CYBER CRIME: MODERNIZING OUR LEGAL FRAMEWORK

FOR THE INFORMATION AGE

- - -

WEDNESDAY, JULY 8, 2015

United States Senate,

Committee on the Judiciary,

Washington, D.C.

The Committee met, pursuant to notice, at 2:21 p.m., in room SD-226, Dirksen Senate Office Building, Hon. Lindsey Graham, Chairman of the Subcommittee on Crime and Terrorism, presiding.

Present: Senators Graham, Cornyn, Whitehouse, Klobuchar, and Blumenthal.

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

Senator 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. So 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. But 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. So 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. But 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 non-defense 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. So to those who say that we do not need to deal with sequestration on the non-defense 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 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. And 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 two 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. So 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.

Senator Graham. Thank you.

Could you please stand?

[Witnesses sworn.]

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

Mr. Bitkower. You did, sir.

Senator 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 DAVID BITKOWER, DEPUTY ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, CRIMINAL DIVISION

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 in -- 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 obtain 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 affected 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 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.

Senator 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.

Senator 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.

Senator 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 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.

Senator Graham. So 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.

Senator Graham. Okay. And 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.

Senator 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.

Senator 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 it is a narrow interpretation. The statute is "more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking to circumvent -- circumvention of technological access barriers, not misappropriation of trade secrets, a subject Congress has

dealt with elsewhere."

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."

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 in the 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 effect 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 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. And then going to the $5,000 figure, how did you arrive at that figure? What is the rationale or justification for it?

Mr. Bitkower. Well, 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 am I 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 and it is true however that that is a compromised position that you are hearing from the government.

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

Mr. Bitkower. Thank you.

Senator 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. But 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.

But according to reports, Cardinals 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.

But assuming these facts are true, is there a potential violation of the Computer Fraud and Abuse Acts prohibition against accessing a protected computer without authorization?

Mr. Bitkower. Thank you, Senator, and of course and as of course 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, 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. And 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 a liability there.

Senator Cornyn. And 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 read the same reports that you have and that you referred 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, and 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.

But when we pull back and look at the larger spectrum of cyber threats that include 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 response.

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 into American courtrooms to face justice. So 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.

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

Senator Whitehouse. We will stipulate to that.

Senator Graham. Senator Whitehouse?

Senator Whitehouse. Thank you, Chairman. I appreciate this. And 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.

But when we talk about foreign actors in particular, we have certainly seen foreign actors around the globe targeting American systems because of the valuable and sensitive information that is contained there and 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 and 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 the next will trade 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 and when they are of course are 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.

So adding the hacking statute as a predicate for money laundering or RICO would allow us in certain cases where we are targeting 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. And 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 prosecution now in the District of Nevada which uses the RICO statute to go after a set 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 National Security

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. And 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 five 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. Well, 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. So 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. But 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 and 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.

But 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.

So 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. And 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 wouldd say resources, other things.

Mr. Bitkower. So certainly other than the proposals we have set forth in the President's legislative proposals, certainly resources are a major concern for us. And 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 ten times the budget of our computer crime intellectual property section for a year.

Senator Klobuchar. Yes. And 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.

But 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. So 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.

Senator 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, terrorists acts as 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.

Senator 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.

So I heartily endorse your earlier comments about sequestration.

Senator Graham. Thank you very much, Mr. Bitkower.

Mr. Bitkower. Thank you.

Senator Graham. Next panel, please.

[Pause.]

Senator Graham. Thank you all for coming. Please

stand.

[Witnesses sworn.]

Senator 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

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 and 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 multi-faceted 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 five years ago were the first to really attempt botnet take downs 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 take down 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 Europole's European Cyber Crime Center.

So 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 within 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.

STATEMENT OF JEN ELLIS, SENIOR DIRECTOR OF COMMUNITY AND PUBLIC AFFAIRS, RAPID7

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 use 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 trouble makers.

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.

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

Mr. Wright. Thank you. Chairman Graham, Senator Whitehouse and Members of the subcommittee, thank you for the opportunity 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 three 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 which 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 three 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. So 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 bot master. From DDoS attacks to bitcoin mining bitcoin mining to harvesting personal information from infected computers, similar to hackers for hire, bot

masters 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. But 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 five 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 take downs of financial fraud botnets. Last year law enforcement mounted major operations 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 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.

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

Senator Cornyn. Thank you, Mr. Chairman. Well, it seems like it is the wild, wild west all over again. But 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. But 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.

But 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. But 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? And 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. So I am obviously a little biased towards security research. So 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 for them, the barriers to entry, and so much of what I talk about around security research is really geared towards 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 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 sort of be mindful of the third party components being used and would use sort of 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. So I would recommend you look at that bill.

Senator Cornyn. My experience has been that government and technology do not mix very well. And to your point, even if the technology exists, it may not be being used.

But 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. Yeah, 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. So 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. So 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. And 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. And you have a lot of clients who you do that with; correct?

Ms. Ellis. Absolutely. But there is also --

Senator Whitehouse. A more freelance mode?

Ms. Ellis. Yeah. And that research can actually be either intentional or accidental; right? It can be accidental discovery such as the five-year-old boy who was trying to get into his dad's X-box 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. And 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. And 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. Yeah, absolutely. So 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. And it is a crime that can

literally occur at the speed of light.

Mr. Wright. Correct. And we are dependent on at least on the law enforcement information sharing on laws that were written in the 18 or 1700s. We need to have that MLAT process streamlined so that 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. And finally, why do you support aggravated penalties for attacks on critical infrastructure?

Mr. Wright. Well, 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.

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

Senator Graham. Well, thank you. You would be and you corrected that problem. I want everybody in the world

to wish me a happy birthday.

Mr. Johnson. Secondly, 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.

And 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.

Senator 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. Well, 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 ten 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.

Senator 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.

Senator Graham. Thank you.

Mr. Wright. Happy birthday to you.

Senator Graham. Welcome to the party. Thank you very

much.

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.

So 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. But 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.

Senator 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.

But 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.

Senator Graham. Well, 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. Yeah. 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.

So 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.

Senator Graham. Well, 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.

But 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.

So thank you all very much and the hearing is adjourned. We will leave it open for any comments for a

week. I apologize. Now the hearing is adjourned and happy birthday to me.

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

I N D E X