U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 18, 2015

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find the corrected transcript of the testimony of Mr. David Bitkower, Deputy Assistant Attorney General, Criminal Division, Department of Justice, at the hearing held before the Committee on July 8, 2015, entitled "Cyber Crime: Modernizing our Legal Framework for the Information Age."

Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Peter J. Kadzik
Assistant Attorney General

Enclosure

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510–6275

KOLAN L. DAVIS, *Chief Counsel and Staff Director*
KRISTINE J. LUCIUS, *Democratic Chief Counsel and Staff Director*

August 25, 2015

Deputy Assistant Attorney General
U.S. Department of Justice
Criminal Division
Computer Crime and Intellectual Property Section
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Deputy Asistant Attorney General Bitkower:

Thank you for your testimony at the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism hearing entitled "Cyber Crime: Modernizing our Legal Framework for the Information Age" on July 8, 2015. I appreciated you taking the time to appear before the Committee.

I have enclosed a copy of the unedited hearing transcript for you to review and make grammatical changes to your testimony, if needed. This is not the official hearing transcript and should not be copied or distributed under any circumstance.

Please mark any changes you may have directly on the transcript, flag the pages and return it to my office, to the attention of Jason Covey, Hearing Clerk, Senate Judiciary Committee, 224 Dirksen Senate Office Building, Washington, D.C., 20510 or by email to Jason_Covey@judiciary-rep.senate.gov. In order to complete the hearing record, please return this transcript with your changes as soon as possible and in no event later than **September 22, 2015.**

Again, thank you for your participation. If you have any questions, please contact Jason Covey at (202) 224-5225.

Sincerely,

Chuck Grassley

Charles E. Grassley
Chairman

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 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 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 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. 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 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 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, 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

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

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 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

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 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 would 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 and 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 access 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.