

S. HRG. 114-906

# CYBER CRIME: MODERNIZING OUR LEGAL FRAMEWORK FOR THE INFORMATION AGE

---

## HEARING BEFORE THE SUBCOMMITTEE ON CRIME AND TERRORISM OF THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JULY 8, 2015

**Serial No. J-114-23**

Printed for the use of the Committee on the Judiciary



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

U.S. GOVERNMENT PUBLISHING OFFICE

## COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

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

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

KRISTINE LUCIUS, *Democratic Chief Counsel and Staff Director*

## SUBCOMMITTEE ON CRIME AND TERRORISM

LINDSEY O. GRAHAM, South Carolina, *Chairman*

|                          |                                                         |
|--------------------------|---------------------------------------------------------|
| DAVID VITTER, Louisiana  | SHELDON WHITEHOUSE, Rhode Island, <i>Ranking Member</i> |
| JEFF SESSIONS, Louisiana |                                                         |
| JOHN CORNYN, Texas       | CHARLES E. SCHUMER, New York                            |
| JEFF FLAKE, Arizona      | AMY KLOBUCHAR, Minnesota                                |
|                          | AL FRANKEN, Minnesota                                   |

DAVID GLACCUM, *Majority Chief Counsel*

AYO GRIFFIN, *Minority Chief Counsel*

# CONTENTS

---

## OPENING STATEMENTS

|                               | Page |
|-------------------------------|------|
| Graham, Hon. Lindsey O. ....  | 1    |
| Whitehouse, Hon. Sheldon .... | 3    |

## WITNESSES

|                                                     |    |
|-----------------------------------------------------|----|
| Bitkower, David .....                               | 4  |
| Prepared statement .....                            | 28 |
| Questions submitted with no response returned ..... | 66 |
| Ellis, Jen .....                                    | 17 |
| Prepared statement .....                            | 53 |
| Responses to written questions .....                | 68 |
| Johnson, Doug .....                                 | 15 |
| Prepared statement .....                            | 45 |
| Wright, Bill .....                                  | 18 |
| Prepared statement .....                            | 56 |

## APPENDIX

|                                      |    |
|--------------------------------------|----|
| Items submitted for the record ..... | 27 |
|--------------------------------------|----|



## **CYBER CRIME: MODERNIZING OUR LEGAL FRAMEWORK FOR THE INFORMATION AGE**

**WEDNESDAY, JULY 8, 2015**

UNITED STATES SENATE,  
COMMITTEE ON THE JUDICIARY,  
SUBCOMMITTEE ON CRIME AND TERRORISM,  
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 2:21 p.m., in Room 226, Dirksen Senate Office Building, Hon. Lindsey O. Graham, Chairman of the Subcommittee, presiding.

Present: Senators Graham [presiding], Cornyn, Whitehouse, Klobuchar, and Blumenthal.

### **OPENING STATEMENT OF HON. LINDSEY O. GRAHAM, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA**

Chairman GRAHAM. The Subcommittee will come to order. Senator Whitehouse is on his way, but I have been told I can go ahead and start.

The title of this hearing is “Cyber Crime: Modernizing our Legal Framework for the Information Age,” and we have a very great panel, two panels, and I will go ahead and get started.

Senator Whitehouse is probably the most informed person I have ever dealt with regarding all things cyber. I have enjoyed the relationship we have had as Chairman and when he was in charge. We had a good working relationship. He has been trying to push the Congress, the Senate in particular, to get more serious about the cyber threats we face.

Today we are talking about the criminal aspects, espionage and theft. They tell me by 2029, that we can expect between espionage—cyber espionage and cyber theft, that could affect the world to about a trillion dollars. That is a stunning number to me, that as we look out into the future cyber espionage, stealing intellectual property, to get an advantage economically and literally stealing money out of an account could account for a trillion dollars worth of theft.

Having a bank robber come into a bank and rob the bank and loot your account is one problem. When you compare the threats we face as a Nation to a cyber attack on a bank, they pale in comparison.

The FBI and other organizations that I have been dealing with worry greatly about cyber attacks on our financial institutions. The legal framework we have in place is 20 years old, and technology has changed a great deal since then. The purpose of this hearing

is to get ahead of what I think is going to be a major drain on our economy and, quite frankly, a threat to our way of life.

Those of us who bank assume certain things; that when we put the money in the bank, it is going to be safely guarded and that we can rely upon our deposit being there when we need it. At the end of the day, our banking and financial services industry are under constant siege by criminal networks all over the world, many tied to terrorist organizations, constantly trying to break into their systems to steal money.

On the commercial espionage front, nation-states like China, but other criminal enterprises, are constantly trying to short circuit the development of technology and steal intellectual property that has been developed in this country and other places through hard work and investment.

I hope that the Congress will look at the draft that we have sent out from myself and Senator Whitehouse that Members of the Senate will look at it. We can get input and bipartisan support for what we are trying to do. Now, comes Senator Whitehouse. At the end of the day, I am very concerned about where the criminal enterprise in cyber is headed. We need to reform our laws and up our game and I would end on this.

Under sequestration, the ability to defend this Nation against cyber threats is going down, not up. The FBI and other organizations at the Department of Justice tasked with defending us against cyber crime and espionage, their budget is going to be dramatically affected if sequestration is fully implemented.

We often talk about the Department of Defense going down to 420,000 personnel in the United States Army, the smallest Navy since 1915; one contingency Marine Corps and half the fighter squadrons in the Air force not being combat ready as a result of sequestration.

We do not, in my view, talk enough about how our national security is affected on the nondefense side. How our way of life is very much at risk. The Department of Justice is on the front lines of many endeavors to protect this Nation, but you are the lead organization, the lead agency when it comes to dealing with cyber theft, cyber espionage and cyber crime.

What we are doing in my view is short circuiting the ability to defend this Nation, requiring the Department of Justice to have to make draconian decisions between the growing threat of cyber crime and lone wolf attacks on our country. To those who say that we do not need to deal with sequestration on the nondefense side, I would argue that the Department of Justice, the FBI and other organizations are prime example of what we are losing in terms of capability if we continue to implement sequestration.

We expect you to do more in the cyber arena. We expect you to do more in the lone wolf arena. We expect you to keep us safe, but our expectations are not realistic given what we are doing to your budgets, and it is just a matter of time before we pay a heavy price of short changing those who are defending this country.

With that, I will turn it over to Senator Whitehouse.

**OPENING STATEMENT OF HON. SHELDON WHITEHOUSE,  
A U.S. SENATOR FROM THE STATE OF RHODE ISLAND**

Senator WHITEHOUSE. Thank you, Chairman. First of all, congratulations on your birthday, I think, tomorrow. Second, congratulations on the terrific leadership that you and our colleague, Senator Scott, showed in the wake of the tragedy in your home State, in Charleston. Thank you for the very strong bipartisan cooperation you have showed on cyber issues not just through this hearing, but back when we were trying to negotiate a comprehensive cyber bill and actually came pretty darn close.

This hearing is important, and I am really grateful that you have allowed it to go forward and have been such a staunch advocate for these issues.

The seriousness of the cyber threat is no longer a matter of debate. Recent events have made this very clear. Hackers have infiltrated sensitive State and Federal networks, they have stolen data on millions of Americans, terrorist groups around the world are expanding their efforts to wage cyber war against our critical infrastructure.

American businesses continue to suffer relentless theft of their valuable intellectual property. Fighting this threat requires we have to do a better job of securing government networks, business and individual computers, we have to be better secured and really basic steps maintained by their private sector owners to protect their data and keep themselves from becoming victims.

We need to increase the threat information that is shared between the private sector and the Government, but we cannot just play defense. Here in this Committee in particular we are interested to see that we go after cyber criminals and see to it that they are arrested and prosecuted wherever they may be found.

I am encouraged that Federal law enforcement agencies and DOJ prosecutors are increasing their efforts to hold cyber criminals accountable.

Just 2 weeks ago, one of the world's most wanted cyber criminals, Ercan, I am not sure I can pronounce this, Findikoglu, a man believed to be responsible for stealing more than \$50 million from banks around the world was extradited to the United States where he now sits in an American jail awaiting trial.

The leader of the international Blackshades criminal network, Alex Yucel, was recently sentenced to prison in an American courtroom for producing and selling a powerful form of malicious software that could be bought for less than \$50 and was capable of taking complete control over victims' computers. Chinese military officers have been indicted by a U.S. grand jury. These are all very positive signs and I hope we see more action in the future.

We have a responsibility in this Committee to make sure that our laws are up to date and many of our key cyber laws are as much as 30 years old. We could not then have anticipated the cyber universe we live in now and so we need to update things. I look forward to today's hearing. I hope our witnesses will share their thoughts about how we can update and strengthen our laws against cyber crime.

I look forward to working with Chairman Graham in the days and weeks ahead to enact legislation that will give prosecutors and

law enforcement agencies new and improved tools to go after criminal actors while protecting the legitimate activities millions of Americans engage in every day on the internet.

If we take a balanced, thoughtful approach, I believe we can update our laws to strengthen our ability to stop hackers, to shut down botnets, to bring cyber criminals to justice, all while providing greater clarity for security researchers and ordinary internet users who should not have to fear Federal prosecution.

I look forward to working with Chairman Graham toward that goal and I appreciate the witnesses being here today. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you. Could you please stand?

[Witnesses are sworn in.]

Senator GRAHAM. Our first witness is Mr. David Bitkower. Did I get that right?

Mr. BITKOWER. You did, sir.

Chairman GRAHAM. Great. Deputy Assistant Attorney General, U.S. Department of Justice, Criminal Division and one of the leading experts on this area of the law. Welcome to the Committee.

**STATEMENT OF HON. DAVID BITKOWER, DEPUTY  
ASSISTANT ATTORNEY GENERAL, U.S.  
DEPARTMENT OF JUSTICE, CRIMINAL DIVISION  
WASHINGTON, DC**

Mr. BITKOWER. Thank you and good afternoon, Chairman Graham, Ranking Member Whitehouse and Members of the Subcommittee. Thank you for the opportunity to be here today to discuss legislative proposals that will enhance our ability to combat cyber crime and protect the privacy and the security of the American people.

In particular, I would like to thank the Chair and the Ranking Member for their continued leadership on these important issues and also to wish the Chair a happy birthday.

As the Attorney General has emphasized, fighting cyber crime is one of our Justice Department's highest priorities. Every day our society becomes more reliant on computer networks and electronic devices in almost every aspect of our lives.

At the same time, however, individual hackers, organized criminal groups and nation-states are becoming more sophisticated at using these networks and devices against us—stealing from our bank accounts, compromising sensitive and private information and even spying on innocent citizens through their webcams.

These invasions of privacy make us feel vulnerable and unsafe and rightly so. The effects of these crimes are only compounded when we realize that cyber criminals often sell the stolen data to other criminals or even use it to extort and terrorize their victims.

The Department's prosecutors and our law enforcement partners strive to protect our citizens and businesses and vindicate their privacy rights, but our laws have not always kept pace with global realities and advances in technology. That is why earlier this year the President announced legislative proposals designed to protect the online privacy and security of American citizens and companies.

Among these proposals were targeted updates to the criminal laws that govern cyber crime. I would like to specifically discuss two of those proposals today. The first one addresses the “insider threat,” the threat to privacy and security caused by computer users who are authorized to access computers and networks but exceed that authority.

As you know, the Computer Fraud and Abuse Act, or CFAA, is the primary statute that we use to charge computer crime cases. It applies to hackers located on the other side of the world who have no right to access your data, but it is also the statute we use to prosecute individuals such as Government or corporate employees who knowingly abuse their access to misappropriate sensitive data.

For example, we have used this provision of the CFAA to charge corrupt police officers who were entitled to access law enforcement databases for official police purposes but who instead obtained confidential information from databases for personal reasons, or so they could sell it for profit.

The same provision would also apply to corporate employees whose employers grant them specialized access to valuable information so they can do their jobs, but who then access that information contrary to their authorization.

Unfortunately, recent judicial decisions have imposed obstacles to the Government’s ability to prosecute cases like this in large parts of the country. As a result, corrupt insiders may be effectively immune from prosecution under the CFAA, even when they intentionally exceed the bounds of their legitimate access and steal their employer’s intellectual property or invade the privacy of the people whose data is improperly accessed.

These judicial decisions stem from the concern that the relevant provision of the CFAA could potentially make relatively trivial conduct a Federal crime such as checking baseball scores during lunch in violation of an employer’s internet use policy.

The Department has no interest in prosecuting such harmless acts. That is why we have proposed amendments to the CFAA that would address this concern while also making sure the law applies to those who commit serious security violations and invasions of privacy.

We look forward to discussing these proposals further with the Subcommittee. The second legislative proposal I would like to highlight now would enhance our ability to combat botnets.

As you know, botnets are networks of victim computers surreptitiously infected with malware, and criminals can use botnets to steal personal information from the infected computers or even hold that information for ransom.

Criminals can also use botnets to commit distributed denial of service attacks or to conceal their locations and identities while committing other crimes such as exploiting children online.

One powerful tool that the Department has used to disrupt botnets and free victim computers is the civil injunction. For example, civil injunctions were instrumental in our successful operations against the Coreflood and Gameover Zeus botnets, which liberated hundreds of thousands of compromised computers from the criminals who controlled them.

The problem is that current law only permits courts to consider injunctions for a limited category of crimes such as certain financial frauds. Botnets, however, can be used for other kinds of illegal conduct as well, and the administration has therefore proposed clarifying that injunctions are available for the full range of crimes that botnets are used to commit.

In my written statement, I describe several other legislative proposals that address problems such as spyware and the sale of our financial information abroad. We look forward to working with this Committee to address all of these issues in order to effectively protect the privacy and security of our citizens and businesses.

Our cyber crime laws must continue to evolve to counter these cyber threats. Thank you, and I look forward to answering any questions.

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

Chairman GRAHAM. Thank you, very much. Have you been provided our discussion draft between me and Senator Whitehouse about how we can improve the statutes in question?

Mr. BITKOWER. Yes, Senator.

Chairman GRAHAM. What is your general view of what we are trying to do?

Mr. BITKOWER. As a general matter, we think the discussion draft is an excellent start, and it has many proposals that will increase our ability to combat cyber crime.

Chairman GRAHAM. To the average American, how would you explain the gap we have between the laws we need and the laws we have when it comes to protecting against corporate espionage, against basic theft of your hard earned money if it is in a bank or some other financial institution? What is the gap?

Mr. BITKOWER. Senator, the proposals that we have made and the proposals that your discussion draft addresses are, I think it is fair to say, a targeted set of enhancements to the current laws that we have.

We do have currently authorities and capabilities to address a vast array of cyber crime, but we have observed through the prosecutions and investigations we have done that there are gaps in very specific areas such as the ones I just discussed in my opening statement.

When it comes to corporate espionage, I think the biggest statutory gap we have now is the problem with being able to address insider threats in those affected circuits.

Chairman GRAHAM. If we could pass something like the draft proposal, do you think we would substantially close those gaps?

Mr. BITKOWER. I think we would substantially close the statutory gaps, yes, sir.

Chairman GRAHAM. Okay. If we failed to do so, what does that mean?

Mr. BITKOWER. That means that there are certain categories of criminal cyber activity that we are seeing today which will continue to go unaddressed.

Chairman GRAHAM. Okay. From an average American's point of view, what is more likely to happen to your money, a cyber theft or a bank robbery?

Mr. BITKOWER. I think doubtlessly a loss of financial information from a cyber theft is much more likely to occur.

Chairman GRAHAM. Thank you. Senator Whitehouse.

Senator WHITEHOUSE. With your permission, Mr. Chairman, I would like to yield to Senator Blumenthal, whose schedule is pressing and who needs to move on, and if it is fine with you, I will let him take my time and I will take his.

Senator BLUMENTHAL. Thanks. Thank you very much, Mr. Chairman, and I appreciate your having this hearing on this very important topic.

As you know, in the *Nosal* case, the 9th Circuit held if Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly, and then the circuit court went on, as you also know, to say that its narrow interpretation of the statute is, quote, “more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking the circumvent—circumvention of technological access barriers, not misappropriation of trade secrets, a subject Congress has dealt with elsewhere,” end of quote.

The administration’s recent proposal on cyber crime defines “exceeds authorized access” in very broad terms simply as, and I am quoting, “for the purpose that the accessor knows is not authorized by the computer owner,” end of quote.

In your view, will that kind of broad terminology actually provide prosecutors and courts with the clarity they need?

Mr. BITKOWER. Thank you for the question, Senator Blumenthal, and yes, we believe that the language in our proposal would provide courts with the clarity that they need to address this threat.

In fact, of course we thought that was one intent of Congress in the first instance when it passed the CFAA, but I think at this point after the circuit court decision you described, it would be helpful to clarify that.

Senator BLUMENTHAL. It would be helpful to clarify it?

Mr. BITKOWER. Yes.

Senator BLUMENTHAL. Because if your intent is not to include trivial offenses such as minor violations of the website’s use policy, there need to be mechanisms in place to provide protections for a person who may not know that their conduct violates the computer’s authorization but believes that their conduct may be harmless, and the kind of clarity you are talking about, I think, is necessary with such an expansive terminology.

Mr. BITKOWER. Yes, Senator, and there are, in fact, two different protections there that would protect against prosecution for trivial conduct.

The first is the one you have identified that the statute would clarify that the accessor would have to know that their access was not authorized by the computer owner and as a second matter, the Government has proposed adding requirements to this provision of the CFAA, which would in fact narrow the application of the statute overall and only apply it in certain categories where valuable or sensitive information was accessed.

Senator BLUMENTHAL. Then going to the \$5,000 figure, how did you arrive at that figure? What is the rationale or justification for it?

Mr. BITKOWER. Senator, the \$5,000 number is one that in our view sets an appropriate line that carves out trivial or very minor conduct that the Federal Government would not typically have an interest in prosecuting.

It is a number that appears in other similar statutes involving the theft of stolen property and the possession of stolen property, so it is a number that already exists in the code. It also already exists in the CFAA as an aggravating factor to separate harmful hacks from less harmful hacks.

Senator BLUMENTHAL. I am aware that it is used elsewhere in the code where perhaps the loss is more easily quantifiable where the financial impact is more easily or readily measurable.

I am wondering whether it might fail to capture some of the serious crimes that may not meet that threshold.

Mr. BITKOWER. I think it is certainly correct that when we set a financial threshold to apply to exceeds authorized access violations, there will be certain violations that might be culpable or harmful that will not be able to be prosecuted anymore.

The goal that we were following in trying to set a financial threshold was to make clear that for the category of truly trivial or harmless violations, not only are we not interested in prosecuting those cases, we think that ensuring that the law clearly applies to the serious crimes that we are trying to prosecute, it is worth it to make clear that there is that line. It is true however that that is a compromise position that you are hearing from the Government.

Senator BLUMENTHAL. Thank you. I appreciate your helpful testimony today and I look forward to continuing this conversation. Thanks.

Mr. BITKOWER. Thank you.

Chairman GRAHAM. Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman. Mr. Bitkower, welcome. It recently came to light that the Saint Louis Cardinals are under investigation for hacking the proprietary database of the Houston Astros which happens to have the best record in the American League West.

I am not sure if it is fear or jealousy, but it could be difficult for a dynasty to watch an upstart like the Astros. I think we would all agree that none of this would justify cheating, or as appears to be the case here, potential criminal activity, and I hope the FBI and DOJ will take the ongoing investigation into any criminal activity seriously and ensure that any wrongdoing is fully investigated and prosecuted.

According to reports, Cardinal's employees used a list of passwords left behind by Jeff Luhnow when he moved from the Cardinals to the Astros to log into the Astro system. I would just like to ask you a few hypotheticals, recognizing that we do not have all the facts, and we trust a thorough investigation will take place.

Assuming these facts are true, is there a potential violation of the Computer Fraud and Abuse Act's prohibition against accessing a protected computer without authorization?

Mr. BITKOWER. Thank you, Senator, and, of course, and as you note, I am not in a position to talk about any particular case or any ongoing investigation.

As a general matter, accessing a protected computer without authorization would be a violation of the CFAA.

Senator CORNYN. As a general matter, could accessing such information which would include trade secrets by the Astros, would that—does that give rise to a potential illegal economic espionage charge as well?

Mr. BITKOWER. Again, as a general matter, accessing trade secrets from a protected computer could potentially violate two different statutes, both the protection for the computer itself under the CFAA as well as the trade secret statute.

Senator CORNYN. As a general matter, if the leadership were aware of that hacking, could that mean that in addition to its employees, the franchise included could be charged with a violation of CFAA or trade secret laws?

Mr. BITKOWER. Again, speaking generally the question now goes, I think, to accessorial liability for a particular violation and the doctrines and statutes that govern whether one individual can be liable for the conduct of another are very fact specific.

Certainly if there was a common plan or agreement to violate the law, there could be liability there.

Senator CORNYN. My last question along these lines, hypothetical, a general question. What sort of remedies could be available for such illegal access to computer systems, assuming this general set of facts prove to be true?

Mr. BITKOWER. Again, without regard to any particular set of facts or any particular case, the CFAA carries both criminal liability as well as civil liability.

Senator CORNYN. Let me ask you about the OPM hack. According to reports, the personal information of up to 18 million Americans was stolen from the Office of Personnel Management.

Because the stolen information has not yet appeared for sale on the dark web and the hack reportedly bears the signatures of Chinese hackers, many experts are saying that the Chinese government is using the data breach to build a database of personal information on Federal employees and, of course, some of the reports are that the very security clearance application forms with extensive personal information would be included, which would of course allow the hackers to build a profile on people who have classifications or who hold classified clearances.

If this is true, what sort of remedies might be available to deal with such actions?

Mr. BITKOWER. Senator, again to just point out that, of course, I cannot comment on any particular investigation. The FBI is, of course, hard at work in investigating the OPM hack and, of course, I have read the same reports that you have and that you refer to today.

If we talk about criminal access to Government databases, again the CFAA could well be implicated if there is unauthorized access to those databases. In fact, putting aside hacking by outsiders or hacking by foreign nation-states, one of the purposes of our targeted update proposals today is to make sure we can prosecute those cases even if it is an insider who is involved in a particular attack.

When we pull back and look at the larger spectrum of cyber threats that include those from nation-states, criminal prosecution definitely can be part of our set of responses, but it certainly is not going to be a complete response, and the administration has taken a holistic approach that includes both criminal prosecution, diplomatic trade policy and other responses.

Senator CORNYN. Refresh my memory, if the Chairman will indulge me. It seems to me the U.S. Government indicted four Chinese individuals for computer hacking in the not too distant past, but that is mainly a symbolic gesture because without ability to extradite those people for prosecution, that prosecution is not likely to occur. Do you agree?

Mr. BITKOWER. Senator, first of all we did indict five individuals last year. That prosecution is being handled by our National Security Division and the U.S. Attorney's Office in Pittsburgh.

As a general matter, again without reference to this particular case, we do often indict foreign actors operating from abroad and they do often find themselves in American courtrooms to face justice. We would not rule out that justice could be achieved in any particular case.

Senator CORNYN. They find themselves in American courtrooms?

Mr. BITKOWER. Yes, sir.

Senator CORNYN. That is what I thought you said. Thank you.

Chairman GRAHAM. Let it be said that the Astros have no bigger fan or supporter than John Cornyn.

[Laughter.]

Senator WHITEHOUSE. We will stipulate to that.

Chairman GRAHAM. Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman. I appreciate this. Thank you, Mr. Bitkower, for being here and also for your service to our country in a very complicated and fast moving area.

The bill that we have been talking with you about focuses on foreign actors in a number of different ways. It clarifies that U.S. economic espionage statutes cover acts that are committed on behalf of a foreign government. It clarifies that foreign individuals who possess or traffic in American credit card numbers can be prosecuted even if they are not in the United States doing their criminal act.

It improved the capacity for service on foreign defendants. In the spirit of those elements, could you just tell us a little bit about, in your experience, what is the role in the significance of foreign actors in cyber crime?

Mr. BITKOWER. Thank you, Senator, and thank you for the opportunity to answer that question. There is no doubt that in just about every complex cyber crime matter we handle here at the Department of Justice there is some foreign element of one kind or another. Whether it is individuals acting from abroad to target Americans or even individuals acting from the United States but using criminal infrastructure that can be located abroad in whole or part, and even individuals acting here where evidence winds up being abroad and in order to successfully investigate and prosecute the crime, we need access to that evidence.

When we talk about foreign actors in particular, we have certainly seen foreign actors around the globe targeting American sys-

tems because of the valuable and sensitive information that is contained there. One of the greatest challenges we have in investigating and prosecuting these crimes is not only being able to prove what happened, but also attempting as Senator Cornyn referred to, to get them into our courtrooms to face justice.

Senator WHITEHOUSE. Fair to say that the internet has knocked down geographic borders that has made American victims much more vulnerable to people who have never even set foot in the country but have access to a keyboard in Russia and Latvia and a great number of places around the world?

Mr. BITKOWER. That is exactly right.

Senator WHITEHOUSE. The legislation would make certain conduct a money laundering predicate or a RICO predicate. Could you tell us what the value is in making an offense a money laundering predicate or a RICO predicate?

Mr. BITKOWER. Certainly, Senator. One of the things we have observed in cyber crime in recent years is that organized criminal groups follow the money and they have observed that the internet is an excellent way to victimize Americans and American businesses. Therefore, complex cyber crime cases are often committed by organizations and they may even have an assembly line type of structure where one individual may develop the software to commit an intrusion, another individual may execute that intrusion and exfiltrate data. A third individual or set of individuals may then monetize that data by creating fake ATM cards or through other means.

When we encounter criminal organizations, we find it is very effective to use the RICO statute. When they are, of course, using money to further their crimes or to conceal their profits, we like to use our money laundering statutes as well to make sure we hit them in the pocketbook.

Adding the hacking statute as a predicate for money laundering or RICO would allow us in certain cases where we are targeting a criminal organization to do a more effective job of making sure that the charges capture the full range of activity and the sentence reflects the appropriate range of conduct.

Senator WHITEHOUSE. The size of these foreign criminal activities can be?

Mr. BITKOWER. They can be millions, tens of millions, hundreds of millions of dollars. We have an ongoing of actors involved in a carding forum.

We have charged over 50 individuals. We have now convicted over 25 and the conduct in that case caused tens of millions of dollars in losses.

Senator WHITEHOUSE. Mr. Bitkower, I have admired the Department of Justice's civil efforts to go after botnets, starting with Coreflood and then onto Gameover Zeus and others. That is not traditionally part of the criminal law brief of the Criminal Division or the Division, but purging the net of these botnets really damages the criminal potential that they have for criminal actors.

How has the integration been between the civil folks who are doing these botnet take downs and the criminal side? Sometimes there is a bit of tension between criminal and civil actors in the Department.

I gather that has been cured, but I would just like to hear your assessment of how well integrated the civil process on botnets is and to your overall criminal pursuit of these malefactors.

Mr. BITKOWER. Thank you, Senator. As you point out, when we attack the botnet threat, occasionally we use our traditional criminal tools such as arrest warrants or search warrants to seize and take down infrastructure, but occasionally we do have to use civil authority to do a more technical remediation of the harm caused by a botnet.

We have a little more practice with it now than we did earlier and the expertise that has been developed over time in the Department, particularly in the last 5 years is still retained and centralized within our Computer Crime and Intellectual Property Section in the Criminal Division.

Senator WHITEHOUSE. It has been institutionalized.

Mr. BITKOWER. It has, sir.

Senator WHITEHOUSE. Very well. Great. I appreciate you being here and I thank you for your testimony and for your work and I thank you particularly for your support of the way in which we have narrowed the Computer Fraud and Abuse Statute.

It is not often that prosecutors like to see statutes narrowed, but I think it is pretty clear that this will be a good step in terms of going after the real criminals without risking concerns that innocent actors might get swept up or trivial, to use your phrase, acts might get swept up in it. Thank you for that.

Mr. BITKOWER. Thank you. We share that goal.

Senator WHITEHOUSE. Mr. Chairman.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you so much, Mr. Bitkower, for being here and for your work.

In your opinion, what are the two or three gravest threats to our national security when it comes to computer fraud?

Mr. BITKOWER. Senator, that is a difficult question because many of the gravest threats are ones that thankfully are still in our heads. Certainly, we look to protect our national security information from breach and being obtained by foreign actors.

Obviously we look to protect our critical infrastructure that is essential to the way our country operates. It goes without saying, I think that the valuable trade secrets, intellectual property of American businesses is vital to our national security and to our future success.

Senator KLOBUCHAR. Good answers. This morning we actually had an interesting hearing on encryption, and I do not think anyone has asked you about that yet and your view on that.

I mean, I thought that the Deputy Attorney General and that the Director of the FBI made a pretty good case for why they are concerned about this, that you would no longer have access when tracking down criminal cases.

Could you talk about your perspective on that from a sort of a computer fraud, that type of perspective?

Mr. BITKOWER. Thank you, Senator, and certainly the Deputy Attorney General and the Director of the FBI speak for the Department on these issues, so, I certainly second whatever it is they said this morning, which I did not have the opportunity to hear.

I would note from a cyber perspective we definitely do see encryption being used as a tool to further crime. In particular, in some of our botnet cases, we have seen criminal actors using encryption as a means of protecting their criminal network to ensure that it can continue to victimize Americans.

Senator KLOBUCHAR. Very good. I think a lot of the focus we had there was how law enforcement will be able to continue their work where they are trying to track people down if they are encrypted, and I would think that you would have that same concern. That is what you are talking about?

Mr. BITKOWER. Yes, Senator, and it goes beyond mere encryption of data. The access to electronic evidence in a variety of contexts is essential to investigating and prosecuting these cases.

Senator KLOBUCHAR. Very good. As you discussed in your testimony, the President has announced new legislative proposals to update the Computer Fraud and Abuse Act, including making it clear that an insider who uses data inappropriately violates the CFAA and that those who sell financial data overseas are covered by the Act.

You described these proposals are targeted and previous reforms to the legislation is modest. Given the growth and sophistication and frequency of cyber crime, how much will these reforms help? In a perfect world, what would you like to see us pass? Two different questions.

Mr. BITKOWER. Yes, Senator, but two questions I am very happy to answer. As you have seen, the administration's proposals, I do think they are targeted. I do not think we are under the illusion they are going to solve the cyber crime problem that we face today, but they will solve the problems that we have seen in sets of investigations that we are currently facing.

Every one of these proposals, I believe, came out of actual case experience that our prosecutors have seen in cases where we either could not achieve the appropriate result or almost could not achieve the appropriate result because of these particular fact patterns.

We are trying to advance the ball, but we recognize that there are other things that we have to do as a Nation to make ourselves more secure.

Senator KLOBUCHAR. Again, if you could wave a wand, what tools would you really like to see that you think would be helpful? Are there any other additional tools? I would think you would say resources, other things.

Mr. BITKOWER. Certainly, other than the proposals we have set forth in the President's legislative proposals, certainly resources are a major concern for us. Just to give a sense of scale, the Gameover Zeus botnet that the Department was able to take down last year was responsible for over \$100 million in losses to our Nation's businesses, particularly small- and mid-size businesses, and that number alone is over 10 times the budget of our Computer Crime and Intellectual Property Section for a year.

Senator KLOBUCHAR. Yes. We had a vote recently, there is a bill that has come through, a bipartisan bill actually through the Intelligence Committee. You focused when you mentioned your three

biggest national security threats, one of them was business information and intellectual property.

That bill, which I hope we vote on again, would make it easier for businesses to share information with the Government and report breaches and things like that. Having come from the State which had a company, I do not ever want to bring them down into the ground because they were victims of this, that had one of these major hacking incidences. Do you think this would be helpful in terms of sharing information of these breaches?

Mr. BITKOWER. Yes, Senator. The administration believes that legislation absolutely is necessary to promote better cybersecurity information sharing between the Government and the private sector and also to encourage information sharing among the private sector.

Senator KLOBUCHAR. I have had interesting debates on that with some of my colleagues. Most people are for that bill, as you know, both Democrats and Republicans, despite the vote which I guess was for other reasons.

There are some people who are against it and they think that that will open us up somehow to more data breaches if somehow the sharing is done. I have tried to explain that explicitly in the bill as the provision that the personal data is not shared, just generally, and how do you respond to that argument?

Because my perspective on this is if we just keep going the way we are and do not come up with more sophisticated ways to go after the crooks, they are just going to become more sophisticated about stealing our data and pretty soon we are going to be protecting no one's privacy because they are going to be able to hack into it.

Mr. BITKOWER. Senator, certainly we agree with you in a principle. We are still reviewing the particular text of the Senate Intelligence Committee's bill that I believe you are referring to and we are aware that some have expressed concerns about privacy protections in the bill, but we look forward to working with this Committee and other committees to improve the bill and make sure it can pass.

Senator KLOBUCHAR. Thank you very much. I appreciate it.

Chairman GRAHAM. Any other questions? One final question. In terms of the terrorist world, how much are they being enriched by these cyber crimes? Is there a connection between terrorist organizations and the thefts we are talking about?

Mr. BITKOWER. Senator, terrorist access to our networks would obviously be a nightmare scenario, and I think that is information that we could probably get to you in another setting.

Chairman GRAHAM. Okay. Thank you.

Mr. BITKOWER. Thank you.

Senator WHITEHOUSE. Mr. Chairman, as Mr. Bitkower leaves, I just want to note that he has a really exemplary academic record, record of judicial clerkships. He has been awarded the Attorney General's Award for Exceptional Service, which is an extraordinarily high honor within the Department of Justice, as well as the Henry Stimson Medal, which is given by the New York City Bar to the folks, U.S. attorneys in the New York City area, and that represents the kind of people that Department of Justice can

draw into service to your point that if we are not kicking the Department of Justice in the face with sequestration, we can continue to attract people like Mr. Bitkower and have them feel rewarded at least in some ways even if they are never going to be rewarded in the ways that big corporate law firms can reward them. I heartily endorse your earlier comments about sequestration.

Chairman GRAHAM. Thank you very much, Mr. Bitkower.

Mr. BITKOWER. Thank you.

Chairman GRAHAM. Next panel, please.

[Pause.]

Chairman GRAHAM. Thank you all for coming. Please stand.

[Witnesses are sworn in.]

Chairman GRAHAM. Our second panel is Mr. Doug Johnson, senior vice president and chief advisor, payments and cybersecurity policy, American Bankers Association; Ms. Jen Ellis, senior director of community and public affairs, Rapid7; and Mr. Bill Wright, director, government affairs global cybersecurity partnerships, Symantec.

All of you are experts in your area. Thank you very much for taking time to come to the Committee, and we will start with Mr. Johnson and go to my right.

**STATEMENT OF DOUG JOHNSON, SENIOR  
VICE PRESIDENT AND CHIEF ADVISOR,  
PAYMENTS AND CYBERSECURITY POLICY,  
AMERICAN BANKERS ASSOCIATION  
WASHINGTON, DC**

Mr. JOHNSON. Thank you, sir. Chairman Graham, Ranking Member Whitehouse and Members of the Subcommittee, my name is Doug Johnson. I am senior vice president of payments in cybersecurity policy for the American Bankers Association.

I also have the privilege of serving as the vice chairman of the Financial Services Sector Coordinating Council, and I am also on the board of the Financial Services Information Sharing and Analysis Center as well, and I certainly do appreciate the opportunity today to speak to you and discuss the importance of modernizing our legal framework in the current cyber crime environment.

As the 114th Congress engages in public debate on the important issue of cybersecurity and cyber crime, we share your concerns about the need to modernize our laws, to meet the cybersecurity challenges our Nation faces. Cyber threats to the U.S. national and economic security are increasing in frequency, scale, sophistication and severity of impact.

Attacks that once were singular in focus, be it a denial of service attack on a financial institution, an attack on a merchant point of sale, or an attempt to destroy or wipe data from an energy company, it may now contain a variety of such attack vectors; many such multifaceted attacks create particular challenges for the victimized company or companies, necessitating the simultaneous maintenance of availability, integrity and confidentiality of data where formally a cyber attack might have impacted only one of these vital data security components.

The significant and purportedly nation-state-based denial of service attacks that were experienced by our financial sector, I think,

demonstrated our capacity to, through the FS-ISAC, act collectively to respond to major attacks and minimize their capacity to essentially cascade through our financial sector.

Our sector has also initiated civil legal action in conjunction with the FS-ISAC and Microsoft. I think that we actually, 5 years ago, were the first to really attempt botnet takedowns and did it essentially as a private sector, and we very much welcome the fact that now it is a partnership between the private and the public sector, and I think that the fact that we have a recent very successful case of an international botnet takedown when we are talking about the Beebone botnet, I think that is a very good sign of really what is to come, because essentially that was a court authorized seizure of over 1,000 domains and those infected PC's no longer report to a criminal. They report to Europol's European Cyber Crime Center.

For at least a moment in time, they are safe and they are being cleansed as individual PC's, and I think while we always have to continually refresh that process, I think this is an impressive level of international law enforcement cooperation and should serve as our model going forward.

We also support the administration's Executive order on sanctions. We do believe that attackers are becoming increasingly adept at defeating cybersecurity practices and mitigating measures point to the need for industry and Government to develop and deploy enhanced measures with ongoing speed.

While threat detection information sharing and incident response capabilities within our sector leave us well positioned to withstand such attacks, we also must increase the potential for our attackers to feel real consequences associated with these attacks.

The nation-states that generally attack us deny attribution or even if they take credit for the attacks, they currently do not fear the consequences. While the Department of Justice and the FBI have had increasing success in indicting and in some cases extraditing members of overseas criminal networks and partnering with the private sector to disrupt botnets and other malicious activity, generally these organizations perpetrating these acts are not fearful of attribution, extradition or prosecution to the degree that impacts their risk/reward calculation and that currently must stop, and I think Congress can certainly assist in that by passing legislation to fill important gaps that do exist as we have just heard with in current law or executive action that cannot be filled that way under existing law.

As such, we endorse the Committee's efforts through the proposed International Crime Prevention Act of 2015, and we thank you for holding this important hearing. We look forward to working with Congress and this Committee and the administration as we strive to improve the legal and the operational tools necessary to address this threat. Thank you very much.

[The prepared statement of Doug Johnson appears as a submission for the record.]

**STATEMENT OF JEN ELLIS, SENIOR  
DIRECTOR OF COMMUNITY AND PUBLIC AFFAIRS, RAPID7  
SAN FRANCISCO, CALIFORNIA**

Ms. ELLIS. Mr. Chairman, Senators, thank you for the opportunity to contribute to this hearing. I am the senior director of community and public affairs at Rapid7, a security data and analytics company trusted by more than 3,900 organizations.

We work extensively with security researchers around the world. According to the open source vulnerability database, researchers discovered and disclosed more than 13,500 technology vulnerabilities in 2014, including Heartbleed.

We also saw research reveal a bug in 5,300 gas tank gauges across the United States, exposing them to remote attack. These findings come from testing computer systems to discover technical flaws and configuration issues that make them vulnerable to attack.

Once vulnerabilities are found, technology providers and users are alerted so they can mitigate the threat. Some researchers work for the companies that build and deploy the systems, but many more operate independently.

As independent testers, validators, and problem solvers, they are the antibodies of the digital immune system. Yet while this research is essential to our safety, it is at risk from both current and future legislation.

The Computer Fraud and Abuse Act and similar State laws do not differentiate between well-intentioned research and genuine bad actors. Though they are primarily used to address cyber crime, these laws also deter security research.

In the 30 years since the CFAA was first enacted, technology has changed a great deal and the vagueness of the language has become an increasing problem. Today, we see the statute being applied inconsistently by the courts and unpredictably by prosecutors.

The lack of clear definitions and boundaries creates uncertainty over whether well-meaning research efforts will violate the law. This unfortunate effect is exacerbated because the law contains both criminal and civil penalties. Technology providers fear for the reputational fallout from a vulnerability disclosure and uses the threat of a lawsuit as a stick to scare researchers away.

This is a worryingly common occurrence and many technology providers focus on the short term impact to their business and view independent researchers as troublemakers.

For example, when a researcher found that a flaw in this interactive toy could let an attacker talk to a child without their parent's knowledge and provide the child's name, age and location, the toy maker threatened legal action. This is not a standalone example, I have many others.

In one, a State prosecutor investigated a researcher despite the FBI having determined that his work was bonafide and valuable. Yet for all the discussion around cybersecurity legislation, this is not a problem being discussed.

Most discussions around updating CFAA focus on extending its application and making penalties more stringent. Penalties are certainly an important part of deterring crime, but they are less likely

to be impactful internationally when you consider how hard it is to prosecute foreign actors.

Studies suggest that people determine whether to commit a crime based primarily on the likelihood of being caught, not the severity of the punishment. This is probably even more the case with large organized crime groups such as the Russian Business network or state-sponsored hacking groups such as China's Deep Panda.

This brings me to the Committee's proposed legislation, the International Cyber Crime Prevention Act of 2015. I would like to thank the Committee for giving us the chance to comment on the draft proposal. We applaud your emphasis on the prevention of cyber crime and think the bill does a number of things well.

In particular, we support the idea that law enforcement should be able to shut down botnets within the checks and balances of a legal framework. We also commend the bill's focus on protecting critical infrastructure and making the requirements stringent.

However, we are concerned that the bill does not address the issues affecting security researchers. In fact, it could make the situation worse for them. We understand that creating a carve-out is challenging, as often researchers' efforts mirror those of cyber criminals, but we strongly urge the Committee to consider this problem, perhaps as a way to create an exemption for research based on intent or hurtful outcomes.

Clarifying and updating some of the language of the bill would also help by giving researchers more confidence over what is or is not permissible. For example, the statute revolves around the concept of authorization, but this term is not well-defined.

Likewise, notions of protected computers and obtaining information are drastically out-of-date and do not consider the role that technology providers and owners may play in exposing data.

Without clarifying the CFAA and creating greater consistency in the way it is prosecuted and litigated, we diminish the value of security research and make it harder for U.S. organizations and consumers to protect themselves.

The reality is that technical systems are complex by nature and they will never be perfect. We will always have bugs that provide opportunities for attackers. The only way to mitigate this is to support a culture where these issues can be proactively identified, disclosed and addressed.

It is not the imperfection of systems that should define us. It is how we respond to the knowledge that they will not be perfect.

Once again, I would like to thank you for the opportunity of testifying today. I welcome your questions and comments and wish the Chairman a happy birthday for tomorrow.

[The prepared statement of Jen Ellis appears as a submission for the record.]

**STATEMENT OF BILL WRIGHT, DIRECTOR,  
GOVERNMENT AFFAIRS, GLOBAL  
CYBERSECURITY PARTNERSHIPS, SYMANTEC  
WASHINGTON, DC**

Mr. WRIGHT. Thank you. Chairman Graham, Senator Whitehouse and Members of the Subcommittee, thank you for the oppor-

tunity to testify today. I am especially pleased that you are again focusing attention on cyber crime and how industry and Government partnering can help deter it.

As the largest software company, Symantec protects much of the world's data infrastructure. Our mission is to help consumers, businesses and governments secure and manage their information and identities.

The cyber threat we face today is growing in both numbers and sophistication. Over the last 3 years, we have seen more than 1 billion identities exposed through breaches. Sensitive trade secrets and intellectual property are being pilfered at an unprecedented rate.

The use of malware is growing and becoming more sophisticated with more than 1 million new malware variance released into the wild each day in 2014. Attackers are also continuing to evolve their criminal tools to avoid detection. These attackers include highly organized criminal enterprises, disgruntled insiders, so-called hactivists with a political agenda, and of course, nation-states.

The damage to the economies and the security of governments and businesses around the globe is unrelenting. Even the most unskilled attackers can buy cyber crime tools or hire skilled hackers to do their dirty work. In fact, today we released a report on a previously unknown cyber crime group known as Morpho.

What sets this group apart is that they perform corporate espionage with a laser focus on operational security. Over the past 3 years, they have stolen confidential information and intellectual property from companies such as Twitter, Facebook, Apple, and Microsoft, who have all publicly acknowledged being victims.

Numerous pharmaceutical companies, technology firms, law practices, and oil and precious metal mining organizations also were victims. Morpho is a timely reminder that as well as defending against nation-state sponsored attacks, we must also be vigilant against corporate espionage, where attacks are performed at the behest of competitors or by criminals looking to monetize stolen information.

Botnets remain at the heart of the cyber criminal ecosystem. Their uses are only constrained by the imagination of the botmaster. From DDoS attacks to Bitcoin mining to harvesting personal information from infected computers, similar to hackers for hire, botmasters can rent out their botnets as well as use them for stealing passwords, credit card data, intellectual property which is then sold on the black market to other criminals.

Taking down cyber crime networks can be complex. It requires a high level of expertise and coordination. Despite these obstacles, law enforcement and private sector working together have made progress in the past year. We have seen a string of successful arrests and prosecutions of some of the most notorious cyber criminals in the world.

These include the sentencing of the creator of Blackshades trojan to 5 years in prison and the arrest and extradition an orchestrator of one of the biggest bank heists in history of more than \$55 million.

We have also seen a number of successful takedowns of financial fraud botnets. Last year, law enforcement mounted major oper-

ations against Gameover Zeus botnet and the ransomware network Cryptolocker, as well as against the Shylock botnet, and earlier this year the servers and infrastructure of the Ramnit botnet were seized.

These law enforcement operations and others have helped lead to an 18-percent decline in botnet infections in the year 2014. Unfortunately, cyber criminals are quick to adapt and these successes are often followed by the emergence of new threats such as the Dyre group. The Dyre financial fraud botnet has emerged as one of the most dangerous financial trojans in the world, capable of defrauding customers from financial institutions in multiple countries.

Despite an impressive year of law enforcement actions, there is always a new threat ready to fill the void. In combating botnets and cyber crime, cooperation is key. In the private sector, we need to know that we can work with Government and industry partners to disrupt botnets without undue legal barriers.

Modernizing cyber crime laws is a crucial element. We need to amend such—amend laws such as the Computer Fraud and Abuse Act to enhance judicial authority to disrupt botnets and allow prosecutors to go after not just those who profit directly from the botnets, but also those who provide access and traffic in botnets.

Similarly, we need to ensure that we can prosecute overseas criminals that possess or traffic in stolen credentials and financial information, regardless of whether that individual was the one who actually had stolen the information in the first place.

As this Subcommittee knows well, we face significant challenges dismantling cyber crime networks. However, the work that industry and Government are doing together is paramount to future success. At Symantec, we are committed to improving online security across the globe, and we will continue to work collaboratively with our customers, industry and governments on ways to do so.

Thank you again for the opportunity to testify and I will be happy to answer any questions. Thank you.

[The prepared statement of Bill Wright appears as a submission for the record.]

Chairman GRAHAM. Thank you. I will yield my time to Senator Cornyn and ask questions later. Thank you.

Senator CORNYN. Thank you, Mr. Chairman. It seems like it is the wild, wild west all over again. This time it looks like the bad guys are winning and operating with a lot of impunity.

Tell me if you think I am wrong, but my impression is that the private sector is much farther along in protecting its networks than the Government is. We all know that we are dealing with a rising level of state actors and sophisticated criminal organizations that have very little to lose because the chances of actually getting caught and being hauled into court and serving time are very, very small.

I know both Senator Graham and Senator Whitehouse have been working on this issue a long time, and I am hopeful that we will take up a cybersecurity bill this month before we leave. I would just like to hear from each of you given your experiences in the private sector with cyber research and also with Symantec.

What can the United States do to better equip itself to deter and respond to these threats? In other words, what sort of legislation do you think we need to make sure is included? What are the elements of that legislation?

It strikes me—things like information sharing, liability protection are a couple of them, but I would just like to hear your response starting with you, Mr. Johnson.

Mr. JOHNSON. Thank you, Senator, and I appreciate the question, and I would like to address the information sharing component of that question because I mentioned cascading effects within my testimony.

I think one of the things that we have experienced within the FS-ISAC environment is an ability to share information at a level of velocity that keeps events from cascading more than they actually potentially could cascade through other financial institutions.

I think as we debate the nature of an information sharing bill that we need to think very carefully about that particular issue to the extent that we do not in the process of, for instance by example, putting a civilian agency in the middle of the information sharing process impede the velocity, the manner in which the information is shared so that we can actually stop the event from reaching other institutions and other institutions, because the faster that information flows from one institution to the other, the quicker we will be able to essentially stop the threat and also have the recognition that the vast, if not all, the information that is being shared in that environment is not personally identifiable and so therefore should be treated as such as we think about what sort of impediments we put associated with that information sharing.

Senator CORNYN. Ms. Ellis, I understand your enterprise has a significant Austin presence. Thank you for that.

Ms. ELLIS. Thank you.

Senator CORNYN. I would be delighted to hear your response.

Ms. ELLIS. Thanks. I am obviously a little biased toward security research. I think that we have to look at the way that we are creating opportunities for these attackers, and we have to think about how we can reduce the opportunities and also how we can raise the barriers to entry for them. Much of what I talk about around security research is really geared toward doing that.

We are trying to identify the opportunities that are created for attackers in our technical systems that we rely on, and we are trying to mitigate those opportunities so that we make it more technically complex for them to be able to perpetrate attacks.

Legislatively, I think we need to look at how the legislation we already have impacts research and likewise the legislation that we are thinking about introducing. I think there are a couple of other things as well, though. There was a bill that was introduced in the lame duck, I believe, on the House side that basically aimed to make sure that Government entities when they were using technology would be mindful of the third-party components being used and would use the most up-to-date versions, and ensure that they were patching and that they were transparent about the systems being used so that again, where you have systems that are so complex and so interconnected and so reliant on different pieces of technology, some of those pieces of technology are already out-of-

date and you need to make sure that you're not using the stuff that we already know is out-of-date that we know has issues in it. I would recommend you look at that bill.

Senator CORNYN. My experience has been that Government and technology do not mix very well. To your point, even if the technology exists, it may not be being used.

Mr. Wright, your company is in the business of protecting computers and networks. What does the Federal Government need to do to protect not only the 18 million files of those who were hacked at the OPM recently, but the American people more generally?

Mr. WRIGHT. Yes, so I would like to add on to what Mr. Johnson said there. Information sharing is certainly a very important piece, a very important element to all of this. However, it is not a panacea.

There is also a lot of information sharing going on right now between public sector and private sector and private sector and private sector. New organizations are popping up every day and this information is flowing.

I would say to the extent that it—that information sharing legislation could help facilitate that exchange, then it would be very important. Parts that we would like to see certainly are privacy protections that are part of that information sharing, data minimization, and actually to have a civilian lead.

We think that the civilian agencies have a background in these sort of privacy protections and it could be very helpful protecting that.

I would also say a lot of the work that this Committee is doing and considering in modernizing our cyber crime tools could be very, very effective. As Senator Whitehouse pointed out, time to go on the offensive.

If we can find a way to insert some risk into the risk/reward scenario that a lot of these cyber criminals are going through, I think we can see effects not only on the current cyber criminal problem, but future cyber criminal problems. Thank you.

Senator CORNYN. Thank you, Mr. Chairman.

Senator WHITEHOUSE. Mr. Johnson, you are here on behalf of the American Bankers Association. On behalf of America's banks, what can you tell us about the size of the cyber threat and the role of overseas and foreign actors in that threat?

Mr. JOHNSON. The size is very difficult to quantify, but it is without question that every one as we heard in the first panel, every one of the major exploits that we see has a foreign component associated with it.

It may be a nation-state, it may be a criminal enterprise.

Senator WHITEHOUSE. Every one has a foreign component?

Mr. JOHNSON. Yes. Every one has a foreign component to it and that becomes very problematic whether it is a nation-state or whether it is a criminal enterprise. We are very grateful to see the sanctions definition of the kinds of lines in the sand essentially which create an activity that a nation-state has conducted which actually would potentially cause the United States to take action.

I think that is one thing that we did not see in the denial of service attacks that has a level of frustration in our industry associated with it. We did not know where that line was. We did not know

when a particular activity by a particular government would actually fall into the foreign policy equation and be considered as a part of that, and now I think we know that with a greater level of certainty. I think that is very important.

Senator WHITEHOUSE. You mentioned botnets. We would expand so that not just fraud but also abuse and misuse was a reason to shut down a botnet.

If you are a bank, a botnet can be used to attack you not just for purposes of fraud and stealing money, but for purposes of a critical infrastructure attack against the bank and against the country with the intention of actually doing destruction rather than stealing and getting money.

Mr. JOHNSON. That is—

Senator WHITEHOUSE. This clarification would be helpful to you and supported by the bankers?

Mr. JOHNSON. Yes, Senator, it would because we very much look to the potential of the disruptive types of attacks which we have seen from nation-states becoming destructive types of attacks and that is something that we look at very closely and take very seriously.

Senator WHITEHOUSE. Ms. Ellis, you have looked at the proposed draft that we have. The narrowing of the Computer Fraud and Abuse Act is one that I understand you support and believe that it would not cause any reduction in security but in fact would allow security companies like yours to have more confidence going about their business.

Ms. ELLIS. Yes, I think that that is true, but I do also think that there is still work to be done on the proposal. Specifically the definitions are just still a huge concern and—

Senator WHITEHOUSE. A quick question on that.

Ms. ELLIS. Yes.

Senator WHITEHOUSE. You attack corporate systems with the permission of the corporation in order to test the security of the systems. Why is your contract with the company not enough of a defense?

Ms. ELLIS. Because that is not what we are talking about when we talk about research. That is a particular kind of research. There are corporations who employ people to do that, absolutely.

Senator WHITEHOUSE. You have a lot of clients who you do that with, correct?

Ms. ELLIS. Absolutely. There is also—

Senator WHITEHOUSE. A more freelance mode?

Ms. ELLIS. Yes. That research can actually be either intentional or accidental, right? It can be accidental discovery such as the 5-year-old boy who was trying to get into his dad's Xbox and found out that he could circumvent the controls on it.

Once that issue gets disclosed, that becomes a vulnerability finding, and so we want to make sure that that kind of behavior is protected.

Senator WHITEHOUSE. Mr. Wright, you agree that the amendments that we have made to the Computer Fraud and Abuse Act create no harm to computer security and are supported by Symantec, one of our leading computer security companies?

Mr. WRIGHT. Yes. We definitely support the intent of the various pieces. We too would want to obviously make sure that innocent usage was not covered so that the scope could narrow. As it reads now, we do support.

Senator WHITEHOUSE. In the strengthening of our ability to pursue offshore criminals, you mentioned the MLATS and the letters rogatory and some of the somewhat antiquated tools.

Just give us a quick comparison between the speed at which cyber crime takes place and the speed at which MLATS and letters of rogatory operate.

Mr. WRIGHT. Yes, absolutely. Cyber crime and technology are changing every day. The tactics of criminals are changing every day, they are becoming more and more sophisticated.

Senator WHITEHOUSE. It is a crime that can literally occur at the speed of light.

Mr. WRIGHT. Correct. We are dependent on at least on the law enforcement information sharing on laws that were written in the 1800s or 1700s. We need to have that MLAT process streamlined so that we can—our law enforcements can share information.

Cyber crime is global by nature. This type of communication is absolutely essential and it is key in fact to fighting cyber crime.

Senator WHITEHOUSE. Finally, why do you support aggravated penalties for attacks on critical infrastructure?

Mr. WRIGHT. Critical infrastructure, obviously the most sensitive, the most dangerous. It puts lives at risk. It makes a lot of sense then to add penalties to that, to those attackers that are going after our critical infrastructure that they are putting lives at stake. Thank you.

Senator WHITEHOUSE. Mr. Chairman, over to you.

Chairman GRAHAM. Thank you all very, very much. If Congress continues to do nothing in this area, what does it mean for the bankers?

Mr. JOHNSON. Senator, first of all, I would be remiss if I did not wish you a happy birthday.

[Laughter.]

Chairman GRAHAM. Thank you. You would be and you corrected that problem. I want everybody in the world to wish me a happy birthday.

[Laughter.]

Mr. JOHNSON. Second, if I remember the question, I think that the status quo has three different components to it now. I think we have a three-legged stool that we are working on essentially here.

We have got the necessity to develop a national data breach and data security standard, we have got the necessity to buttress and have clarity in our information sharing environment, so we do no harm to as Mr. Wright indicated, what already exists, but also improve the clarity associated with the liability protections and the ability to share information, particularly across sectors.

Then we have the necessity to be able to do harm to criminals, and it is only if we do all three of those things will we be able to move the needle and the way that you are suggesting is more difficult to do over time.

If we do nothing, we do not move that needle. If we do nothing, we potentially regress as opposed to progress because we have not

really buttressed the tools that are necessary in the new environment and increasingly sophisticated environment to be able to address these threats.

Chairman GRAHAM. I do not know how many bank robberies there are every year, but compare bank robberies to cyber theft. What kind of ratio are you looking at?

Mr. JOHNSON. I can use a very simple number for you. The average bank robbery is around \$5,000—\$5,000 to \$6,000. The average ATM skim, which is a fairly modest cyber crime, is 10 times that, and that is one of the less sophisticated crimes.

You can get \$50,000 from a skimming exploit and \$5,000 from a bank robbery on average, and then if you take the more sophisticated crimes, you are exponentially growing the ability of a criminal to essentially monetize as we heard in the first panel some of the dollar amounts.

Chairman GRAHAM. I forgot to ask this question, but will send it in writing. I want to know the number of FBI agents that are involved in preventing bank robberies, which I am glad they are, and prosecutors dedicated to that versus the number of FBI agents and other Government officials designed to prevent cyber theft. I imagine I would be surprised.

Mr. Wright, you said that cyber attacks can cause physical damage to critical infrastructure. Could you explain what you are talking about there?

Mr. WRIGHT. Sure. First off, the pressure is certainly mounting to wish you a happy birthday.

Chairman GRAHAM. Thank you.

[Laughter.]

Mr. WRIGHT. Happy birthday to you.

Chairman GRAHAM. Welcome to the party. Thank you very much.

[Laughter.]

Mr. WRIGHT. As you know, our critical infrastructure is dependent on computer systems and networks. In addition to that, part of the controls are industrial control systems. Those actually have—control moving parts.

By attacking those, you are able to make sort of kinetic movement, kinetic changes to physical property. In that sense, there can be physical change. I am also talking about if they hit a power plant or something, the kind of danger that that could cause a society as well.

Chairman GRAHAM. Thank you. Ms. Ellis, one, we want to get your input about how to make the statutes that we are talking about clearer to make sure that we do not grab the wrong people.

You said something, and maybe I missed this, but I thought I heard you say that there is some research projects that revealed that a bug that can be used to actually blow up a building. Did you say that?

Ms. ELLIS. I did not say it in my testimony, but I have been known to talk about it, yes.

Chairman GRAHAM. You have got my attention. It is one thing to shut down your computer. It is another thing to blow up the building.

Ms. ELLIS. Yes. Basically the way it works is that people use systems that were never designed to be connected to the internet and then they put something on top of that to connect it to the internet.

In the particular example that we are talking about, there are some churches that have old boiler systems and somebody came up with the brilliant idea of connecting them to the internet so they could be turned on and off, and unfortunately they can also be turned all the way on, which is not something you want to have happen.

Chairman GRAHAM. I guess the point is that we need to up our game when it comes to punishment. The risk/reward calculation is way out of line with what it should be, so if we accomplish nothing else, I hope we can accomplish that.

The three necessities you mentioned, Mr. Johnson, we are trying our best to address them in this Subcommittee in a bipartisan way.

I want to end on this. Of all the people I have met in the Congress about this topic, Senator Whitehouse has been the most engaged, incredibly knowledgeable trying to find solutions to complicated problems, so I would like to be his partner to the extent that I can and see if we can come up with some legislation that would make our country safer and give the private sector the tools they need to move forward.

Thank you all very much and the hearing is adjourned. We will leave it open for any comments for a week. I apologize. The hearing is adjourned and happy birthday to me.

[Laughter.]

[Whereupon, at 3:37 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

## **A P P E N D I X**

**Submitted by Senator Graham:**

|                                                  |    |
|--------------------------------------------------|----|
| National Association of Convenience Stores ..... | 69 |
|--------------------------------------------------|----|



## **Department of Justice**

---

STATEMENT OF

DAVID M. BITKOWER  
DEPUTY ASSISTANT ATTORNEY GENERAL  
CRIMINAL DIVISION  
DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM  
COMMITTEE ON THE JUDICIARY  
UNITED STATES SENATE

AT A HEARING ENTITLED

"CYBER CRIME: MODERNIZING OUR LEGAL FRAMEWORK FOR THE  
INFORMATION AGE"

PRESENTED

JULY 8, 2015

**Statement of  
David M. Bitkower  
Deputy Assistant Attorney General  
Criminal Division  
Department of Justice**

**Before the  
Subcommittee on Crime and Terrorism  
Committee on the Judiciary  
United States Senate**

**At a Hearing Entitled  
“Cyber Crime: Modernizing our Legal Framework for the Information Age”**

**Presented  
July 8, 2015**

Good afternoon, Chairman Graham, Ranking Member Whitehouse, and Members of the Subcommittee. Thank you for the opportunity to appear before the Subcommittee today to discuss legislative proposals to combat cybercrime. I also particularly want to thank the Chair and Ranking Member for holding this hearing and for their continued leadership on this important issue.

As the Attorney General has made clear, fighting cybercrime is one of the highest priorities of the Department of Justice. Recent revelations about the massive thefts of financial and other sensitive information from both the public and private sector serve as a stark reminder to all of us about how vulnerable we are to those who take advantage of our computer networks to steal our personal and financial information.

Our growing reliance on computer networks and electronic devices in almost every aspect of our lives has been accompanied by an increasing threat from individuals, organized criminal networks, and nation states that victimize American citizens and businesses. Hackers

steal and hold for ransom our most valuable and personal information. They invade our homes by secretly activating webcams. They steal financial information to line their pockets while jeopardizing the financial stability of everyday Americans. A new generation of organized criminals is able to steal the personal information of millions of victims from a computer halfway around the world. These developments also pose a widespread threat to American businesses and the economy. Cyber criminals can orchestrate massive disruptions of businesses and can electronically spirit away trade secrets worth millions of dollars in seconds. Every individual has a stake in protecting computers and computer networks from intrusions and abuse. According to one report, just this past May there were over 44 million new pieces of malicious software — or “malware” — created around the globe. Another report found that in 2014, there were about 24,000 ransomware attacks per day. I’ll talk more about ransomware later. A study from last summer estimated that cybercrime costs the global economy approximately \$400 billion annually. A study from this past May projects that, by 2019, cybercrime will cost businesses worldwide \$2 trillion per year.

An essential part of the mission of the Department of Justice is to protect Americans from emerging criminal threats such as the cyber threats described above and to deter, disrupt, and prosecute the criminals who are responsible for them. These invasions of privacy, for good reason, make us feel vulnerable and unsafe. And that fear is only compounded when we realize that the criminals who hack into our computers often sit on the other side of the world; peddle the stolen information to other criminals; and use the information for financial gain or even to terrorize and extort their victims. As the Deputy Attorney General testified this morning, the Department supports the use of strong encryption to help protect against unauthorized access to

sensitive information. But just as locking your door cannot offer complete protection from crime, cybersecurity cannot provide perfect protection from cyber criminals. That's why the Department's prosecutors, along with agents from the Federal Bureau of Investigation, the United States Secret Service, and other law enforcement agencies, work every day using the legal authorities at our disposal to protect personal information and vindicate the privacy rights of citizens and businesses. But just as our adversaries adapt to new technologies and global realities, so must we. If we want to remain effective in protecting our citizens and businesses, our laws and our resources must keep pace with the tactics and numbers of our adversaries. We ask that Congress continue its support of these critical efforts.

Earlier this year, the President announced new legislative proposals designed to protect the online privacy and security of American citizens and businesses. These proposals include a set of targeted updates to the criminal code to provide additional capabilities to prosecute offenders and deter and disrupt criminal conduct.<sup>1</sup> Some of the proposals will enable the Department to address the growth of specific types of crime, such as the sale of illegal spyware or the use of botnets — networks of victim computers surreptitiously infected with malware. Other proposals address shortcomings in existing statutory capabilities, such as the Government's ability to prosecute cases involving insiders, including Government or corporate employees, who use their access to information systems to misappropriate sensitive and valuable data. The proposals also respond to changes in the threats posed by cyber criminals, such as by adding provisions to enable the prosecution of hacking by organized crime groups and to give

---

<sup>1</sup>See <https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat>; <https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf>.

Federal courts the authority to sentence perpetrators of the most significant cybercrimes in line with those who commit similar financial crimes.

#### **Computer Fraud and Abuse Act**

One of the most important of the substantive criminal statutes used to bring cyber criminals to justice is the Computer Fraud and Abuse Act, also called the “CFAA.” The CFAA is the primary Federal law against hacking. It protects the public against criminals who hack into computers to steal information, install malware, and delete files. The CFAA, in short, reflects our baseline expectation that people are entitled to have control over their own computers and are entitled to trust that the information they store in their computers remains safe.

The law was first enacted in 1984, at a time when the problem of cybercrime was still in its infancy. Over the years, a series of measured, modest changes have been made to the CFAA to reflect new technologies and means of committing crimes and to equip law enforcement to respond to changing threats. The CFAA has not been amended since 2008, and in the intervening years the need again has arisen for the enactment of modest, incremental changes. We support targeted legislative changes to help the CFAA keep up with rapidly-evolving technologies and uses.

#### **Deterring Insider Threats**

Ensuring that the law enables us to protect privacy and security without ensnaring harmless or legitimate conduct is particularly important in the context of the CFAA, which protects the privacy and security of computer owners and users. The CFAA applies both to hackers who gain access to victim computers without authorization from halfway around the world, and to those who have some authorization to access a computer — like company

employees entitled to access a sensitive database for specified work purposes — but who intentionally abuse that access. The CFAA needs to be updated to make sure that the statute continues to appropriately deter privacy and data security violations. Targeted legislative changes would maintain the law’s key privacy-protecting function while ensuring that trivial violations of things like a website’s terms of service do not constitute Federal crimes.

The part of the CFAA that covers the conduct of those who have some authorization to access a computer is the statute that Department prosecutors have used to charge, for example, police officers who take advantage of their access to confidential criminal records databases in order to look up sensitive information about a paramour, sell access to private records to others, or even provide confidential law enforcement information to a charged drug trafficker. We’ve also used this part of the statute to prosecute a consultant of a health insurer who used his access to the company’s sensitive databases to improperly obtain the names and Social Security numbers of thousands of current and former employees.

Unfortunately, recent judicial decisions have limited the Government’s ability to prosecute such cases in large parts of the country.<sup>2</sup> As a result of these decisions, insiders may be effectively immunized from punishment even where they intentionally exceed the bounds of their legitimate access to confidential information and cause significant harm to their employers and to the people — often everyday Americans — whose data is improperly accessed.

Let me offer you an example. Suppose a criminal in Eastern Europe hacks into a healthcare database located in California and steals the financial and personal information of millions of Americans. That crime could be charged today under the CFAA because the

---

<sup>2</sup>See <http://cdn.ca9.uscourts.gov/datastore/opinions/2012/04/10/10-10038.pdf>.

offender accessed the database “without authorization.” Now suppose that a customer service employee has access to the healthcare company’s records in the ordinary course of the employee’s work. Because the database contains sensitive information, the company’s rules explicitly state that employees can only access the database for official business. But if the employee intentionally violates those rules, and accesses the private medical records of a political candidate in order to later embarrass that person by publicizing the records, the individual likely could not be prosecuted under the CFAA in one of the affected judicial circuits.

The narrow judicial interpretation of the term “exceeds authorized access” in the CFAA stemmed from the concern that the statute potentially makes relatively trivial conduct a Federal crime. For example, a Federal court feared that the statute could be construed to permit prosecution of a person who accesses the internet to check baseball scores at lunchtime in violation of her employer’s strict internet use policy.<sup>3</sup> Or someone who accesses a dating website but lies about his height even though the site’s terms of service require users to provide only accurate information.

We understand these concerns. The Department of Justice has no interest in prosecuting harmless violations of use restrictions like these. That’s why we’ve crafted proposed amendments to the CFAA to address these concerns — while making sure that the law applies to those who commit serious thefts and privacy invasions.

To accomplish this, our proposal does two things. First, it addresses the recent judicial decisions that have posed obstacles to important prosecutions. It does this by clarifying that the definition of “exceeds authorized access” includes the situation where the person accesses the

---

<sup>3</sup>*Id.*

computer for a purpose that he knows is not authorized by the computer owner. This clarification is necessary to permit the prosecution of, for example, a law enforcement officer who is permitted access to criminal records databases, but only for official business purposes. Second, at the same time, the proposal adds new limitations to make clear that trivial conduct does not constitute an offense. In order to constitute a crime under the new wording, not only must an offender access a protected computer in excess of authorization and obtain information, but the information must be worth \$5,000 or more, the access must be in furtherance of a separate felony offense, or the information must be stored on a Government computer.

These changes will empower the Department to prosecute and deter significant threats to privacy and security, but make sure that the CFAA doesn't inadvertently cover trivial conduct.

#### **Sale of U.S. Financial Data Overseas**

Another priority in addressing threats to privacy and financial security is shutting down the international black market for Americans' stolen financial information. One of the most common motivations for hacking is the theft of financial information. In recent years, organized, multinational criminal enterprises have emerged that steal large volumes of credit card numbers and other personally identifiable information. Middlemen then sell the stolen data to the highest bidder, often using underground "carding" forums. Statutory reforms should be aimed at making sure that these middlemen — those who profit from the sale of stolen financial data of Americans — can be brought to justice even if they are operating outside of the United States.

Current law makes it a crime to sell "access devices" such as credit card numbers. The law allows the Government to prosecute offenders located outside the United States if the credit card number involved in the offense was issued by an American company *and* meets a set of

additional requirements. In the increasingly international marketplace for stolen financial information, however, these requirements have proven increasingly unworkable in practice. The Government has to prove either that an “article” used in committing the offense moved through the United States, or that the criminal is holding his illicit profits in an American bank. But with the theft of digital data, it’s not always clear what “article” is involved. And foreign criminals generally move their money back to their home countries rather than keep it in the United States.

These requirements unduly limit the Department of Justice’s ability to prosecute criminals residing outside of the United States who commit crimes that harm Americans. Indeed, law enforcement agencies have identified foreign-based individuals holding for sale vast quantities of credit card numbers issued by American financial institutions where there is not necessarily any evidence that the person selling the numbers is the same person who stole them, and no evidence of “articles” in the United States. The United States has a compelling interest in prosecuting such individuals because of the great harm they cause to U.S. financial institutions and citizens.

A targeted amendment would strike the unnecessary language in the current statute. It would permit the United States to prosecute anyone possessing or trafficking in credit card numbers with intent to defraud as long as the credit cards were issued by a United States financial institution, regardless of where the possession or trafficking takes place. This kind of jurisdiction over conduct that occurs abroad is fully consistent with international norms and other criminal laws aimed at protecting Americans from economic harm. Moreover, in an era of global cybercrime where criminals steal Americans’ financial information so that they can traffic it abroad, it is necessary to prevent criminals from victimizing our citizens with impunity.

**Botnets**

Another striking example of cybercrime that victimizes Americans is the threat from botnets — networks of victim computers surreptitiously infected with malware. Once a computer is infected with the malware, it can be controlled remotely from another computer with a so-called “command and control” server. Using that control, criminals can steal usernames, passwords, and other personal and financial information from the computer user, or hold computers and computer systems for ransom. Criminals can also use armies of infected computers to commit other crimes, such as distributed denial of service (DDoS) attacks, or to conceal their identities and locations while perpetrating crimes ranging from drug dealing to online child sexual exploitation. The scale and sophistication of the threat from botnets is increasing every day. Individual hackers and organized criminal groups are using state-of-the-art techniques to infect hundreds of thousands — sometimes millions — of computers and cause massive financial losses, all while becoming increasingly difficult to detect. If we want security to keep pace with technological innovations by criminals, we need to ensure that we have a variety of effective authorities to combat evolving cyber threats like these.

One powerful method that the Department has used to disrupt botnets and free victim computers from criminal malware is the civil injunction process. Current law gives Federal courts the authority to issue injunctions to stop the ongoing commission of specified fraud crimes or illegal wiretapping, by authorizing actions that prevent a continuing and substantial injury. This authority played a crucial role in the Department’s successful disruption of the Coreflood botnet in 2011 and the Gameover Zeus botnet in 2014. These botnets used keystroke logging or “man-in-the-middle” attacks to collect online financial account information, and they transferred

stolen funds to accounts controlled by the criminals. The Gameover Zeus botnet, which infected computers worldwide, was estimated to have inflicted over \$100 million in losses on American victims alone, often on small and mid-sized businesses. Because the criminals behind these particular botnets used them to commit fraud against banks and bank customers, existing law allowed the Department to obtain court authority to disrupt the botnets by taking actions such as disabling communication between infected computers and the command and control servers.

The problem is that current law only permits courts to consider injunctions for limited categories of crimes, including certain frauds and illegal wiretapping. Botnets, however, can be used for many different types of illegal activity. They can be used to steal sensitive corporate information, to harvest email account addresses, to hack other computers, or to execute denial of service attacks against websites or other computers. Yet — depending on the facts of any given case — these crimes may not constitute fraud or illegal wiretapping. In those cases, courts may lack the statutory authority to consider an application by prosecutors for an injunction to disrupt the botnets in the same way that injunctions were successfully used to incapacitate the Coreflood and Gameover Zeus botnets.

Appropriate legislative changes would add activities like the operation of a botnet to the list of offenses eligible for injunctive relief. Specifically, our proposal includes an amendment that would permit the Department to seek an injunction to prevent ongoing hacking violations in cases where 100 or more victim computers have been hacked. This numerical threshold focuses the injunctive authority on enjoining the creation, maintenance, operation, or use of a botnet, as well as other widespread attacks on computers using malware (such as “ransomware”).

The same legal safeguards that currently apply to obtaining civil injunctions, and that applied to the injunctions obtained by the Department in the Coreflood and Gameover Zeus cases, would also apply here. Before an injunction is issued, the Government must civilly sue the defendant and demonstrate to a court that it is likely to succeed on the merits of its lawsuit and that the public interest favors an injunction; the defendants and enjoined parties have the right to notice and to have a hearing before a permanent injunction is issued; and the defendants and enjoined parties may move to quash or modify any injunctions that the court issues.

In sum, a targeted amendment would provide the Government with an effective capability to shut down illegal botnets or certain widespread malware, and better match the ways that criminals are using these technologies. It assures that the legal mechanism that has proven effective to date will be available.

#### **Sale of Botnets**

The Department has also striven to identify and bring to justice those who create and control botnets. While we have had significant successes to date prosecuting these offenders, we have encountered some shortcomings in the existing law.

Criminals continually find new ways to make money illegally through botnets. Law enforcement officers now frequently observe that those who create botnets not only use the botnets for their own illicit purposes, but also sell or even rent access to the infected computers to other criminals. The criminals who purchase or rent access to botnets then go on to use the infected computers for various crimes, including theft of personal or financial information, the dissemination of spam, for use as proxies to conceal other crimes, or in denial of service attacks

on computers or networks. Americans are suffering extensive, pervasive invasions of privacy and financial losses at the hands of these hackers.

Current criminal law prohibits the creation of a botnet because it prohibits hacking into computers without authorization. It also prohibits the use of botnets to commit other crimes. But it is not similarly clear that the law prohibits the sale or renting of a botnet. In one case, for example, undercover officers discovered that a criminal was offering to sell a botnet consisting of thousands of victim computers. The officers accordingly “bought” the botnet from the criminal and notified the victims that their computers were infected. The operation, however, did not result in a prosecutable U.S. offense because there was no evidence that the seller himself had created the botnet in question or used it for a different crime. While trafficking in botnets is sometimes chargeable under other subsections of the CFAA, this problem has resulted in, and will increasingly result in, the inability to prosecute individuals selling or renting access to many thousands of hacked computers.

We believe that it should be illegal to sell or rent surreptitious control over infected computers to another person, just like it is already clearly illegal to sell or transfer computer passwords. That’s why we recommend amending current law to prohibit the sale or transfer not only of “password[s] or similar information” (the wording of the existing statute) but also of “means of access,” which would include the ability to access computers that were previously hacked and are now part of a botnet. In addition, the proposal would replace the current requirement that the Government prove that the offender had an “intent to defraud” with a requirement to prove that the offender not only knew his conduct was “wrongful,” but that he also knew or should have known that the means of access would be used to hack or damage a

computer. This last change is necessary because, as noted above, criminals don't only use botnets to commit fraud — they also use them to commit a variety of other crimes.

Some commentators have raised the concern that this proposal would chill the activities of legitimate security researchers, academics, and system administrators. We take this concern seriously. We have no interest in prosecuting such individuals, and our proposal would not prohibit such legitimate activity. Indeed, that's precisely why our proposal requires that the Government bear the burden to prove, beyond a reasonable doubt, that the individual intentionally undertook an act (trafficking in a means of access) that he or she knew to be wrongful. And the Government would similarly have to prove that the individual knew or had reason to know that the means of access would be used to commit a crime by hacking someone else's computer without authorization.

This approach makes clear that ordinary, lawful conduct by legitimate security researchers and others is not at risk of criminal prosecution. We want to work with the members of this Subcommittee to make sure any amendment prohibits the pernicious conduct we've described without chilling the activities of those who are trying to improve cybersecurity for all.

#### **Spyware**

The widespread use of computers and cellular phones has created a market for malware that allows perpetrators to surreptitiously intercept their victims' communications. For a small fee, people can purchase this software and download it onto a victim's device. Operating secretly in the background, the spyware allows perpetrators to read a victim's email and text messages. They can track a victim's location and listen to their calls. They can even turn on the

microphone in a victim's phone or computer and listen to conversations in the room. They can do all of this from afar and without the victim knowing.

These privacy invasions have far-reaching implications. Spyware can be used by abusive spouses to track, control, and terrorize former partners. Competitors can commit corporate espionage. Spyware can even be used to eavesdrop on law enforcement and national security personnel. As one example, the Department recently prosecuted the maker of a spyware application called "StealthGenie." This application, which was available for the Apple iPhone, Android phones, and Blackberry devices, could surreptitiously record all incoming/outgoing voice calls; it allowed the purchaser to secretly activate the phone to monitor nearby conversations within a 15-foot radius; and it enabled the purchaser to monitor the incoming and outgoing email and text messages. The application was intended for, and I quote from the business development plan: "Spousal cheat: Husband/Wife o[r] boyfriend/girlfriend suspecting their other half of cheating or any other suspicious behaviour or if they just want to monitor them."

The market for this software has made these capabilities widely available to many who would not otherwise have access to them. We need to do more to counter the increase in privacy invasions.

It is already illegal to sell or advertise surreptitious interception devices of this type. Indeed, the Department successfully prosecuted the maker of the "StealthGenie" spyware, and the court fined the offender half-a-million dollars. Yet the people who make and sell these products often reside outside of the United States, making it more difficult to bring them to justice. And they are making millions of dollars of profit selling spyware inside the United

States. These same criminals try to conceal their ill-gotten gains and transfer them out of the reach of law enforcement. Because current law does not authorize the forfeiture of proceeds from the sale of spyware, U.S. law enforcement is unable to disgorge such criminals of the money that they amass.

Our proposal includes an amendment that would expand the scope of the statute that already provides for the forfeiture of surreptitious interception devices themselves to include forfeiture of proceeds from the sale of spyware and property used to facilitate the crime. The proposal includes standard language drawn from other areas of the criminal code regarding the rules and safeguards for civil and criminal forfeiture.

In addition, violators of the surreptitious interception device statute often engage in money laundering by transferring proceeds through multiple overseas accounts to conceal the profits of their criminal enterprise. Because the spyware statute is not listed as a predicate offense in the money laundering statute, however, prosecutors are unable to charge defendants for money laundering activities related to the sale of spyware unless they can link it to some other crime, which will often be difficult or impossible. The proposal therefore adds violations of the spyware statute to the list of money laundering predicate offenses.

#### **Conclusion**

I very much appreciate the opportunity to discuss with you the ways in which the Department protects the privacy and security of American citizens and businesses from cyber threats and to discuss targeted legislative changes that would strengthen our ability to counter this increasingly sophisticated threat going forward. We understand how devastating it is to victims of cybercrime who have their personal and financial information siphoned away, whether

by hackers on the other side of the world or by insiders at a company that holds their personal information. The Justice Department is committed to using the full range of investigative capabilities available to us to fight these privacy invasions and protect Americans, and we will continue to use these capabilities responsibly. We appreciate the continued efforts of Congress and this Subcommittee to ensure that statutory authorities to counter cybercrime are updated and effective.

Thank you for the opportunity to discuss this important area of our work, and I look forward to answering any questions you might have.

*July 8, 2015*

---

**Testimony of**

**Wm. Douglas Johnson**

*On behalf of the*

**American Bankers Association**

*before the*

**Subcommittee on Crime and Terrorism**

*of the*

**Committee on the Judiciary**

**United States Senate**



July 8, 2015

---

**Testimony of**  
**Wm. Douglas Johnson**  
*On behalf of the*  
**American Bankers Association**  
*before the*  
**Subcommittee on Crime and Terrorism**  
*of the*  
**Committee on the Judiciary**  
**United States Senate**

**Wednesday, July 8, 2015**

Chairman Graham, Ranking Member Whitehouse, members of the subcommittee, my name is Doug Johnson, senior vice president, payments and cybersecurity policy, of the American Bankers Association (ABA). In that capacity, I currently lead the association's physical and cybersecurity, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership.

I appreciate the opportunity to be here to represent the ABA and discuss the importance of modernizing our legal framework in the current cyber-crime environment. The ABA is the voice of the nation's \$15 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard \$11 trillion in deposits and extend over \$8 trillion in loans.

I also have the privilege of serving as vice chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and on the board of directors of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Established in 2002, the FSSCC is the national critical infrastructure protection coordinator for the financial sector, focused on operational risks. Because the FSSCC fits into a larger

network of sector coordinating councils, it is uniquely positioned as the leader within financial services for developing strategies to improve shared critical infrastructure and homeland security.

Established in 1999, the FS-ISAC is the designated operational arm of the FSSCC. The Center supports the protection of the global financial services sector by assisting FSSCC, Treasury as well as regional agencies and entities to identify, prioritize and coordinate the protection of critical financial services, infrastructure service and key resources. The FS-ISAC also facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures and practices.

As the 114th Congress engages in public debate on the important issue of cybersecurity and cybercrime, we share your concerns regarding the need to modernize our laws to meet the cybercrime challenges our nation faces. The ABA, now through its Center for Payments and Cybersecurity Policy, has historically been very supportive of these collaborative efforts to protect our sector's and nation's cyber infrastructure from private criminal actors and nation state threats. The financial sector is an acknowledged leader in defending against such threats. These efforts are highly mature and increasingly focused on international and cross-sectorial efforts to enhance our collective ability to defend against and respond to cybersecurity attacks that attempt to disrupt or destroy the systems we depend on, compromise personally identifiable information, steal intellectual property, or otherwise conduct criminal acts. We support buttressing our nation's ability to defend against, deter, and prosecute the perpetrators of these acts and will continue to work with Congress and this committee to achieve these goals.

In my testimony I will focus on three main points:

- **The cyber threats we face continue to evolve and become more complex.**
- **Our defenses against these threats continue to mature but challenges remain.**
- **Congress can assist by enhancing the civil and criminal penalties and tools we can use against our attackers.**

**I. The Cyber Threats We Face Continue to Evolve and Become more Complex**

According to the “Worldwide Threat Assessment of the US Intelligence Community,” cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact, and the range of cyber threat actors, methods of attack, targeted systems, and victims are also expanding, highlighting the persistent and ever-changing nature of the threats the private sector faces and will face in the future.<sup>1</sup> Attacks that once were singular in focus, be it a denial of service attack on financial institutions, an attack against merchant point-of-sale devices, or an attempt to destroy or wipe data of an energy company, may now contain a variety of such attack vectors. Such multi-faceted attacks create particular challenges for the victimized company or companies, necessitating the simultaneous maintenance of availability, integrity, and confidentiality of data when formerly a cyber-attack might have impacted only one of these vital data security components.

Attackers of every variety are also becoming increasingly adept at defeating security practices, increasing the velocity with which companies must move to ensure they understand how cyber risks are changing and what mitigating measures are most effective against these risks. It is indeed an arms race. The tools that these perpetrators are using now have the capacity to destroy as well as compromise data, or in the alternative remain on systems for extended periods of time prior to detection.

Another increasing challenge for financial institutions and the private sector generally is the need to digest an increasingly larger volume of cyber threat data. Determining the relevance of a particular piece of threat data, analyzing the magnitude of the threat, evaluating which systems might be impacted, and devising the appropriate course to take to mitigate the threat if necessary has become increasingly difficult.

Who is being attacked is also changing. Prior to 2014, much of the private and public sector cyber security focus was on critical infrastructure and the payments system. Now there is recognition that, given the broader motivations of attackers for conducting a cyber-attack, essentially any company and any sector could be subjected to a significant, highly visible attack.

---

<sup>1</sup> Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, James R. Clapper, Director of National Intelligence, February 26, 2015, available at: [http://www.dni.gov/files/documents/Unclassified\\_2015\\_ATA\\_SFR\\_-\\_SASC\\_FINAL.pdf](http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf)

The motivations for such attacks are indeed broadening. Nation states are becoming more adept at compromising private and public computer systems for reasons ranging from retribution for perceived wrongs to espionage.

## **II. Our Defenses against These Threats Continue to Mature but Challenges Remain**

The cybercrime threat certainly knows no boundaries. The increased activities of nation states and foreign criminal enterprises attempting to disrupt financial services through denial of service attacks, compromise U.S. customer financial data, or steal U.S. company and governmental trade secrets, point to the challenge we as a nation currently face in reaching overseas to apprehend and prosecute such actors. The overseas sale of the spyware and other tools used to facilitate these crimes is also difficult to prevent. We face vast botnet armies of infected computers, distributed internationally, attempting to use these tools to infect our financial customers' electronic devices, compromise their personal financial information or hijack their internet banking sessions.

The financial services sector's capacity to withstand the direct attack on our critical financial infrastructure as a result of the significant, purportedly nation state-based denial of service attacks demonstrated our sector's capacity to, through the FS-ISAC, act collectively to respond to major attacks and minimize their capacity to cascade through the sector.

Our sector has also initiated civil legal action, in conjunction with the FS-ISAC and Microsoft, to take down botnets responsible for compromising our customer's personal computers in order to extract their financial information. ABA was a declarant in several of the civil suits that successfully seized U.S.-based servers facilitating criminal botnets. These actions also cleansed millions of individual financial customer personal computers that had been infected in order to facilitate botnet traffic.

In April of this year the level of national and international coordination regarding such efforts took an additional step forward in the takedown of the "Beebone" botnet. In this instance, the FBI, the Department of Justice, and the National Cyber Investigative Joint Task Force-International Cyber Crime Coordination Cell (IC4), in coordination with other international law enforcement bodies, coordinated the takedown with the international financial sector. As a result of the court-authorized seizures of over 1000 domains, computers infected with Beebone could no longer report to the criminals responsible for the infection. Instead, infected computers were

redirected to a sinkhole server operated by Europol's European Cybercrime Centre, which is facilitating victim identification and remediation. As was the case with earlier botnet takedowns, as a result of the court-authorized domain seizures, computers infected with Beebone will no longer report to the criminals responsible for the infection. Instead, infected computers will be redirected to a sinkhole server operated by EC3, which will facilitate victim identification and remediation.

We also support recent action by the Administration, through executive order, authorizing the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on those individuals and entities that he determines to be responsible for or complicit in malicious cyber-enabled activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, economic health, or financial stability of the United States.

In addition to making it clear that sanctions authority will in the future be utilized against those that perpetrate cybercrimes, another important component of the order is the specification of what are considered significant malicious cyber-enabled activities to include:

- Harming or significantly compromising the provision of services by entities in a critical infrastructure sector;
- Significantly disrupting the availability of a computer or network of computers, including through a distributed denial-of-service attack;
- Misappropriating funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain;
- Knowingly receiving or using trade secrets that were stolen by cyber-enabled means for commercial or competitive advantage or private financial gain; or
- Attempting, assisting, or providing material support for any of the harms listed above.

The sanctions executive order sends a strong signal to cybercriminals and foreign entities that America is committed to fighting this increasing threat, and that we share this commitment to working together to help protect our critical infrastructure and the economic security of our country.

### **III. Congress can assist by Enhancing the Civil and Criminal Penalties and Tools We Can Use Against our Attackers**

The fact that attackers are becoming increasingly adept at defeating cybersecurity practices and mitigating measures points to the need for industry and government to develop and deploy enhanced measures on an ongoing basis with greater speed. While the threat detection, information sharing, and incident response capabilities our sector has leave us well positioned to withstand such attacks, we must also increase the potential that our attackers face real consequences for their actions.

Nation states that attack us generally deny attribution, or even if they take credit for the attacks currently do not fear the consequences. While the FBI and the Department of Justice have had increasing success in indicting members of overseas criminal networks and partnering with the private sector to disrupt botnets and other malicious activity, generally the organizations perpetrating these acts are not fearful of attribution, extradition, and prosecution to the degree that it impacts their risk/reward calculation.

While the recent executive order regarding sanctions is also important, it is widely recognized that Congress can also assist by passing legislation to fill important gaps that current law or executive action cannot fill. As such, we support this committee's efforts, as outlined in the recently circulated discussion draft, to propose the "International Cybercrime Prevention Act of 2015," which would:

- Clarify that U.S. economic espionage statutes cover acts committed on behalf of a foreign government;
- Enhance law enforcement tools to prosecute trade secret theft;
- Enhance the ability of trade secret owners to recover damages and keep their trade secrets confidential in court proceedings;
- Ensure our government can prosecute foreign individuals that possess or traffic credit card numbers, regardless of whether that individual is the criminal who stole the numbers in the first place;

- Allow service on foreign defendants outside U.S. jurisdiction. Foreign organizations with no agent or principal place of business within the U.S. should not be immune from service;
- Make the use of surreptitious interception devices a money laundering and RICO predicate and a Computer Fraud and Abuse Act violation;
- Authorize the forfeiture of surreptitious interception devices, proceeds from the sale of spyware, and property used to facilitate these crimes. While current law allows for prosecution of these crimes, cybercrime property and proceeds should not be exempted from forfeiture;
- Attack the use of overseas-controlled botnets by permitting the Department of Justice to seek a civil injunction to prevent ongoing Computer Fraud and Abuse Act (CFAA) violations in cases involving large numbers of victim computers;
- Create a CFAA violation for criminals who knowingly cause damage to a computer that controls critical infrastructure systems; and
- Allow the prosecution of government and corporate insiders that use their access for criminal purposes.

We look forward to working with Congress, this committee, and the Administration as we work to improve the legal and operational tools necessary to deter, detect, apprehend, and prosecute those that are using technology designed to create a more efficient and effective global economy for criminal purposes. We also strongly encourage Congress to act swiftly to enhance our abilities to share critical cybersecurity threat information, as well as to enact a national data security and notification law.



**Statement for Hearing on Cyber Crime: Modernizing our Legal Framework for the Information Age**

**Before the Subcommittee on Crime and Terrorism  
United States Senate Committee on the Judiciary  
July 8<sup>th</sup>, 2015**

Mr. Chairman, Ranking Member Whitehouse, members of the Committee, thank you for the opportunity to contribute to this hearing. I am the senior director of community and public affairs at Rapid7, a security data and analytics company trusted by more than 3,900 organizations. We are participating in this hearing to represent the perspective of security researchers. I work extensively with researchers, both within Rapid7, and through the Metasploit Framework, which is an open source penetration testing platform driven by contributions from researchers. Metasploit gives organizations the ability to safely test their defenses against the tools and techniques used by cybercriminals in the wild, so defenders can understand whether attacks will be successful, what the impact of an attack will be, and what steps they need to take to protect their organization.

Given the complexity of technology, the pace of innovation, and the potential for human error, we can never expect to build or deploy completely invulnerable systems. Researchers act as independent auditors or antibodies in the digital immune system, mimicking the behavior of cybercriminals in order to test whether computing systems and networks are vulnerable to attack. Once flaws are identified, researchers alert the vendors and technology users, either directly or through a third party, providing the information needed to fix weaknesses and better protect customers and technical systems. Some work for the companies who build and deploy the systems, but many more operate separately. As independent testers, validators, and problem solvers, they are the antibodies of the digital immune system.

According to the Open Source Vulnerability Database, more than 13,500 technology vulnerabilities were disclosed in 2014<sup>1</sup>. This included the Heartbleed vulnerability, which impacted 17% of the secure servers powering the internet, undermining the security of hundreds of thousands of websites, including banking and healthcare sites that deal extensively with confidential personal information.<sup>2</sup> We also saw research revealing a bug in around 5,300 gas station tank gauges across the United States, exposing them to remote attack.<sup>3</sup> It's clear that research is essential to our safety, yet it is at risk from both current and future legislation. The Computer Fraud and Abuse Act (CFAA) and similar state laws make no distinction between the well-intentioned work of researchers and the nefarious efforts of bad actors. Though they are primarily used to address cybercrime, these laws also deter security research.

Essentially an online anti-trespass law<sup>4</sup>, the CFAA is intentionally broad; however, in the 30 years since the law

<sup>1</sup> The Open Source Vulnerability Database: <http://blog.osvdb.org/>

<sup>2</sup> "Half a million widely trusted websites vulnerable to Heartbleed bug," Netcraft, April 2014: <http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html>

<sup>3</sup> "The Internet of Gas Station Tank Gauges," Rapid7, January 2015: <https://community.rapid7.com/community/infosec/blog/2015/01/22/the-internet-of-gas-station-tank-gauges>

<sup>4</sup> "Obama's proposed changes to the computer hacking statute: A deep dive," Washington Post, January 2015: <http://www.washingtonpost.com/news/voikh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/>

## **RAPID7**

was first enacted, technology has changed a great deal and the vagueness of the statutory language has become an increasingly big problem for the security research community. Today we see the statute being applied inconsistently by the courts, and unpredictably by prosecutors. The lack of clear definitions and boundary lines creates uncertainty over whether well-meaning research efforts will violate the law. This murkiness deters researchers from engaging in independent research projects, or disclosing accidental discoveries to those who can fix them.

This unfortunate effect is exacerbated by the law containing both criminal penalties and a private cause of action. Technology providers that fear the reputational fallout from a vulnerability disclosure use the threat of a lawsuit as a stick to scare researchers away. This is a worryingly common occurrence as many technology providers focus on the short-term impact to their business, and view independent researchers as trouble makers.

For example, a researcher found a flaw in an interactive toy designed to enable people to communicate with young children. Users were only supposed to be able to communicate with the child once approved by the child's parents, but the bug meant anyone could start talking to the child without their parents' knowledge. In addition, the system would send out information on the child including their name, age and location. When the researcher disclosed his findings to the toy's manufacturer, they threatened legal action. The researcher persevered and eventually the issues were addressed; however, the stress of the experience left the researcher wary of conducting further research.

While the majority of legal threats to researchers come from technology providers, they are not the most frightening concern. A researcher that worked on an internet scanning project that revealed vulnerabilities affecting tens of millions of routers in homes and offices around the U.S. faced the possibility of criminal prosecution. The project involved scanning publicly accessible assets on the internet and revealed important issues such as a bug that could be used to blow up buildings. This was disclosed to the technology vendors and infrastructure operators through the CERT Coordination Center<sup>5</sup> so they could be addressed. Despite the FBI determining that the research project was bona fide and valuable, the prosecutor thought it might be a violation of a state law that is similar to the CFAA. Eventually the prosecutor did drop the investigation; however, facing jail time understandably shook the researcher's confidence, and he ended the project and took a break from research altogether – not an outcome that makes any of us safer.

One of the problems this example highlights is the inconsistency with which these cases are brought, and the challenges presented by the complexity of them. Few prosecutors are actually experts in computer crimes, particularly at the state level, yet cybercrime convictions have become an appealing way to move ahead. This may encourage some to pursue prosecutions that penalize the people who are actually trying to make us more secure.

These are just two examples; there are many more. When researchers suffer legal threats, it is not just them or security companies that lose; we all do. I assure you that criminals are looking for these bugs and will take advantage of them, so we need the expertise of researchers to help us protect ourselves. Ignorance is not bliss, it is insecurity. Chilling security research means we won't know what we don't know, and we cannot address issues until we become aware of them.

Yet for all the discussion around cybersecurity legislation, this is not a problem being addressed yet. Most discussions around updating the CFAA focus on extending its application and making penalties more stringent. Penalties are certainly an important part of deterring crime, particularly domestically within the U.S., but they

<sup>5</sup> CERT Coordination Center: <https://www.cert.org/about/>



are less likely to be impactful internationally when you consider how hard it is to prosecute foreign actors. Studies suggest that people determine whether to commit a crime based primarily on the likelihood of being caught, not the severity of the penalty<sup>6</sup>. This is probably even more the case with large organized crime groups such as the Russian Business Network<sup>7</sup>, or state-sponsored hacking groups, such as Deep Panda<sup>8</sup>.

This brings me to the Committee's proposed legislation, the International Cybercrime Prevention Act of 2015 (ICPA), which, among other things, would update the CFAA. I'd like to thank the Committee for giving us the chance to comment on the draft proposal. We applaud your emphasis on the prevention of cybercrime. There are a number of things the Bill does well and we were encouraged to see some updates to the proposal we saw from the Department of Justice at the start of the year.

In particular, we are very supportive of the provision intended to shut down botnets and agree this is best undertaken by law enforcement within the checks and balances of a legal framework. We also commend the Bill's focus on protecting critical infrastructure. It makes sense to include the requirement that "the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Our concern with the Bill is that it does not address the issues affecting security researchers. In fact, it could make the situation worse for them. We understand that creating a carve-out is a challenge as often researchers' efforts mirror those of cybercriminals, despite radically-different intentions. We strongly urge the Committee to consider this problem and whether there is a way to create an exemption for research, perhaps based around intent or outcomes.

In addition, clarifying and updating some of the language of the Bill will at least enable researchers to act with more confidence over what is or is not permissible. For example, the statute revolves around the concept of "authorization," but this term is not well defined. Likewise, notions of protected computers and obtaining information are drastically out of date and do not consider the role technology providers and owners may play in exposing data.

Without clarifying the CFAA and creating greater consistency in the way it is prosecuted and litigated, we diminish the value of security research and make it far harder for U.S. organizations and consumers to protect themselves. The reality is that technical systems are complex by nature and will always have bugs that provide opportunities for attackers. The only way to mitigate this is to support a culture where these issues can be proactively identified, disclosed, and addressed. It's not the imperfection of systems that should define us, it's how we respond to the knowledge that they will not be perfect.

Once again, I'd like to thank you for the opportunity of testifying today. I welcome your questions and comments.

<sup>6</sup> "Deterrence in Criminal Justice," The Sentencing Project, 2010:  
<http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf>

<sup>7</sup> "Shadowy Russian Firm Seen as Conduit for Cybercrime," Washington Post, 2007:

<http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html>

<sup>8</sup> Deep Panda implicated in Aithem attack: <http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack>



Prepared Testimony and  
Statement for the Record of

**Bill Wright**  
**Director of Government Affairs, Cybersecurity Partnerships**  
**Symantec Corporation**

Hearing on

**"Cyber Crime: Modernizing our Legal Framework for the Information Age"**

Before the

United States Senate  
Committee on the Judiciary  
Subcommittee on Crime and Terrorism

July 8, 2015

226 Dirksen Senate Office Building

Chairman Graham, Ranking Member Whitehouse, and distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Bill Wright and I am the Director of Government Affairs for Cybersecurity Partnerships at Symantec. In this role, I manage a number of global relationships, working extensively with industry, non-profits, and governments to counter cybercrime and improve cybersecurity. I am also responsible for Symantec's global cybersecurity partnership program, through which we partner with governments around the world to raise awareness, mitigate threats, and share cyber threat information.

Symantec protects much of the world's information, and is a global leader in security, backup and availability solutions. We are the largest security software company in the world, with over 32 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of 57 million attack sensors in 157 countries, recording thousands of events per second. We maintain 9 Security Response Centers around the globe and we process 30 percent of the world's e-mail messages and nearly two billion web requests every day. All of these resources allow us to capture worldwide security data that give our analysts a unique view of the entire Internet threat landscape.

The cyber headlines of the past year have focused on data breaches, cyber espionage and cybercrime. I am pleased that the Subcommittee is again focusing attention on how industry and government can work together to disrupt these threats. In my testimony today, I will discuss:

- The size and scope of the cyber threat landscape, including botnets;
- Successful efforts to disrupt botnets and cybercrime;
- Enhancing cybersecurity through public-private partnerships; and
- Improving laws to fight cybercriminals.

#### **The Size and Scope of the Cyber Threat Landscape**

If there is one thing that can be said about the threat landscape, and Internet security as a whole, it is that the only constant is change. The scale of theft of personally identifiable information (PII) is unprecedented – over just the past three years alone, the number of identities exposed through breaches is more than *one billion*. And this is just from known breaches, as many go unreported or undetected. Data breaches touch all parts of society around the globe, from governments and businesses to celebrities and individual households. While many assume that breaches are the result of sophisticated malware or a well-resourced state actor, the reality is much more troubling. According to a recent report from the Online Trust Alliance, 90 percent of last year's breaches could have been prevented if organizations implemented basic cybersecurity best practices.<sup>1</sup> The Center for Internet Security describes these best practices as basic “cyber hygiene.” These include creating an inventory of authorized devices, identifying and patching software vulnerabilities in a timely manner, deploying

---

<sup>1</sup> <https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented>

strong malware defenses, backing up all systems, and utilizing data loss prevention technology to stop the unauthorized transfer of sensitive data.<sup>2</sup>

Statistics from our 2015 Internet Security Threat Report demonstrate that the cyber threats we are facing on a day-to-day basis are growing. Last year, five out of every six large companies (2,500+ employees) were targeted with spear-phishing attacks, a 40 percent increase over the previous year. Since the beginning of this year, more than 115 million identities have already been exposed, including major breaches in our government, financial, healthcare and educational sectors.<sup>3</sup> These breaches often expose real names, birth dates, and government ID numbers. This stolen data is often sold on the black market for other criminals to exploit (See attachment 1). In addition to their value on the black market, this personal information helps facilitate future attacks by providing cybercriminals a trove of information that can help them create highly customized phishing emails. Some breaches – such as the recent intrusions at the U.S. Office of Personnel Management – also expose other highly sensitive data. While we have not seen this data for sale on the black market yet, it may just be a matter of time.

While the focus on data breaches and the identities put at risk is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and can have dangerous consequences. There are a wide set of tools available to the cyber attacker, and the incidents we see today range from basic confidence schemes to massive denial of service attacks to sophisticated (and potentially destructive) intrusions into critical infrastructure systems. The economic impact can be immediate with the theft of money, or more long term and structural, such as through the theft of intellectual property and trade secrets. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in the Internet and their government. In some cases, cyber attacks can cause physical damage to our critical infrastructure systems and the computers that operate them.

The attackers run the gamut from highly organized criminal enterprises, disgruntled employees, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary – from pure financial gain, to the promotion of a political cause, to espionage (traditional spycraft or economic). These boundaries, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals often offer their skills for hire to the highest bidder. Attribution has always been difficult in cyberspace, and is further complicated by the ability of cyber actors to mask their motives and objectives through misdirection and obfuscation.

#### *Attackers are Moving Faster than Defenses*

Vulnerabilities have always been a big part of the security picture, where operating system and browser-related patches have been critical to keeping systems secure. However, the discovery of vulnerabilities such as Heartbleed and ShellShock, and their wide-spread prevalence across a number of operating systems, brought the topic front and center. Within four hours of the Heartbleed vulnerability becoming public, Symantec saw a surge of attackers stepping up to exploit it. Advanced attackers continue to favor zero-day vulnerabilities to silently sneak onto victims' computers, and last year we saw an all-time high of 24 used in attacks. As we observed with Heartbleed, attackers moved in to exploit these vulnerabilities much faster than vendors could create patches, and users could apply them.

<sup>2</sup> <https://www.cisecurity.org/documents/CSC-MASTER-VER5.1-10.7.2014.pdf>

<sup>3</sup> [http://www.idtheftcenter.org/images/breach/DataBreachReports\\_2015.pdf](http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf)

*Cybercriminals Are Streamlining and Upgrading Their Techniques*

With the glut of personal information on the Internet and black markets, attackers continued to breach networks with highly targeted spear-phishing attacks, which increased eight percent overall. Notably, they were more refined in their targeting than the previous year, deploying fewer emails per attack campaign. Attackers also perfected their use of watering hole attacks. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cyber criminals have become adept at lying in wait on legitimate websites and using them to try to infect visitors' computers. Watering hole attacks compromise legitimate websites that their victims are likely to visit and then modify the sites so that they will surreptitiously deliver malware to targeted companies.

Further complicating organizations' ability to defend themselves was the appearance of "Trojanized" software updates. Attackers identified common software programs used by targeted organizations, hid their malware inside software updates for those programs, and then waited for their targets to download and install that software – in effect, leading companies to infect themselves when they thought they were applying protective patches. Last year, 60 percent of all targeted attacks struck small- and medium-sized organizations. These organizations often have fewer resources to invest in security, and many are still not adopting basic best practices like blocking executable files and screensaver email attachments. This puts not only the businesses, but also their business partners who are often connected via computer networks, at higher risk.

*Malware Volume Increases and Becomes More Sophisticated*

We also saw the use of malware grow and become more sophisticated. In fact, more than 317 million new pieces of malware were created last year, meaning nearly one million new threats were released into the wild each day. Attackers are also figuring out ways to fashion their malware to avoid detection. In 2014, up to 28 percent of all malware was "virtual machine aware." Virtual Machines (VM) have become a common security tool, as potential malware can be detected, executed and analyzed without endangering the overall system. Unfortunately, this VM-aware malware can recognize that it is on a virtual machine and lie dormant until it determines that it is safe to execute. It can even transmit false data in an attempt to confuse security researchers.

**Botnets – Today and into the Future**

Much of the cybercrime we see today is facilitated by malicious botnets. They allow cybercriminals to exponentially increase their distribution power and provide a potent tool for any number of crimes.

A "bot" is a type of malware that allows an attacker to take control of an infected computer. Also known as "Web robots," bots are usually part of a network of infected machines, collectively known as a "botnet." These typically are made up of victim machines that stretch across the globe and are controlled by "bot herders" or "bot masters."<sup>4</sup> About half of these bots are what we would call helpful bots, such as the automated web crawlers that check to see that websites are running in good order or that index and update information for search engines. The others are malicious bots.

---

<sup>4</sup> "Bots and Botnets – A Growing Threat," *Symantec*, <http://us.norton.com/botnet/>

### Botnet Uses

The uses for malicious bots are only limited by the imagination of the criminal bot master. The most common use for botnets is still for Distributed Denial-of-Service (DDoS) attacks. DDoS attacks occur when multiple infected systems are used to overload a website with traffic and render it unable to respond to legitimate requests. Another recent use of DDoS attacks has been to provide cover for other, more sophisticated attacks. Organized crime groups have been known to launch DDoS attacks against banks to divert the attention and resources of the bank's security team while the main attack is launched, which can include draining customer accounts or stealing debit and credit card information.

Another common use for botnets is creating bitcoins, commonly known as bitcoin "mining." The mining process involves compiling information from recent bitcoin transactions and performing complex mathematical computations. Any single computer would take far too long to do the calculations to provide any value, so bot masters co-opt the processing power of thousands of hijacked computers to do so, thus "mining" valuable bitcoins for the bot master. Those bitcoins can then be used to purchase even more powerful cybercrime tools on the black market.

Cybercriminals also use botnets as launch points for attacks or to amplify their own processing power and bandwidth for various criminal activities such as spam generation, malware distribution and click fraud. Bot masters also can rent out their botnets for illegal purposes and can generate hundreds of thousands of dollars by making their botnets available to other users. Harvesting information such as passwords, credit card data, intellectual property, or other confidential information from infected computers is another common use for botnets. When this information is stored on a computer that is part of a botnet, the bot master has access to all of it – in an operational sense, they "own" that device. This information is often then sold to other criminals for fraudulent use.

### Efforts to Disrupt Cybercriminals

Every day we read about the impact of cybercrime, but we do not often hear about the successes that law enforcement and the private sector have had in thwarting crime and bringing these criminals to justice. Recently, we have seen a string of successful arrests and prosecutions of some of the most notorious cyber criminals in the world. Earlier this month, a New York judge sentenced Alexander Yucel, the creator of the *Black Shades* Trojan to five years in prison and the forfeiture of \$200,000. *Black Shades* was a password-stealing Trojan designed to infect computers and spy on victims through their web cameras, steal files and account information, and log victims' key strokes. Yucel was arrested by the U.S. Federal Bureau of Investigation (FBI) and Europol last year along with dozens of other individuals in the U.S. and abroad. Symantec worked closely with the FBI in this coordinated takedown effort, sharing information that allowed the agency to track down the location of the command and control infrastructure.<sup>5</sup> And just two weeks ago, Ercan "Segate" Findikoglu, the man who prosecutors say orchestrated one of the biggest cyber bank heists in American history was extradited to the U.S. to stand trial for stealing more than \$55 million by hacking bank computers and withdrawing millions in cash from ATMs.<sup>6</sup>

<sup>5</sup> <http://www.wsj.com/articles/blackshades-leader-sentenced-to-prison-1435093984>

<sup>6</sup> [http://www.nytimes.com/2015/06/25/business/suspect-in-55-million-atm-scheme-is-extradited-to-us.html?\\_r=0](http://www.nytimes.com/2015/06/25/business/suspect-in-55-million-atm-scheme-is-extradited-to-us.html?_r=0)

We have also seen a number of successful takedown operations against prominent financial fraud botnets. In June of 2014, the FBI, the U.K. National Crime Agency, and a number of international law enforcement agencies mounted a major operation against the financial fraud botnet *Gameover Zeus* and the ransomware network *Cryptolocker*. *Gameover Zeus* was the largest financial fraud botnet in operation last year and is often described as one of the most technically sophisticated variants of the ubiquitous *Zeus* malware. Symantec provided technical insights into the operation and impact of both *Gameover Zeus* and *Cryptolocker*, and worked with a broad industry and government coalition during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cybercriminals behind both threats.<sup>7</sup>

In July 2014, another law enforcement operation targeted the group behind *Shylock*, another dangerous financial fraud botnet, that was designed to intercept online banking transactions and steal victims' credentials. *Shylock* was responsible for the theft of millions of dollars from victims before the U.K.'s National Crime Agency seized the command and control servers, and the domains that *Shylock* used to communicate between infected computers.<sup>8</sup>

And in February of this year, an operation led by Europol struck against the *Ramnit* botnet and seized its servers and infrastructure. *Ramnit* facilitated a vast cybercrime operation, harvesting banking credentials and other personal information from their victims. The group was in operation for at least five years and in that time evolved into a major criminal operation, infecting more than three million computers.

These law enforcement operations and others have knocked out or severely curtailed the operations of some of the most prominent financial fraud groups in the world. In fact, the number of bots declined by 18 percent in 2014 compared to the previous year. In large measure, this decline is because the FBI, the European Cybercrime Centre (EC3) at Europol, and other international law enforcement agencies, working with Symantec and other technology companies, disrupted and shut them down.

Unfortunately, these successes have led to the emergence of new threats, such as the *Dyre* group. In a very short time, the *Dyre* financial fraud bot has emerged as another dangerous financial Trojan, capable of defrauding customers from a range of financial institutions spanning multiple countries. *Dyre* is capable of using several different types of man-in-the-browser (MITB) attacks against the victim's web browser to steal credentials. One such MITB attack involves scanning every web page a user visited and checking it against a list of sites that *Dyre* is pre-configured to attack. If a match is found, it redirects the victim to a fake website that looks similar to its genuine counterpart. This fake website will harvest the victim's credentials before redirecting back to the genuine website.<sup>9</sup>

#### **Enhancing Cybersecurity Through Public-Private Partnerships**

Preventing data theft caused by bots and protecting privacy starts with basic electronic device hygiene such as having security software installed, good patch management practices, using strong passwords, and recognizing suspicious emails. But that is just the start, because as we have seen in these high

<sup>7</sup> <http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network>

<sup>8</sup> <http://www.symantec.com/connect/blogs/all-glitters-no-longer-gold-shylock-trojan-gang-hit-takedown>

<sup>9</sup> <http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat>

profile botnet cases, sophisticated and well-funded attackers are persistent and highly skilled. Anti-virus software (AV) should be part of any security program and will stop known malware, but it is just one element in a broad security toolbox.

Today, even moderately sophisticated malware have unique signatures and can slip past systems that are using only AV software. Thus, strong security is layered security – in addition to basic computer hygiene and AV, consumers and organizations need comprehensive protection that includes intrusion protection, reputation-based security, behavioral-based blocking, and data loss prevention tools. These advanced tools look not just for known threats, but they can check the reputation of any file that is loaded on a computer and look for other behavior that could indicate the presence of previously unknown malware.

However, even with modern security suites, there is a risk that your device or network may become compromised. If that occurs, there are a number of things Symantec is doing to assist victims of botnets and other types of cybercrime. It is important to recognize that these are not victimless crimes; at best, owners of infected computers suffer decreased functionality, and at worst they have their identities compromised and their bank accounts raided. Part of our efforts to stop botnets, and indeed cybercrime *writ large*, is helping individual victims.

In April 2014, we partnered with the National White Collar Crime Center (NWC3) to develop an online assistance program, VictimVoice.org, that helps cybercrime victims better understand the investigation process and help prevent future attacks. We also make security tools available to the public to assist them if they are infected by a botnet. For example, we offer free software that allows victims of ransomware and botnets to remove malware from their system.<sup>10</sup>

Because cyberspace is a domain without borders, where crimes are often committed at a great distance, every device in the U.S. is a potential border entry point, making investigation and prosecution of cybercrimes a difficult task. This reality makes international engagement on cybersecurity essential. For example, Symantec recently partnered with AMERIPOL and the Organization of American States to publish a report that provides the most comprehensive snapshot to date of cybersecurity threats in the Latin American and Caribbean region. The goal was to raise awareness of cybercrime issues and promote the importance of cybersecurity throughout the region as a national and economic security imperative.<sup>11</sup> Similarly, Symantec is partnering with the African Union and the U.S. Department of State to develop a report looking at the cybersecurity threats and trends in Africa. That report will be published later this year.

Symantec also maintains close relationships in the U.S. and around the world with international cyber response organizations and law enforcement entities including INTERPOL, EUROPOL, and dozens of national Computer Emergency Response Teams (CERTs) and police forces. Among other things, we share the latest security technology trends, threats, and the techniques that cyber criminals use to launch attacks.

Private to private partnerships have also proven to be effective in fighting cybercrime. An excellent example of the private sector banding together is the establishment of the Cyber Threat Alliance (CTA). The CTA is a group of cyber security practitioners founded in 2014 by Symantec, Fortinet, Intel Security

<sup>10</sup> [http://www.symantec.com/security\\_response/removaltools.jsp](http://www.symantec.com/security_response/removaltools.jsp)

<sup>11</sup> <http://www.symantec.com/page.jsp?id=cybersecurity-trends>

and Palo Alto Networks who share threat information to improve defenses against advanced cyber adversaries across member companies. By sharing detailed security information, we can improve overall protection for our customers. The bulk of information sharing before the CTA was established primarily involved sharing malware samples. The CTA builds upon this foundation to combat advanced attacks by sharing more actionable threat intelligence, including data on zero day vulnerabilities, botnet command and control server information, mobile threats, and indicators of compromise related to advanced persistent threats.<sup>12</sup>

#### **A Path Forward – Improving Laws to Fight Cybercriminals**

Symantec welcomes the Subcommittee’s sustained interest in fighting cybercrime, and appreciates your efforts to provide additional legal tools to fight this growing threat. We believe there are several areas that Congress could act on to help fight cybercrime and strengthen cybersecurity.

First, Symantec supports amending the Computer Fraud and Abuse Act (CFAA), which is the most important law that prosecutors rely on when taking down botnets. While the CFAA has undergone some changes over the years to keep up with changing technology and evolving threats, more changes are needed. Today, laws allow courts to issue injunctions for crimes involving fraud and illegal wiretapping. Using this law, the Department of Justice has had some notable successes in shutting down botnets. However, botnets also are used for crimes such as DDoS attacks, and for stealing sensitive corporate information. In those cases, an injunction to disrupt a botnet may not be considered by a court due to limits in the existing law. Symantec supports an amendment to the CFAA that would permit judges to issue an injunction against those operating a malicious botnet. This measure would enable authorities to act quickly when a malicious botnet is putting financial or personal information at risk.

Second, we agree with the Department of Justice’s recommendation that Congress should modify the so-called “access device fraud statute”, 18 U.S.C. § 1029, to allow prosecution of offenders based in other countries who directly and significantly harm individuals or financial institutions in the U.S. This would provide prosecutors the ability to bring charges against foreign criminals that possess or sell stolen credit card numbers, regardless of whether that individual is the one that stole the information in the first place. Prosecutors need this measure in order to pursue the entire criminal chain of individuals that profit from stolen financial information, not just those who conducted the attack.

Third, international cooperation is hampered by outdated legal mechanisms. In order for governments to share cyber information on criminal investigations and prosecutions, we must still proceed through Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory – processes first developed in the 1800s – that take far too long to address the real-time nature of cybercrime. To keep pace with 21st Century threats, the MLAT process should be overhauled and streamlined.

Fourth, intrusions into the computers and systems that run our critical infrastructure are increasing in volume and becoming more sophisticated. For instance, destructive cyberattacks against a power plant or transportation systems could cripple our economy and endanger lives. Symantec supports an amendment to the CFAA that creates a violation and enhanced penalties for criminals who knowingly cause damage to a computer that controls critical infrastructure systems.

---

<sup>12</sup> <http://cyberthreatalliance.org>

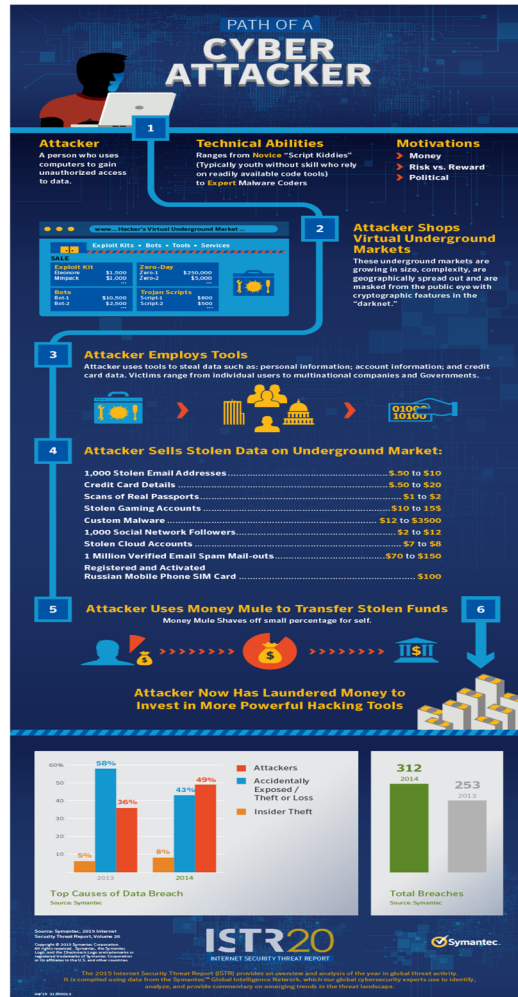
Last, we should remain vigilant against new laws and regulations that are not properly considered or vetted, no matter how well meaning their intent may be. For instance, last month the Department of Commerce published a proposed rule, stemming from the Wassenaar Arrangement, that imposes strict controls on the export of certain cybersecurity items. Our concern is that, as written, the rule is so vague that it could potentially cover a wider range of cybersecurity products and processes than the Department of Commerce had originally intended. As such, the rule could inadvertently impair security research, damage U.S. security companies, and severely impair our ability to protect our customers around the world.

#### **Conclusion**

As this subcommittee knows better than most, we still face significant challenges in our efforts to fight cybercrime and take down botnets. We have made notable progress over the last year but the attackers have evolved and continue to become more sophisticated. Today, both government and industry recognize the imperative for cooperation to fight cybercrime. No single organization can “go it alone” in the current threat landscape. The threats are too complex and the stakes are too high. Ultimately, defeating criminal networks and deterring cybercrime requires strong technical capabilities, effective countermeasures, industry collaboration and smart changes to existing laws that empower law enforcement while still protecting individual rights.

At Symantec, we are committed to improving Internet security across the globe, and will continue to work collaboratively with international industry and government partners on ways to do so. I would also like to commend this subcommittee for its leadership on this important issue. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

## Attachment 1



**SENATOR LINDSEY O. GRAHAM**

**JULY 15, 2015**

**U.S. SENATE COMMITTEE ON THE JUDICIARY**

**SUBCOMMITTEE ON CRIME AND TERRORISM**

**RE: "CYBER CRIME: MODERNIZING OUR LEGAL FRAMEWORK FOR  
THE INFORMATION AGE"**

**QUESTION FOR THE RECORD FOR MR. DAVID BITKOWER:**

1. Your testimony at the July 8, 2015 hearing established that the amount of money being stolen, and at risk of being stolen, in physical bank robberies is dramatically less than the amount of money being stolen, and at risk of being stolen, through cybercrime. How does the allocation of Department of Justice resources towards preventing financial loss through physical bank robberies and other physical financial crimes compare to the allocation of Department of Justice resources towards preventing financial loss through cybercrime?

**Hearing before the Senate Committee on the Judiciary**  
**“Cyber Crime: Modernizing our Legal Framework for the Information Age”**  
**Questions for the Record Submitted by Senator Al Franken**

**Questions for Ms. Ellis:**

The Computer Fraud and Abuse Act (CFAA) – with its various penalties – is aimed, in part, at deterring cyber-crime. According to your testimony, the threat of punishment works to deter legitimate security researchers.

Do you think it has the same effect on real cyber-criminals, including those overseas? If not, where do you think the government ought to be focused if our goal is preventing cyber-crime?

**Questions for Mr. Bitkower:**

I was pleased to see that the Department of Justice’s cybercrime proposal aimed to improve the agency’s ability to address the manufacture and sale of spyware or stalking apps. As the Ranking Member on the Subcommittee on Privacy, Technology, and the Law, addressing stalking apps has been a focus for me. Many of these apps work by surreptitiously intercepting individuals’ location information. I’ve developed legislation that would bar the manufacture of these apps in the same way that spyware intended to surreptitiously intercept phone calls or emails is prohibited under federal law.

Please describe the chief obstacles – legal or otherwise – that the Department has faced to date when trying to address the growing problem of stalking apps.



**Hearing before the Senate Committee on the Judiciary**  
**“Cyber Crime: Modernizing our Legal Framework for the Information Age”**  
**Questions for the Record Submitted by Senator Al Franken**

The Computer Fraud and Abuse Act (CFAA) – with its various penalties – is aimed, in part, at deterring cyber-crime. According to your testimony, the threat of punishment works to deter legitimate security researchers.

**Do you think it has the same effect on real cyber-criminals, including those overseas? If not, where do you think the government ought to be focused if our goal is preventing cyber-crime?**

Thank you for your question Senator Franken.

In order for penalties to deter crime, criminals need to believe they will be caught<sup>1</sup>. Cybercriminals often don't believe they will get caught, particularly those operating in countries such as China and Russia. So no, I do not believe the threat of punishment deters real cyber-criminals nearly as much as it chills legitimate researchers working to make us safer.

If this is in doubt, we need only look at the booming cybercrime economy and increasing number of attackers. Understanding the elements driving this is a good place to start thinking about prevention:

- Opportunities for cybercriminals abound as our reliance on “connected” technologies increases. The complexity of these technologies provides the opportunity for attacks, while the connectedness enables foreign actors to reach us remotely.
- Attackers are strongly incentivized as it is easy to monetize them through crypto currencies and thriving black markets.
- There are almost no barriers to entry as people share so much information about themselves on the internet, making them easy targets and convenient entry points for attacks on organizations. For more advanced technical requirements, there is a thriving market of hacker-for-hire tools and services.
- These factors provide even stronger incentives in countries with high unemployment/low incomes and wide availability of technical infrastructure (e.g. China and Russia)

To prevent cybercrime in this context, we must address the factors above. The most pragmatic approach is to try to reduce the number of opportunities, and raise the barriers to entry for attackers. To do this requires a combination of measures:

- We must identify and mitigate the bugs in technological systems that create opportunities for attackers. This is where security research plays a critical role, so it is essential that we support research efforts and not chill them legislatively or prosecutorially.
- We must encourage organizations to adopt basic security hygiene and best practices, such as deploying the latest patches; avoiding technologies with a poor security track record; regularly testing for the effectiveness of defenses, optimal configurations of technology, and the likely impact of an attack; using strong encryption standards and not storing non-essential data; etc.
- We must build greater awareness of security threats and best practices for avoiding them amongst consumers and organizations. All internet users should know how to spot phishing attacks, and protect their credentials appropriately.

I would be happy to discuss this in further detail, and again, thank you for the question.

<sup>1</sup> “Deterrence in Criminal Justice,” The Sentencing Project, 2010:  
<http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf>

STATEMENT FOR THE RECORD

ON BEHALF OF

THE NATIONAL ASSOCIATION OF CONVENIENCE STORES

AND

THE SOCIETY OF INDEPENDENT GASOLINE MARKETERS OF AMERICA

FOR THE

HEARING OF THE SENATE JUDICIARY SUBCOMMITTEE ON CRIME AND  
TERRORISM

JULY 8, 2015

“CYBERCRIME: MODERNIZING OUR LEGAL FRAMEWORK FOR THE INFORMATION  
AGE”

Chairman Graham, Ranking Member Whitehouse and members of the subcommittee, thank you for giving us the opportunity to submit this statement for the record on the topic of the elements of sound data breach legislation. We are submitting this statement on behalf of both the National Association of Convenience Stores (NACS) and the Society of Independent Gasoline Marketers of America (SIGMA).

NACS is an international trade association composed of more than 2,200 retail member companies and more than 1,600 supplier companies doing business in nearly 50 countries. The convenience and petroleum retailing industry has become a fixture in American society and a critical component of the nation's economy. In 2013, the convenience store industry generated almost \$700 billion in total sales, representing approximately 2.5% of United States GDP.

SIGMA represents a diverse membership of approximately 270 independent chain retailers and marketers of motor fuel. Ninety-two percent of SIGMA's members are involved in gasoline retailing. Member retail outlets come in many forms, including travel plazas, traditional "gas stations," convenience stores with gas pumps, cardlocks, and unattended public fueling locations. Some members sell gasoline over the Internet, many are involved in fleet cards, and a few are leaders in mobile refueling.

Collectively, NACS and SIGMA represent an industry that accounts for about 80 percent of the motor fuel sales in the United States. And, this is truly an industry of small businesses. While many motor fuel outlets have agreements to use the brand names of major oil companies, those oil companies have largely exited the retail market. The vast majority of those branded outlets are locally owned. For example, more than 70 percent of the NACS' total membership is composed of companies that operate ten stores or less, and more than 60 percent of the membership operates a single store.

With this testimony, we will briefly lay out the interest our members have in this area, note how the payment card system impacts our data security efforts, provide background on data breaches, note the current state of the law on data breach notification, and walk through the elements of data breach legislation that we consider to be most important. We also note that data security ought to be a primary focus given that notice laws have already proliferated around the country.

#### Convenience and Motor Fuel Outlets Interest

With so many small businesses, some may wonder why our industry is concerned about data breaches. Our retailers typically do not store much information about their customers. They store employee information, but the primary reason data breaches affect these small, medium, and larger businesses is that these retailers handle payment card information in order to facilitate transactions that occur every day. In light of the number of fuel and other transactions that our industry engages in, we handle approximately one of every 22 dollars spent in the United States. In fact, our retailers serve about 160 million people per day – around half of the U.S. population. And, a majority of those transactions are made using payment cards.

### The Payment Card System in the United States

Unfortunately, in the United States, payment card information is more vulnerable and enticing to data thieves than it should be. The dominant payment card networks, Visa and MasterCard, control the security of payment cards through promulgating their own proprietary specifications for those cards and their use as well as through the Payment Card Industry (PCI) organization they created and dominate. PCI not only sets data security standards for cards and card issuance, but also for retailers, like NACS and SIGMA members, that accept such cards. This creates an odd dynamic. The companies we represent, and other retailers, do not decide their own data security standards, the payment card networks do that.

Having PCI set data security standards for retailers has not worked well. PCI has consistently put the profits of the companies that control it (principally, Visa and MasterCard) before good security. They have set standards that are both more expensive for retailers than they should be and less effective at providing security than they should be. That is a remarkable combination. Unfortunately, as card security expert Avivah Litan of Gartner Research wrote recently, “The PCI (Payment Card Industry) security standard has largely been a failure when you consider its initial purpose and history.”<sup>1</sup>

For example, the cheapest, most effective way to better protect against the fraudulent use of payment card numbers is to require another piece of information with those numbers in order to make them useable. The financial industry knows this well. That is why, every time any one of us uses a payment card – whether it’s a debit or a credit card – to access our accounts at an automated teller machine (ATM), we enter a personal identification number (PIN). If we don’t enter a PIN, we don’t get to engage in a transaction. The account number of the card is meant to demonstrate the actual card is there and being used (though this has become less effective in the last generation leading to the move to computer chips in cards throughout the world), and the PIN is meant to demonstrate that the person using the card is the person authorized to do so. It does not make sense that the same financial institutions that insist a PIN is used to authenticate the person when someone tries to enter into a transaction with them, do not want consumers to have to enter a PIN when they enter into a transaction with a merchant.

The reason that financial institutions are not as interested in protecting against fraud on transactions with merchants as they are in protecting against fraud on transactions with financial institutions themselves is that those financial institutions push many of the losses from fraudulent transactions onto merchants. While the financial industry often claims that it provides merchants with a “payment guarantee”, it does no such thing. The Federal Reserve studied this a few years ago and found that, on debit transactions that did not use a PIN, merchants paid for more than 40 percent of fraud losses.<sup>2</sup> On credit card transactions, merchants pay for the majority of fraud losses. At our members’ gas pumps, for example, we pay for about 74 percent of fraud losses on debit and credit cards.<sup>3</sup>

<sup>1</sup> “How PCI Failed Target and U.S. Consumers,” by Avivah Litan, Gartner Blog Network, Jan. 20, 2014, available at <http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/>.

<sup>2</sup> 77 Fed. Reg. 46261, 46262 (Aug. 3, 2012).

<sup>3</sup> *Id.*

That is a major reason why PCI does not have the incentive to require the most effective security. The institutions that have the primary voice in PCI's work don't feel the full brunt of the economic consequences of their decisions.

What does this mean for the security of payment card data? Well, if payment card numbers themselves could not be monetized, there would be far less financial incentive for thieves to try to steal that information. PIN numbers are harder to steal than payment card numbers because PINs are typically encrypted as they are entered and remain that way for most of their travels through the payment card system. The major breaches that have garnered news attention during the past year – at banks and at merchants – have not involved the loss of PINs. There is some ability for data thieves to guess some PINs and, at the margins, find some ways to monetize payment card data even when PINs are required. But thieves' ability to make money from stolen payment card numbers is greatly diminished when PINs are required.

Requiring the use of PINs is not a silver bullet solution. There is far more to it than that. But, the failure of the financial industry to make that simple move, and one that is cheap and easy for the vast majority of merchants, is emblematic of the problems we all face protecting payment card data from breaches today.

#### The Picture of Data Breaches

Data thieves steal information from every type of organization in the United States. No one is immune. Manufacturers, utilities, services companies, health care providers, educational institutions, not-for-profits, telecommunications companies, banks, credit unions, payment card networks, payment card processors and merchants have all suffered data breaches. In fact, government agencies also suffer data breaches. Victims of breaches have even included the Defense Department and National Security Agency. These organizations are true experts in this area that go to great lengths to protect their systems. But, again, no one is immune.

Unfortunately, data thieves today include foreign countries and well-funded, sophisticated organized crime organizations, among many others. These thieves know where vulnerabilities are and relentlessly work to exploit them. It is very difficult to protect against these thefts. U.S. entities that suffer data breaches are victims of these crimes. That does not mean they shouldn't have any responsibilities when they are victimized, but it's worth remembering when some want to take a punitive approach to those who suffer breaches.

The Verizon Data Breach Investigations Report is the most comprehensive summary of data threats. The 2014 report (examining 2013 data) determined that there were 63,437 data security incidents reported by industry, educational institutions and governmental entities last year and that 1,367 of those had confirmed data losses. Of those with confirmed data losses, the financial industry suffered 34%, public institutions (including governmental entities) had 12.8%, the retail industry had 10.8%, hotels and restaurants combined had 10%, and, as noted above, other sectors suffered breaches as well. When reviewing these numbers, it is worth keeping in mind that there are approximately 1,000 times as many retailers in the country as there are financial institutions.

### Current State of the Law

Before getting into questions about a potential legislation, it is worth taking a look at the current state of the law. A total of 51 U.S. states and territories have data breach laws on the books today. Companies comply with these laws every day. This is not an area in which there is a lack of regulation.

Many of these 51 laws are very similar. While there may be some benefits to streamlining this system by having one federal law that pre-empts these 51 different laws, that should only be done if it can improve upon the current law. It would be simpler and cheaper for businesses to comply with one law than with many, but that is not the only value at stake in this discussion. Any effort to write federal legislation should take care not to introduce problems that the current law does not have.

### Elements of Data Breach Law

There are several elements that we see as important to a federal law on data breach. First, the law should not have holes in it that result in consumers not getting notice. Second, the law should create a level playing field for businesses so that it does not introduce gaps that data thieves can exploit and does not overly burden any particular sector of the economy. Third, the law needs to have sufficient flexibility to cover the many different circumstances arising from different data breaches. This includes requiring notice only when it makes sense to do so and allowing sufficient flexibility on timing for proper investigations of data incidents to take place. Fourth, the law should not take a punitive approach to businesses that have their data stolen by thieves. Fifth, if there is going to be a law, it should pre-empt state laws. There is no need for a fifty-second data breach law.

### Don't Create Notice Holes

In most instances, when data breaches happen today, consumers can have confidence that if the breach exposes data in a way that may harm them, they will get notice. The 51 different laws around the country help ensure that this happens. That is as it should be.

There are, however, exceptions to this general confidence. The data breach guidance put in place pursuant to the Gramm Leach Bliley Act (GLBA), for example, does not provide such confidence when financial institutions have data breaches. GLBA guidance says that banks and credit unions should have response plans in place in case their systems are breached, but those response plans are not actually required.<sup>4</sup> GLBA guidance recommends that financial institutions have plans in place to provide consumer notification of data breaches, but again those plans are not required.<sup>5</sup> Following a breach, GLBA guidance says that banks should conduct an

<sup>4</sup> Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS) at ¶ III, C.

<sup>5</sup> Incident Response Guidance, 70 Fed. Reg. 15736 (Mar. 29, 2005) promulgating 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12

investigation to determine the likelihood that information has been or will be misused as a result of the breach, but that investigation is not required.<sup>6</sup> GLBA guidance also provides that if a financial institution determines that customer information has been or is likely to be misused then the institution should notify its customers.<sup>7</sup> But, here again, such notice is not required. In short, GLBA results in a system of law in which financial institutions have discretion over how closely to look at their data breaches and whether to inform their customers, if at all. In fact, we are not aware of any financial institutions that have been investigated and fined for not adequately looking into a data breach or not providing customers with notice of such a breach.

Last August, JP Morgan Chase suffered the largest data breach in U.S. history. That breach was reportedly part of a pattern of breaches of financial institutions that included breaches of perhaps a dozen or so banks. In spite of this, only a few of the names of these banks have ever been reported. In fact, even the JP Morgan Chase breach became public only because there was a reference to it in a filing the bank made with the Securities and Exchange Commission. Once it became a front page story, JP Morgan Chase provided notice of its breach. It is not clear which of the other affected banks did the same. And, under GLBA, that appears to be just fine. In October, the USA Today reported that FBI officials had warned that 500 million financial records had been stolen from banks over the previous year. It is not clear how many of those incidents resulted in notice to consumers.

Thankfully, the majority of state laws help patch this major shortcoming in federal law. Based on our analysis, thirty-seven of the fifty-one state and territorial data breach laws cover banks while fourteen of them exempt banks. That helps, but it isn't good enough to provide consumers with the confidence they should have that they will get notice when it is warranted. Any federal law on data breach needs to fix this hole in the current notice system or it is ignoring the most prominent shortcoming of the current system of notice for data breaches around the country.

#### Create a Level Playing Field

Ensuring there are no holes in data breach notice provisions goes hand-in-hand with establishing a level playing field for businesses that handle data. Many types of data are transmitted between different businesses on a regular basis but this is particularly true of payment card data. In fact, merchants, data line providers, processors, acquiring banks, card networks, and card issuers transmit data back-and-forth among one another hundreds of millions of times per day. If data breach legislation focuses on some of these businesses and does not cover others the same way, a couple of problems will result. One is that the lack of standards for some will, because the businesses will operate with different incentives, lead to data security gaps that thieves will exploit. Two is that some businesses will take on the brunt of the costs and reputational harms that can come with notice responsibilities even when they are not responsible for some of those breaches. That would not be appropriate.

---

C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS) [hereinafter *Response Guidance*].

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

The problem of data security weaknesses in the transfer of data among businesses is already part of the landscape. For example, merchants are required by the payment card companies to encrypt payment card data when they hold it on their systems. But, financial institutions are not required to be capable of accepting that data in encrypted form. The result is that data must be de-encrypted as it runs through the payment system in order to complete a transaction.<sup>8</sup> Data thieves have targeted these points of vulnerability in past data breaches. If we are going to have federal legislation, it should avoid creating similar gaps by covering everyone in the payment data chain with the same laws.

For some reason, telecommunications providers have argued that they should not have the same responsibilities as other companies that handle data. Some have raised a fallacious concept to justify this position. They claim that data lines controlled by telecommunications providers are “dumb pipes.” Nothing could be further from the truth. Data lines include switches and routers throughout them that can monitor the carriage of data, watch for problems, and ensure transmissions get to the right place. This is all necessary to making the system operate correctly.

But these complexities are why the Federal Communications Commission and the Congress are considering the issue of net neutrality. If telecommunications lines were actually “dumb” they could not be anything other than neutral. We are not aware, for example, of anyone calling on this committee to examine water or sewer line neutrality. The phrase and concept of “dumb pipes” simply has no place in the discussion of data breaches.

The switches and routers in telecommunications lines consist of millions of lines of computer code – and they have vulnerabilities. In fact, by law these systems are required to have backdoors allowing the companies to tap those lines and access the data being sent. Those requirements are in place so that law enforcement can gather information being transmitted when appropriate. When legitimate actors can access communications in transit to monitor data, unfortunately, illegitimate ones can as well. No one’s system is completely immune from data thieves. Telecommunications providers, just like other businesses, have suffered data breaches in the past. There is no principled basis for absolving these companies from the responsibilities that others have when their systems are breached.

Other businesses should not carry the burden, reputational or otherwise, when telecommunications companies suffer breaches. That is especially true of small businesses. These businesses work hard to secure their own systems, but they don’t have the same resources or sophistication to follow the work of data thieves that big businesses (including many telecommunications companies) do. If a telecommunications provider or financial institution tells a small business that the small business suffered a breach, that small business usually accepts that as fact. But the initial assessment of where a breach occurred is often wrong and if the telecommunications provider and financial institution do not have their own legal responsibilities regarding breaches of their systems, many breaches will be laid at the doorstep of others and no one will ask more questions. If a federal law is going to empower regulators to look into these situations, they must have the latitude to look at everyone involved to ensure they

---

<sup>8</sup> The Nilson Report, Issue 934, Sept. 2009 at 7.

live up to their responsibilities – and don’t simply pawn off those responsibilities onto smaller players with fewer resources.

#### Provide Flexibility

Data breaches can be difficult to detect and it can be even more difficult to determine the full extent of some of them. The complexity of breaches has consistently increased over time along with the increased sophistication and funding of organized crime. In fact, two-thirds of data breaches take months to discover.<sup>9</sup> Providing public notice of data breaches before the full extent of a breach is known, and therefore before a business can be sure that its system is fully secure, can create increased risk for consumers and business. If data thieves become aware that they have been detected, which notice would make clear, they often try to quickly grab as much additional data as they can as fast as they can. That is not a risk that legislation needs to create by setting an arbitrary timing requirement for notice. While many laws provide exceptions to notice requirements when law enforcement requests a delay, that alone may not be sufficient to protect against this type of problem.

In order to avoid setting a requirement that notice be given before a system is fully secured, a flexible timing requirement that includes the concept of the business need for fully protecting against further data theft would be wise.

#### Avoid Punitive Approaches

As noted previously, companies that suffer data breaches are victims of crimes. Without question, consumers and businesses that have their data stolen are victims of crime as well. Some media accounts of these incidents, however, seem to overlook what a significant and difficult problem it is to protect against data thieves. If the Defense Department and NSA can be hacked, it demonstrates how difficult the challenge is for private businesses to fully protect themselves. Given the difficulty, overly punitive measures are not appropriate in these situations. We are not saying that a failure to follow a notice law should not have any penalty associated with it. That can be necessary in some cases to get some businesses to comply. But the penalties should not be ones that are overwhelming, especially for small businesses. The goal should be to help businesses comply with the law to the greatest extent possible – not to play a “gotcha” game that leads to large fines. The costs of dealing with breaches, including paying forensic experts, lawyers, fraud costs, and dealing with reputational harms, already create strong economic incentives for businesses to try to avoid breaches. If one occurs, it should not simply be an excuse to pile on additional financial hits.

#### Pre-empt State Laws

As noted, there are two primary rationales for having a federal data breach law in light of the fact that the 51 state and territorial laws that currently exist cover the area well already. The first reason is to plug the holes that exist in the coverage of these laws today. Most prominently, a federal law would improve on the current set of data breach laws by removing the overly broad discretion given to financial institutions in the fourteen states that exempt them from their laws.

---

<sup>9</sup> 2013 Data Breach Investigations Report, Verizon.

The second reason for a federal law is to create a simpler and more efficient notice system. That way, businesses would only have to comply with one federal law rather than as many as 51 different ones. That efficiency can only be achieved if the state laws in this area are pre-empted. To the extent that pre-emption is not clear, a federal law would become the fifty-second law to comply with and the second rationale for having a federal law at all would be undermined. This pre-emption is necessary then for a federal law to make sense.

Pre-emption, however, makes it even more important to get any federal data breach law right. The state system currently ensures that people get notice in most of the situations that they should. That should not be undermined in the process of creating a federal law. In our view, the principles we've laid out above, if followed, would help protect against the potential negative consequences that could come from pre-emption. Given the hazards, however, we urge that the committee take its time and not rush through legislation before fully weighing all of the trade-offs between a federal bill and the state and territorial laws on the books.

#### Data Security

One thing worth emphasizing here is that data breach notification should not be the first priority in this area. As noted, notice is well-regulated today. Our first priority would be to focus on preventing data breaches. Merchants, including NACS and SIGMA members, collectively spend more than \$6 billion per year just securing payment data.<sup>10</sup> Spending on all data security certainly exceeds this amount. Doing common-sense things like requiring PINs on payment card transactions, developing encryption and tokenization technologies that are effective (and open to all in the industry rather than creating competitive market problems), and increasing information-sharing with private industry and between the private sector and government are all measures that could demonstrably improve our ability to prevent data breaches in the first place. Many of the challenges in these areas stem from problematic standard-setting in the payment card arena and we would urge that particular attention be paid to those issues given the vulnerabilities that anti-competitive standard-setting has allowed to fester.

And, given the prevalence of foreign states in data breaches today, it may be time to more deeply examine to what extent our prism for viewing data security should be based on a national security model rather than a criminal justice model. It may be that, as with national security threats in the physical world, the resources available to data thieves are outstripping the ability of private businesses to individually deal with these threats. That is an issue that this and other committees ought to consider.

\* \* \*

We appreciate the subcommittee providing us with this opportunity to submit our views. We look forward to working with you as the committee continues to consider this topic.

---

<sup>10</sup> "Credit Card and Debit Card Fraud Statistics," CardHub 2013, available at <http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/>.