulled the pin on that, and all of a sudden the cars, you know, stopped abruptly and nobody was injured. Maybe it was lucky. But, you know, how about cyber trespass that would have just as much damage, and that would be a violation of a term of service. And should that not be criminalized as well?

Mr. KERR. It should be criminalized, but not because of the terms of service violation. It could be criminalized under a number of different theories.

First, it would be access without authorization because I am assuming that breaking into the computer that is controlling this machine would itself be password protected. It is not like anyone can walk up and pull something on the machine.

Also it would be a Section 1030(a)(5) violation, which is intentionally causing damage to a protected computer without authorization, and that is a separate criminal statute that does not involve unauthorized access. It is sort of intentionally causing damage without authorization.

So these are all situations that would already be criminalized without the need to go to the unauthorized access prohibition.

Mr. SENSENBRENNER. Okay. Well, my time is up.

So I would like to thank all of the witnesses for appearing today, for being brief in the answers to your questions so that we Republicans can go listen to what the President has to say. And I understand you Democrats will have that pleasure sometime in the future, very soon.

So without objection, this hearing is adjourned.

[Whereupon, at 12:54 p.m., the Subcommittee was adjourned.]