NEAL R. GROSS & CO., INC.

RPTS MORRISON

HIF110020

DECIPHERING THE DEBATE OVER ENCRYPTION:

INDUSTRY AND LAW ENFORCEMENT PERSPECTIVES

TUESDAY, APRIL 19, 2016

House of Representatives,

Subcommittee on Oversight and Investigations,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2123, Rayburn House Office Building, Hon. Tim Murphy [chairman of the subcommittee] presiding.

Present: Representatives Murphy, McKinley, Burgess, Blackburn, Griffith, Bucshon, Brooks, Mullin, Hudson, Cramer, Upton (ex officio), DeGette, Tonko, Yarmuth, Clarke, Kennedy, Welch, and Pallone (ex officio).

Also Present: Representatives McNerney and Eshoo.

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

Staff Present: Rebecca Card, Assistant Press Secretary; Paige Decker, Executive Assistant; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Giulia Giannangeli, Legislative Clerk, Commerce, Manufacturing, and Trade; Jay Gulshen, Staff Assistant; Charles Ingebretson, Chief Counsel, Oversight and Investigations; John Ohly, Professional Staff, Oversight and Investigations; Tim Pataki, Professional Staff Member; David Redl, Chief Counsel, Telecom; Dan Schneider, Press Secretary; Dylan Vorbach, Deputy Press Secretary; Gregory Watson, Legislative Clerk, Communications and Technology; Ryan Gottschall, Minority GAO Detailee; Tiffany Guarascio, Minority Deputy Staff Director and Chief Health Advisor; Chris Knauer, Minority Oversight Staff Director; Una Lee, Minority Chief Oversight Counsel; Elizabeth Letter, Minority Professional Staff Member; Tim Robinson, Minority Chief Counsel; Matt Schumacher, Minority Press Assistant; Ryan Skukowski, Minority Policy Analyst; and Andrew Souvall, Minority Director of Communications, Outreach and Member Services.

Mr. Murphy. Good morning, and welcome to the Oversight and Investigations Subcommittee hearing on "Deciphering the Debate over Encryption: Industry and Law Enforcement Perspectives.@

Before I start with my statement, I want to let our witnesses and other people know we have multiple hearings going on today, and tomorrow, we have a hearing as well, so you will see people coming and going. So especially for our witnesses so you don't think that that is chaos, we have members trying to juggle a lot of things at the same time.

Ms. DeGette. It is chaos.

Mr. Murphy. It is chaos, okay. I stand corrected.

We are meeting today to consider the deceptively complex question: Should the government have the ability to lawfully access encrypted technology and communications? This is the question at the center of a heated public debate, catalyzed earlier this year when the FBI obtained a court order to compel Apple to assist in unlocking an iPhone used by one of the San Bernardino terrorists.

But this isn't a new question. Strong encryption has existed for decades. For years, motivated individuals have had access to the tools necessary to conceal their activities from law enforcement. And for years, the government has repeatedly tried to limit the use of or obtain access to encrypted data.

The most notable example occurred in the 1990s when the development of encrypted communications equipment sparked fears that the government would lose its ability to conduct lawful surveillance. In response, the NSA developed a new encryption chip called the Clipper Chip that would enable encrypted communications, but would also provide the government with a key to access those communications, if necessary. This so-called back door sparked intense debate between the government and the technology community about the benefits and risks of government access to encrypted technology.

One of the principal arguments of the technology community was that such a back door would create a vulnerability that could be exploited by actors outside of the government. This concern was validated when a critical flaw was discovered in the chip's design. I should note that one of our witnesses here today, Dr. Matt Blaze, identified that vulnerability, which made the government's back door more akin to a front door.

As a partial solution, Congress passed the Communications Assistance for Law Enforcement Act, called CALEA. CALEA addressed the government's concern that rapidly evolving technologies were curtailing their ability to conduct lawful surveillance by requiring telecommunications providers to provide assistance in executing authorized surveillance.

However, the law included notable caveats which limited the government's response to encrypted technologies. After the government relaxed export controls on encryption in 2000, the Crypto Wars entered a period of relative quiet.

So what has changed in recent years to renew the debate? Part of the concern is, once again, the rapid expansion of technology. At its core, however, this debate is about the widespread availability of encryption, by default. While encryption has existed for decades, until recently, it was complex, cumbersome, and hard to use. It took effort and sophistication to employ its benefits, either for good or evil. But because of this, law enforcement was still able to gain access to the majority of the digital evidence they discovered in their investigations. But now, the encryption of electronic data is the norm. It's the default. This is a natural response to escalating concerns both from government and consumers about the security of digital information.

The decision by companies like Apple and the messaging application WhatsApp to provide default encryption means more than a billion people, including some living in countries with repressive governments, have the benefit of easy, reliable encryption. At the same time, however, criminals and terrorists have the same access to secure means of communication, and they

know it, and they will use it as their own mission control center.

And that is the crux of the recent debate. Access to secure technologies beyond the reach of law enforcement no longer requires coordination or sophistication. It is available to anyone and to everyone. At the same time, however, as more of our lives become dependent on the internet and information technologies, the availability of widespread encryption is critical to our personal, economic, and national security.

Therefore, while many of the arguments in the current debate may echo those of decades past, the circumstances have changed and so, too, must the discussion. This can no longer be a battle between two sides or a choice between black and white. If we take that approach, the only outcome is that we all lose. This is a core issue of public safety and ethics, and it requires a very thoughtful approach.

That is why we are today, to begin moving the conversation from Apple versus the FBI or right versus wrong to a constructive dialogue that recognizes this is a complex issue that affects everyone and therefore we are in this together.

We have two very strong panels, and I expect each will make strong arguments about the benefits of strong encryption and the challenges it presents for law enforcement. I encourage my colleagues to embrace this opportunity to learn from these experts

to better understand the multiple perspectives, layers, and complexities of the issues.

It is time to begin a new chapter in this battle, one which I hope can ultimately bring some resolution to the war. This process will not be easy, but if it does not happen now, we may reach a time when it is too late and success becomes impossible.

So, for everyone calling on Congress to address this issue, here we are. I can only hope, moving forward, you will be willing to join us at the table.

I now recognize the ranking member from Colorado, Ms. DeGette, for 5 minutes.

Ms. DeGette. Thank you, Mr. Chairman. And thank you for holding this important hearing.

Issues surrounding encryption and particularly the disagreements between law enforcement and the tech community gained significant public attention in the San Bernardino case, but I am not particularly interested in re-litigating that dispute today. As you said, Mr. Chairman, the conversation needs to be broader than just that one case.

Let me state unequivocally that I, like you, and I think the rest of us here today recognize and appreciate the benefits of strong encryption in today's digital world. It keeps our communications secure, our critical infrastructure safe, and our

bank accounts from being drained. It also provides each one of us with significant privacy protections.

But also, like you, I see the flip side of the coin. While encryption does provide these invaluable protections, it can also be used to obscure the communications and plots of criminals and terrorists and increasingly at great risk. It is our task to help find the proper balance between those competing interests.

We need to ask both industry and law enforcement some hard questions today. Last month, the President said, for example, "We want strong encryption because part of us preventing terrorism or preventing people from disrupting the financial system is that hackers, state or non-state, can't get in there and mess around.@ But if we make systems that are impenetrable or warrant-proof, how do we stop criminals and terrorists? If you can't crack these systems, President Obama said, "then everybody is walking around with a Swiss bank account in their pocket.@

I have heard the tech community's concern that some of the policies being proposed like creating a back door for law enforcement will undermine the encryption that everybody needs to keep them safe. And, as they remind us, a back door for good guys ultimately becomes a front door for criminals.

The tech community has been particularly vocal about the negative consequences of proposals to address the encryption

challenge. I think many of these arguments are valid, but I have only heard what we should not do, not what we should do collectively to address this challenge. I think the discussion needs to include a dialogue about how to move forward. I can't believe that this problem is intractable.

Now, the same thing seems to be true from where I sit for law enforcement, which raises legitimate concerns but doesn't seem to be focused on workable solutions. I don't promote forcing industry to build back doors or other circumventions that experts will tell us will undermine security or privacy for all of us. At the same time, I am not comfortable with impenetrable warrant-proof spaces where criminals or terrorists can operate without any fear that law enforcement could discover their plots.

So what I want to hear today is from both law enforcement and industry about possible solutions going forward. For example, if we conclude that expansive warrant-proof spaces are not acceptable in society, then what are the policy options? What happens if encryption is the reason law enforcement can't solve or prevent a crime? If the holder or transmitter of the data or device can't or won't help law enforcement, what then? What are suitable options?

Last week, for example, the Washington Post reported that the government relied on gray-hat hackers to circumvent the San

Bernardino iPhone. Well, thank goodness? I don't think so. I don't think relying on a third party is a good model. This recent San Bernardino case suggests that when the government needs to enhance its capabilities when it comes to exploring ways to work around the challenges posed by encryption. I intend to ask both panels what additional resources and capabilities the government needs to keep pace with technology.

While providing government with more tools or capability require additional discussions regarding due process and the protection of civil liberties, enhancing the government's technical capability is one potential solution that does not mandate back doors.

Finally, the public, the tech community, and the government are all in this together. In that spirit, I really do want to thank our witnesses for coming today. I am happy that we have people from law enforcement, academia, and industry, and I am really happy that Apple came to testify today. Your voice is particularly important because other players like Facebook and WhatsApp declined our invitation to be a part of this panel.

Now, the tech community has told Congress we need to solve this problem, and we agree, but I have got to tell you, it is hard to solve a problem when the key players won't show up for the discussion. And I am here also to tell you, as a longtime member

of this subcommittee, relying on Congres to, on its own, pass legislation in a very complex situation like this is a blunt instrument at best. I think it would be in everybody's best interest to come to the table and help us work on a solution.

Thanks again for holding this hearing. I know we won't trivialize these concerns. I look forward to working with everybody to come up with a reasonable solution, and I yield back.

Mr. Murphy. The gentlelady yields back.

I now recognize the chairman of the full committee, Mr. Upton, for 5 minutes.

The Chairman. Thank you, Mr. Chairman.

For months now, we have witnessed an intense and important debate between law enforcement and the technology community about encryption. While much of this recent debate has focused on the FBI and Apple, this issue is certainly much bigger than any one entity, device, application, or piece of technology. At its very core, this is a debate about what we, as a society, are willing to accept.

If you have paid any attention to the debate, it might appear to be a black-and-white choice. Either we side with law enforcement and grant them access to encrypted technologies, thus weakening the security and privacy of our digital infrastructure, or we can side with the technology community and prevent law

enforcement from accessing encrypted technologies, thus creating a warrantless safe haven for terrorists, pedophiles, and other evil and terrible actors.

It is important that we move beyond the us-versus-them mentality that has encompassed this discussion for too long. This debate is not about picking sides; it is about evaluating options. It begins by acknowledging the equities on both sides. From the technology perspective, there is no doubt that strong encryption is a benefit to our society. As more of our daily lives become integrated with the digital universe, encryption is critical to the security and privacy of our personal and corporate secrets. As evidenced by the breaches over the past year, data theft can have a devastating effect on our personal privacy, economic strength, and national security.

In addition, encryption doesn't just enable terrorists and wrongdoers to do terrible things. It also provides a safe haven for dissidents, victims of domestic violence, and others who wish to remain hidden for noble purposes. And as we look to the future and see that more and more aspects of our lives will become connected to the internet, including things such as cars, medical devices, and the electric grid, encryption will play an important role in minimizing the risk of physical harm or loss of life should these technologies be compromised.

From the law enforcement perspective, while strong encryption helps protect the information and lives, it also presents a serious risk to public safety. As strong, inaccessible encryption becomes the norm, law enforcement loses access to valuable tools and evidence necessary to stop bad actors from doing terrible things. And as we will hear today, this cannot always be offset by alternative means such as metadata or other investigative tools. There are certain situations, such as identifying the victims of child exploitation, not just the perpetrators, where access to content is critical.

These are but a few of the many valid concerns on both sides of this debate, which leads us to the question: What is the answer? Sitting here today, I don't have the answer, nor do I expect that we will find it during this hearing. This is a complex issue, and it is going to require a lot of difficult conversations, but that is not an excuse to put our head in the sand or resort to default positions. We need to confront these issues head-on because they are not going to go away, and they are only going to get more difficult as time continues to tick.

Identifying a solution to this problem may involve tradeoffs and compromise on both sides, but ultimately, it comes down to what society accepts as the appropriate balance between government access to encryption and security of encrypted

technologies. For that reason and others, many have called on us, us, this committee, confront the issues here.

That is why we are holding this hearing, and that is why Chairman Goodlatte and I, along with Ranking Members Pallone and Conyers, established a bipartisan, joint committee-working group to examine this very issue. In order for Congress to successfully confront the issue, however, it will require patience, creativity, courage, and more importantly, cooperation. It is easy to call on Congress to take on an issue, but you better be prepared to answer the call when we do. This issue is too important to have key players sitting on the sidelines, and therefore, I hope all of you are prepared to participate as we take to heart what we hear today and be part of the solution moving forward.

And I yield back.

Mr. Murphy. The gentleman yields back.

I now recognize Mr. Pallone for 5 minutes.

Mr. Pallone. Thank you, Mr. Chairman.

I welcome the opportunity to hear today from both law enforcement and the tech community as we seek to understand and develop solutions to this encryption debate. Encryption enables the privacy and security that we value, but it also creates challenges for those seeking to protect us.

Law enforcement has a difficult job of keeping our nation safe, and they are finding that some encrypted devices and programs are hampering their efforts to conduct thorough investigations. Even when they obtain a warrant, they find themselves unable to access information protected by end-to-end encryption. And this raises questions of how comfortable we are as a nation with these "dark@ areas that cannot be reached by law enforcement.

At the same time, the tech community helps protect some of our most valuable information, and the most secure way to do that is by using end-to-end encryption, meaning the device or app manufacturer does not hold the key to that information. When the tech community tells us that providing back doors will make their job of protecting our information that much more difficult, we should heed that warning and work towards a solution that will not solve one problem by creating many others.

It is clear that both sides in this discussion have compelling arguments, but simply repeating those arguments is not a sufficient response. We need to work together to move forward, and I hope today's hearing is just the beginning of that conversation.

In the last several months and years, we have seen major players in this debate look to Congress for solutions. In 2014,

FBI Director Comey said, "I am happy to work with Congress, with our partners in the private sector, and with my law enforcement and national security counterparts, and with the people we serve, to find the right answer, to find the balance we need.@

In an email to Apple employees earlier this year, Apple CEO Tim Cook wrote about his support for Congress to bring together "experts on intelligence, technology, and civil liberties to discuss the implications for law enforcement, national security, privacy, and personal freedoms.@ And he wrote that "Apple would gladly participate in such an effort.@

So if we have any hope of moving this debate forward, we need all parties to come to the table. The participation of our witnesses today should serve as a model to others who have been reluctant to participate in this discussion. We can't move forward if each party remains in its corner, unwilling to compromise or propose solutions. Both sides need to recognize that this is an effort to strike a balance between the security and privacy of personal data and public safety.

The public needs to feel confident that their information is secure, but at the same time, we need to assure them that law enforcement has all the tools it needs to do their jobs effectively.

So, Mr. Chairman, I would like to yield the remaining time

to the gentlewoman from New York, Ms. Clarke.

Ms. Clarke. I thank Ranking Member Pallone for yielding.

First, let me welcome Chief Thomas Galati, who is the chief of Intelligence for my hometown of New York City. And many refer to the New York City Police Department as New York's finest, but I would like to think of them as the world's finest.

Welcome, Chief Galati.

At its core, our Constitution is about the balance of power. It is about balancing power among the Federal Government, State government, and the rights of individuals. Through the years, getting that balance just right has been challenging and at times tension-filled, but we have done it. We have prevailed.

The encryption-versus-privacy-rights issue is simply another opportunity for us to again recalibrate and fine-tune the balance in our democracy. And as the old cliche states, democracy is not a spectator sport. So it is time for all of us to participate. It is time to roll up our sleeves and work together to resolve this issue as an imperative because it is not going away.

So I am glad that we are having this hearing today because I do believe that, working together, we can find a way to balance our concerns and to address this issue of physical security with our rights to private security.

So I look forward to hearing the perspectives of our witnesses today, and I yield back the remainder of the time. Thank you, Mr. Chairman.

Mr. Murphy. So your side yields back then? Thank you.

I just do ask unanimous consent that the members' written opening statements be introduced into the record. Without objection, the documents will be entered into the record.

[The information follows:]

**********COMMITTEE INSERT 1**********

Mr. Murphy. And now, I would like to introduce the witnesses of our first panel for today's hearing. Our first witness on the panel is Ms. Amy Hess. Ms. Hess is the executive assistant director for Science and Technology at the Federal Bureau of Investigations. In this role she is responsible for the executive oversight of the Criminal Justice Information Services Laboratory and Operational Technology divisions. Ms. Hess has logged time in the field as an FBI special agent, as well as the Bureau's headquarters here in Washington, D.C., and we thank Ms. Hess for preparing her testimony and look forward to hearing your insights in these matters.

We also want to welcome Chief Thomas Galati from the New York City Police Department. Chief Galati is a 32-year veteran of the New York City Police Department and currently serves as the chief of Intelligence. As chief of Intelligence, he is responsible for the activities of the Intelligence Bureau, the Western Hemisphere's largest municipal law enforcement intelligence operation. Thank you, Chief Galati, for your testimony today, and we look forward to hearing your comments.

And finally, for the first panel, we welcome Captain Charles Cohen of the Indiana State Police. Currently, he is the commander of the Office of Intelligence and Investigative Technologies where he is responsible for the Cyber Crime, Electronic

Surveillance, and Internet Crimes Against Children. We appreciate his time today, and once again thank all the witnesses for being here.

I also want to note that Sheriff Ron Hickman of the Harris County Sheriff's Office unfortunately will not be joining us today due to the tragic flooding yesterday in the Houston area. Our prayers and thoughts are with the people of Houston. We know there have been several tragedies there. We all wish Sheriff Hickman could be with us, but we certainly understand travel logistics can sometimes make these things impossible.

I would ask unanimous consent, however, that Sheriff Hickman's testimony be entered into the record, and without objection, his testimony will be entered into the record.

[The prepared statement of Ron Hickman follows:]

**********INSERT 2**********

Mr. Murphy. Now, to our panelists, as you are aware, the committee is holding an investigative hearing, and when doing so, has the practice of taking testimony under oath. Do any of you have any objections to taking testimony under oath?

They all say no.

The chair then advises you that under the rules of the House and rules of the committee, you are entitled to be advised by counsel. Do any of you desire to be advised by counsel during the hearing today?

And all say no as well.

In that case, would you please rise, raise your right hand. I will swear you in.

[Witnesses sworn.]

Mr. Murphy. Thank you. You may be seated. And all the witnesses answered in the affirmative and you are now under oath and subject to the penalties set forth in title 18, section 1001 of the United States Code. You may now give a 5-minute summary of your opening statement.

Ms. Hess, you are recognized for 5 minutes.

STATEMENTS OF AMY HESS, EXECUTIVE ASSISTANT DIRECTOR FOR SCIENCE AND TECHNOLOGY, FEDERAL BUREAU OF INVESTIGATIONS; THOMAS P. GALATI, CHIEF, INTELLIGENCE BUREAU, NEW YORK CITY POLICE DEPARTMENT; AND CHARLES COHEN, COMMANDER, OFFICE OF INTELLIGENCE AND INVESTIGATIVE TECHNOLOGIES, INDIANA STATE POLICE

STATEMENT OF AMY HESS

Ms. Hess. Thank you. Good morning, Chairman Murphy, Ranking Member DeGette, and members --

Mr. Murphy. Just make sure your microphone is pulled as close to you as possible and turned on.

Ms. Hess. Yes, sir.

Mr. Murphy. Thank you.

Ms. Hess. -- and members of the subcommittee. Thank you for the opportunity to appear before you today and engage in this important discussion.

In recent years, we've seen new technologies transform our society, most notably by enabling digital communications and facilitating e-commerce. It is essential that we protect these communications to promote free expression, secure commerce and trade, and safeguard sensitive information.

We support strong encryption, but we've seen how criminals, including terrorists, are using advances in technology to their

advantage. Encryption is not the only challenge we face in today's technological landscape, however. We face significant obstacles in lawfully tracking suspects because they can seamlessly communicate while changing from a known Wi-Fi service to a cellular connection to a Wi-Fi hotspot. They can move from one communication application to another and carry the same conversation or multiple conversations simultaneously.

Communication companies do not have standard data retention policies or guidelines, and without historical data, it's very difficult to put pieces of the investigative puzzle together. Some foreign communication providers have millions of users in the United States but no point of presence here, making it difficult if not impossible to execute a lawful court order. We encounter platforms that render suspects virtually anonymous on the internet, and if we cannot attribute communications and actions to a specific individual, critical leads and evidence may be lost. The problem is exponentially increased when we face one or more of these challenges on top of another.

Since our nation's inception, we've had a reasonable expectation of privacy. This means that only with probable cause and a court order can law enforcement listen to an individual's private conversations or enter their private spaces. When changes in technology hinder or prohibit our ability to use

authorized investigative tools and follow critical leads, we may not be able to root out child predators hiding in the shadows or violent criminals targeting our neighborhoods. We may not be able to identify and stop terrorists who are using today's communication platforms to plan and execute attacks in our country.

So we are in this quandary trying to maximize security as we move into a world where, increasingly, information is beyond the reach of judicial authority and trying to maximize privacy in this era of rapid technological advancement. Finding the right balance is a complex endeavor, and it should not be left solely to corporations or to the FBI to solve. It must be publicly debated and deliberated. The American people should decide how we want to govern ourselves in today's world.

It's law enforcement's responsibility to inform the American people that the investigative tools we have successfully used in the past are increasingly becoming less effective. The discussion so far has been highly charged at times because people are passionate about privacy and security. But this is an essential discussion which must include a productive, meaningful, and rational dialogue on how encryption, as currently implemented, poses significant barriers to law enforcement's ability to do its job.

As this discussion continues, we're fully committed to working with industry, academia, and other parties to develop the right solution. We have an obligation to ensure everyone understands the public safety and national security risks that result from the use of new technologies and encrypted platforms by malicious actors.

To be clear, we're not asking to expand the government's surveillance authority, but rather to ensure we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided us to keep America safe. There is not and will not be a one-size-fits-all solution to address the variety of challenges we face. The FBI is pursuing multiple avenues to overcome these challenges, but we realize we cannot overcome them on our own.

Mr. Chairman, we believe the issues posed by this growing problem are grave and extremely complex. We must therefore continue the public discourse on how best to ensure that privacy and security can coexist and reinforce each other, and this hearing today is a vital part of that process.

Thank you again for your time and your attention to this important matter.

[The prepared statement of Amy Hess follows:]

1 **********INSERT 3**********

Mr. Murphy. Thank you, Ms. Hess.

I now recognize Chief Galati for 5 minutes.

STATEMENT OF THOMAS P. GALATI

Chief Galati. Thank you.

Mr. Murphy. Make sure your microphone is turned on, and again, pull it as close to you as you can.

Chief Galati. Thank you. On behalf of Mayor de Blasio and Police Commissioner Bratton and myself, thanks to the committee for the opportunity to speak with you this morning.

Years ago, criminals and their accomplices stored their information in closets, drawers, safes, and glove boxes. There was and continues to be an expectation of privacy in these areas, but the high burden imposed by the Fourth Amendment, which requires a lawful search be warranted and authorized by a neutral judge, has been deemed sufficient protection against unreasonable government search and seizure for the past 224 years.

But now it seems that that legal authority is struggling to catch up with the times because today, nearly everyone lives their life on a smartphone, including criminals, so evidence that once would have been stored in a file cabinet or a notebook is now archived in an email or a text message. The same exact information that would solve a murder, catch a rapist, or prevent a mass shooting is now stored in that device.

But where law enforcement has legal access to the file

cabinet, it is shut out of the phone, not because of constraints built into the law, but rather limits imposed by technology. When law enforcement is unable to access evidence necessary to the investigation, prosecution, and prevention of a crime, despite the lawful right to do so, we call this "going dark.@

Every day, we deal with this evidentiary dilemma on two fronts. First, it's what is known as "data at rest.@ This is when the actual deviceC-the computer, the tablet, or the phoneC-is in law enforcement's possession, but the information stored within it is inaccessible. In just the 6-month period from October of 2015 through March of this year, New York City, we have been locked out of 67 Apple devices lawfully seized pursuant to the investigation of 44 violent crimes. In addition, there are 35 non-Apple devices. Of these Apple devices, these incidents include 23 felonies, 10 homicides, two rapes, and two police officers shot in the line of duty. They include robberies, criminal weapons possession, criminal sex acts, and felony assaults.

In every case, we have the file cabinet so to speak, and the legal authority to open it, but we lack the technical ability to do so because encryption protects its contents. But in every case, these crimes deserve our protection, too.

The second type of "going dark@ is an incident known as "data

in motion.@ In these cases, law enforcement is legally permitted, through a warrant or other judicial process, to intercept and access a suspect's communications. But the encryption built in to the applications such as WhatsApp, Telegram, or Wickr, and others thwarts this type of lawful surveillance.

So we may know a criminal group is communicating, but we are unable to understand why. In the past, a phone or a wiretap, again, legally obtained from a judge, would alert the police to drop-off locations, hideouts, and target locations. Now, we are literally in the dark, and criminals know it, too.

We recently heard a defendant in a serious felony case make a call from Rikers Island where he extolled the Apple iOS 8 and its encryption software as "a gift from God.@ This leaves the police, prosecutors, and the people we are sworn to protect in a very precarious position.

What is even more alarming is that the position is not dictated by our elected officials, our judiciary system, or our laws. Instead, it is created and controlled by corporations like Apple and Google, who have taken it upon themselves to decide who can access critical information in criminal investigations.

As a bureau chief in our nation's largest municipal police department, an agency that's charged with protecting 8.5 million

residents and millions of daily commuters and tourists every day, I am confident that corporate CEOs do not hold themselves to the same public safety standards as our elected officials and law-enforcement professionals.

So how do we keep people safe? The answer cannot be warrant-proof encryption, which creates a landscape of criminal information outside the reach of search warrants or a subpoena and outside legal authority to establish over centuries of jurisprudence.

But this has not always been Apple's answer. Until 19 months ago, they held the key that could override protections and open phones. Apple used this master key to comply with court orders in kidnappings, murders, and terrorism cases. There was no documented incident or code getting out to hackers or the government. If they were able to comply with constitutionally legal court orders then, why not now?

The ramifications to this fight extends far beyond San Bernardino, California, and the 14 people murdered there. It is important to recognize that more than 90 percent of criminals -- of all criminal prosecutions in our country are handled at the State or local level. These cases involve real people, families, your friends, your loved ones. They deserve police departments that are able to do everything within the law to bring them

justice, and they deserve corporations to appreciate their ethical responsibilities.

I applaud you for holding this hearing today. It is critical that we work together and across silos to fight crime and disorder because criminals are not bound by jurisdictional boundaries or industry standards. But increasingly, they are aware of the safety net that the warrant-proof encryption provides them, and we must all take responsibility for what that means.

For the New York City Police Department, it means investing more in people's lives in -- than in quarterly earnings reports and putting public safety back into the hands of the brave men and women who have sworn to defend it.

Thank you, and I will take any questions.

[The prepared statement of Thomas P. Galati follows:]

**********INSERT 4**********

Mr. Murphy. Thank you very much, Chief.

Now, Captain Cohen, you are recognized for 5 minutes. Again, pull the microphone close to you.

STATEMENT OF CHARLES COHEN

Mr. Cohen. Mr. Chairman, members of the subcommittee, thank you for allowing me to testify. My name is Chuck Cohen, and I'm a captain with the Indiana State Police. I also serve as Indiana Internet Crimes Against Children Task Force commander.

I would not be here today if it were not for encountering serious problems associated with encryption that do not have easy technological fixes. We need your help, and it is increasingly apparent that that help must be legislative.

As far as I know, the FBI is not exaggerating or trying to mislead anyone when they say that there is currently no way to recover data from newer iPhones. Apple has intentionally designed an operating system and device combination that functionally acts as a locked container without a key. The sensitivity of the personal information people keep stored in their phones should be compared with the sensitivity of information that people keep in bank deposit boxes and bedrooms. Criminal investigators with proper legal authorization have the technical means to access both deposit boxes and bedrooms, but we lack the technical means to access newer cellular phones running default hard encryption.

We are often asked for examples of how encryption hinders

law enforcement's ability to conduct criminal investigations. There are numerous encrypted phones sitting in the Indiana State Police evidence rooms waiting for a solution, legal or technical, to the problem. Some of those phones belong to murder victims and child sex crimes victims.

Earlier this year, a mother and son were shot to death inside their home in Indiana. Both victims had newer iPhones. I'm confident that, if they were able, both would give consent for us to forensically examine their phones to help us find the killer or killers. But unfortunately, being deceased, they were unable to give consent, and unfortunately for investigators working to solve their murders, they chose to buy phones running encrypted operating systems by default.

I need to emphasize that we are talking not just about suspects' phones but also victims' phones, and not just about incriminating evidence but also exculpatory evidence that cannot be recovered. It is always difficult to know what evidence and contraband is not being recovered, the child victims that are not being rescued, and the child sex offenders that are not being arrested as a result of encryption.

But the investigation, prosecution, and Federal conviction of Randall R. Fletcher helps to shed light on the type of evidence that is being concealed by encryption. Fletcher lived in

northern Indiana. During the course of an investigation for production and possession of child pornography, computer hard drives with encrypted partitions and an encrypted thumb drive were seized. The encryption was a bust such that it was not possible to forensically examine the encrypted data, despite numerous attempts by several law enforcement agencies.

A Federal judge compelled Fletcher to disclose the encryption key. He then provided law enforcement with a passcode that opened the encrypted partitions but not the encrypted thumb drive. In the newly opened data, law enforcement found thousands of images and videos depicting minors being caused to engage in sexually explicit conduct. To this day, investigators believe the thumb drive contains homemade child pornography produced by Fletcher but have no way of confirming or disproving that belief.

Fletcher had continuing and ongoing access to children, including a child he previously photographed in lascivious poses. Fletcher has previous convictions for conspiracy to commit murder and child sex offenses that are detailed in my written testimony.

There is good reason to believe that, because of hard encryption on the USB storage device, additional crimes committed by Fletcher cannot be investigated and prosecuted. That means additional child victims cannot be provided victim services or access to the justice that they so richly deserve.

I hope that Congress takes the time to truly understand what is at stake with the "going dark@ phenomenon and what problems have been created. There is a cost associated with an encryption scheme that allows lawful access with some theoretically higher chance of lost data, but there is a much greater and very real human cost that we already see across the country because investigations that failed -- fail due to default hard encryption.

In my daily work, I feel the impact of law enforcement going dark. For me, it is a strong feeling of frustration because it makes the detectives and forensic examiners for whom I am responsible less effective. But for crime victims and their families, it is altogether different. It is infuriating, unfair, and incomprehensible why such critical information for solving crimes should be allowed to be completely out of reach.

I have heard some say that law enforcement can solve crimes using metadata alone. That is simply not true. That is like asking a detective to process a crime scene by only looking at the street address on the outside of the house where a crime was committed. I strongly encourage committee members to contact your State investigative agency or local police department and ask about this challenge.

I greatly appreciate your invitation to share my perspective, and I'm happy to answer questions today or at any

point in the future. Thank you, Mr. Chairman, members of the committee.

[The prepared statement of Charles Cohen follows:]

**********INSERT 5**********

Mr. Murphy. I thank the panel.

I would now recognize myself 5 minutes for questions.

Ms. Hess, I think sometimes the FBI's concerns about encryption are broadly characterized as being against encryption. Considering the FBI's work on investigations like the Sony data breach or the recent ransomware attacks on hospitals, I have a tough time believing that your organization is against the technology that is so instrumental in protecting digital information. So to clarify, does the FBI agree that strong encryption is important to the security and privacy of our citizens, our economic strength, and our national security?

Ms. Hess. Yes, sir.

Mr. Murphy. And it also benefits law enforcement? Yes?

Ms. Hess. Yes.

Mr. Murphy. Can you elaborate on that?

Ms. Hess. Yes, sir. Yes. And you are correct. Is that -- as I stated in my opening statement, we do support strong encryption because it does all of the things you just said. We also recognize that we have a continuing struggle, an increasing struggle to access readable information, to access content of communications caused by that encryption that is now in place by default.

Mr. Murphy. And so it brings this question up then. Are

you witnessing an increase in individuals intentionally or even unintentionally evading the law through availability of default encryption?

Ms. Hess. I think it's difficult to discern whether or not they're intentionally doing it. However, we are significantly seeing increases in the use and deployment of decryption because it is a default setting now on most devices.

Mr. Murphy. So related to that then, Chief Galati, would you say that the default application of encryption can create significant hurdles for law enforcement? Is that the issue, as Ms. Hess was just saying, it is the default one?

Chief Galati. Yes, sir. The encryption, a lot of the apps that are being used today, even with legal process or, you know, coverage on the phone, you cannot intercept those conversations. Often, we hear criminals both in -- criminals and also in the terrorism cases that we do, people encouraging participants to go to apps like Telegram, WhatsApp, Wickr, and so on.

Mr. Murphy. You know, Captain Cohen, your testimony was very moving about those cases you described involved with murder and with victimizing children. You know, this debate is oftentimes been about picking sides, the most notable being Apple v. FBI. So either you support law enforcement or you support the tech community. That feels like a lose-lose proposition.

Look, I understand people want to be able to have encrypted technology, but based upon the responses, Captain, that you heard from Ms. Hess and from the chief, do you think this is an us-versus-them debate or are there answers that we can be going forward here? What do you think? Because you are on the frontlines dealing with these terrible cases. Is this an us-them? Is there an answer?

Mr. Cohen. Mr. Chairman, I definitely do not think it's an us-them. What we do see, though, is a challenge with default encryption that functionally cannot be turned off. I mean, I don't have the option to even disable that encryption.

The difference with Mr. Fletcher, the example I gave you, was that after two prior convictions, he then learned that he needed to do something to protect himself better from criminal investigation and then went out in search of, we assume, encryption and ways to do that.

The difference is now we are seeing increasingly, to talk to your question of Ms. Hess as well, what we're seeing now is discussion among a wide variety of criminals -- and I see it daily -- discussion among those that sexually solicit children online, sexually extort children, trade in child pornography, discussing the best possible systems to buy, the best combination of cell phone and operating system to buy to prevent encryption.

Please make no mistake that criminals are listening to this testimony and learning from it. They're learning which messaging app to use to protect themselves against encryption. They are also learning which messaging app is located outside the United States and has no bricks-and-mortar location here in the United States, which ones are located in countries with which we have a mutual legal assistance treaty and which ones we don't. Criminals are using this as an education to make themselves more effective at their criminal tradecraft.

Mr. Murphy. So given that, Ms. Hess, what answer will we have here for those cases where, whether it is a terrorist planning a plot or they have already killed some people and we are trying to find out what the next move is or it is a child predator? Will there be an answer for this?

Ms. Hess. Yes, sir. And to clarify my earlier statement, too, we do see individuals -- criminals, terrorists -- encouraging others to move to encrypted platforms, and we've seen that for some time. And the solution to that for us is no investigator, no agent will take that as an answer to say that they should stop investigating. They will try to find whatever workaround they possibly can, but those solutions may be time-intensive. They may not eventually be effective. They may require an additional amount of resources or an additional amount of skill in order to

get to those solutions.

But primarily, we are in usually a race against the clock, and that's the key component of how we're finding additional solutions around this problem.

Mr. Murphy. I know this is a frightening aspect for Americans. Look, we understand privacy, but if there is some child predator hiding in the bushes by the playground watching to snatch a victim, you can find them. But now, if this has given them this cloak of invisibility, it is pretty frightening. We better find an answer.

My time is up. I now recognize Ms. DeGette for 5 minutes.

Ms. DeGette. Thanks, Mr. Chairman.

Well, just to follow up on the chairman's questioning, the problem really isn't default encryption because if you eliminated default encryption, criminals could still get encryption, and they do, isn't that correct, Ms. Hess?

Ms. Hess. Yes, that's correct.

Ms. DeGette. Right. And so the problem is that criminals can have easy access to encryption. And I think we can stipulate that encryption is really great for people like me who have bank accounts who don't want them to be hacked, but it is just really a horrible challenge for all of us as a society, not just law enforcement, when you have a child sex predator who is trying to

encrypt, or just as bad really, a terrorist.

So what I want to know is, what are we going to do about it? And the industry says that if Congress forces them to develop tools so that law enforcement, with probable cause and a warrant, can get access to that data, that then will just open the door. Do you believe that is true, Ms. Hess?

Ms. Hess. I believe that there certainly will be always no such thing as 100 percent security. However, industry leaders today have built systems that enable us to be able to get or receive readable content.

Ms. DeGette. And, Chief Galati, what is your view on that?

Chief Galati. I believe that in order to provide -- and I don't want to call it a back door but rather a front door -- I think if the companies can provide law enforcement, I don't believe that it would be abused. We have to --

Ms. DeGette. Why not? Why not?

Chief Galati. We have the CALEA law from 1994, and that was not abused, so I don't see how by making a law -- making law enforcement --

Ms. DeGette. What they are saying is the technology -- once they develop that technology, then anybody could get access to it and they could break the encryption.

Chief Galati. I believe that if we look at Apple, they have

the technology going back to about 18, 19 months ago where they were doing it for law enforcement, and I don't -- I am not aware of any cases of abuse that came out when Apple actually did have the key. So I could see if that -- they still have the key today, then they hold it --

Ms. DeGette. I will ask them that because they are coming up.

Captain Cohen?

Mr. Cohen. I think it might be helpful to look for real-world analogies. If you think of an iPhone or an Android OS phone as a safety deposit box, the key the bank holds, that's the private key encryption. The key the customer holds, that's the public key encryption. But what the bank does is it builds firewalls around that. There's a difference between encryption and firewalls. The --

Ms. DeGette. And you think that technology exists?

Mr. Cohen. The technology does exist.

Ms. DeGette. Okay.

Mr. Cohen. So when we're --

Ms. DeGette. I am sorry. I don't have a lot of time but I am going to --

Mr. Cohen. No, go ahead. I'm sorry.

Ms. DeGette. -- ask them the same question. Now, there

is something else that can be done, forcing the industry to comply, or like in the San Bernardino case, the FBI hired a third party to help them break the code in that phone. And that was what we call gray hats, people who are sort of in this murky market. What do you think about that suggestion, Ms. Hess?

Ms. Hess. Yes, ma'am. That certainly is one potential solution, but that takes me back to my prior answer, which is that the solutions are very case-by-case specific. They may not work in all instances. They're very dependent upon the fragility of the systems or vulnerabilities we might find, and also, they're very time-intensive and resource-intensive, which may not be scalable to enable us to be successful in our investigations.

Ms. DeGette. Do you think there is any ethical issue with using these third-party hackers to do this?

Ms. Hess. I think that certainly there are vulnerabilities that we should review to make sure that we identify the risks and benefits of being able to exploit those vulnerabilities in a greater setting.

Ms. DeGette. Well, I understand you are doing it because you have to in certain cases. Do you think it is a good policy to follow?

Ms. Hess. I do not think that that should be the solution.

Ms. DeGette. And one more question is if third-party

individuals can develop these techniques to get into these encrypted devices or programs, why can't we bring more capabilities in-house to the government to be able to do that?

Ms. Hess. Certainly, these types of solutions -- and as I said, this should not be the only solution -- but these types of solutions that we do employee and can employ, they require a lot of highly skilled, specialized resources that we may not have immediately available to us. And that --

Ms. DeGette. Can we develop those with the right resources?

Ms. Hess. No, ma'am, I don't see that --

Ms. DeGette. Okay.

Ms. Hess. -- possible. I think that we really need the cooperation of industry, we need the cooperation of academia, we need the cooperation of the private sector in order to come up with solutions.

Ms. DeGette. Thank you.

Mr. Murphy. The gentlelady's time is expired.

I now recognize the gentlelady from Indiana, Mrs. Brooks, for 5 minutes.

Mrs. Brooks. Thank you, Mr. Chairman.

In 2001 after I was appointed U.S. attorney for the Southern District of Indiana, I began work with the Indiana Crimes Against Children Task Force, which was led primarily by Assistant U.S.

Attorney Steve DeBrota, working hand-in-hand with you, Captain Cohen, and I want to thank you so much for being here. Because prior to that time I would say that I was certainly not aware about what really went into and what horrific crimes really were being perpetrated against children back at that time in 2001, 2002.

And when we talk about child exploitation against children, we need to realize this involves babies up to teenagers. This is not all about just willing teenagers being involved in these types of acts. These are people preying on children of all ages.

And I want to walk you through, Captain Cohen, what some of the impediments are, more about how this works, how you are being thwarted in your investigations, and I also want to wrap up and make sure you have time for you to explain your thoughts about the firewalls.

First of all, if you could just please walk through with us, offenders -- and I am talking about older children now -- older kids who have access to social media. Offenders, perpetrators are making connections through social media platforms, correct?

Mr. Cohen. Yes, ma'am.

Mrs. Brooks. And are those typically unencrypted or encrypted?

Mr. Cohen. Two years ago, I would have said typically unencrypted; now, typically encrypted.

Mrs. Brooks. Okay. And I left my services as U.S. attorney in '07, so things, I think, have changed pretty dramatically.

Then, in the second step, the conversation moves to encrypted discussions. Would that be correct? They encourage particularly young people to go to apps like WhatsApp, Kik, and others.

Mr. Cohen. Correct. They'll generally go trolling for a potential victim in an unencrypted app. Once they have a victim they think that they can perpetrate against, then they'll move to an encrypted communication now.

Mrs. Brooks. And then would it be fair to say that, through the relationship that has been developed, they typically encourage them to send an image?

Mr. Cohen. Correct. They're going to want that offender -- that victim to do one compromising act that they can then exploit.

Mrs. Brooks. And that image is sent typically from one smartphone to another or from one smartphone to a computer?

Mr. Cohen. Generally, from one smartphone to another in the United States, involving an Android phone or an iPhone.

Mrs. Brooks. But this doesn't just happen in our country, correct?

Mr. Cohen. Correct. It's possible like never before for

someone even in another country to victimize a child here in the U.S.

Mrs. Brooks. And in fact, so we have out-of-country perpetrators, as well as in-country perpetrators focusing on even out-of-country victims as well, is that right?

Mr. Cohen. Correct, ma'am, yes.

Mrs. Brooks. Then, are those typically encrypted? The transmission of those photos is typically encrypted?

Mr. Cohen. Yes, that's one of our challenges. The transmission is encrypted, as well as when the data sits at rest on the phones. It's encrypted there as well.

Mrs. Brooks. And you presenting that image to a jury if an individual is caught and is prosecuted, it is imperative, is it not, for you to present the actual image to a jury?

Mr. Cohen. Yes, ma'am. The metadata alone, who was talking with whom, doesn't matter. It's the content of the communication. It's the images that were sent and received.

Mrs. Brooks. So if you can't get these encrypted images and the encrypted discussions, what do you have in court?

Mr. Cohen. We have nothing in court. We can't complete the investigation.

Mrs. Brooks. How do you find the victims?

Mr. Cohen. Oftentimes, we don't have a way of identifying

the victims. They go un-served.

Mrs. Brooks. And can you please talk to us a bit more about what it is that you actually do to find the victims?

Mr. Cohen. We do everything we can. We try to look for legal solutions, meaning trying to get records from service providers, from the technology companies, trying to identify them through that. The challenge we encounter there many times, as Ms. Hess mentioned, is because of retention periods. The records no longer exist. The metadata no longer exists. And then we try to get the content and communication to show who was talking with whom, and oftentimes, we're unable to do that because of encryption.

Mrs. Brooks. And isn't it pretty common that when you find one of these phones or a computer or a perpetrator, there are usually thousands of images --

Mr. Cohen. Thousands --

Mrs. Brooks. -- involving multiple victims?

Mr. Cohen. Thousands or hundreds of thousands, and increasingly, we're finding those also in encrypted cloud storage sites like Dropbox and Google Drive and OneDrive.

Mrs. Brooks. And could you please just expand a little bit on what you previously started to answer, a potential solution with respect to firewalls?

Mr. Cohen. A potential solution is to provide a better firewall. Think of that as the vault door where the safety deposit box is. Think of that as the doors to the bank. So while you think of the actual locks on the bank deposit boxes as the encryption, you build firewalls around that. Those firewalls can, with legal process, be opened up, can -- you can go inside it.

But just like a safety deposit box, if we go to the bank with a search warrant, the bank uses their key, we get a drill and we drill the customer's lock and we see what's inside the safety deposit box. I've done that dozens of times in the course of my career. The difference is, with encryption, my drill doesn't break the lock.

Mrs. Brooks. Thank you. I yield back.

Mr. Murphy. The gentlelady yields back.

I now recognize Ms. Clarke for 5 minutes.

Ms. Clarke. I thank you, Mr. Chairman, and I thank our ranking member.

In October of 2014, FBI Director Comey gave these remarks on encryption before the Brookings Institute: "We in the FBI will continue to throw every lawful tool we have at this problem, but it is costly, it is inefficient, and it takes time. We need to fix this problem. It is long past time. We need assistance and

cooperation from companies to comply with lawful court orders so that criminals around the world cannot seek safe haven for lawless conduct. We need to find common ground, and we care about the same things.@

So, Ms. Hess, I would like to ask this question of you. Other than tech companies creating back doors for law enforcement, what do you believe are some possible solutions to address the impasse between law enforcement's need to lawfully gain access to critical information and the cybersecurity benefits of strong encryption?

Ms. Hess. Yes, ma'am. And as previously stated, I really believe that certain industry leaders have created secure systems, but they are still yet able to comply with lawful orders. They're still able to access the contents to either -- of those communications to either provide some protection for their customers against malicious software or some other types of articles. In addition to that, they're able to do it perhaps for business purposes or for banking regulations, for example.

In addition to those solutions, we certainly don't stop there. We look at any possible tools we might have in our toolbox, and that might include the things we previously discussed here today, whether that be individual solutions, metadata, whether it could be an increase in physical surveillance, but each of those things comes at a cost, and all of those things are not as

responsive as being able to get the information directly from the provider.

Ms. Clarke. So do you believe that there is some common ground?

Ms. Hess. I do.

Ms. Clarke. To the other panelists, are there solutions that you can see that might solve this impasse?

Mr. Cohen. The solution that we had in place previously in which Apple, as an example, did hold a key, and as Chief Galati mentioned, that was never compromised so they could comply with the proper service of legal process. Essentially, what happened in this instance is Apple solved a problem that does not exist.

Chief Galati. I would say by Apple or other industries holding the key, it reduces at least the law enforcement having to go outside of those companies to find people that can get a solution. So, as mentioned earlier about the gray-hat hackers, you know, they're going to be out there, but if the companies are doing it, it reduces the risk, I believe.

Ms. Clarke. Very well. In the San Bernardino case, press accounts indicate that the FBI has used the services of private sector third parties to work around the encryption of the iPhone in question. This case raises important questions about whether we want law enforcement using nongovernmental third-party

entities to circumvent security features developed by private companies. So I have questions about whether this is a good model or whether a better model exists.

Ms. Hess, assuming press accounts are true and you procured the help of a third party to gain access to that iPhone, why were you apparently not able to solve this problem on your own?

Ms. Hess. For one thing, as previously discussed, technology is changing very rapidly. We live in such an advanced age of technology development, and to keep up with that, we do require the services of specialized skills that we can only get through private industry. And that partnership is critical to our success.

Ms. Clarke. So this is to the entire panel. Do you believe that the U.S. Government needs enhanced technological capabilities?

Chief Galati. I think it does. Private industry provides a lot of opportunity, so I think the best people that are out there are working for private companies and not working for the government.

Mr. Cohen. I agree with the chief. Essentially, we need the help of private industry, both the industry that makes that technology and others. We need industry to act as good corporate citizens and help us because we can't do it alone. There are over

18,000 police agencies in the United States, and while the FBI may have some technical ability internally, those other agencies do not. And as the chief mentioned, over 90 percent of all the investigations are handled at the State and local level. We need industry's help.

Ms. Clarke. Very well. I will yield back, Mr. Chairman.

Mr. Murphy. The gentlelady yields back.

I now recognize Mr. Griffith for 5 minutes.

Mr. Griffith. Well, thank you all for being here for this important discussion that we are having today.

I will tell you, we have to figure out what the balance is both from a security standpoint but also to make sure that we are fulfilling our obligations under our Constitution, which was written with real-life circumstances in mind where they said we don't want the government being able to come in and get everything.

They were aware of the situation of general warrants both in London used against John Wilkes and the Wilkesite Rebellion. And the Founding Fathers were also aware of James Otis and his fight in Massachusetts, which John Adams said sowed the seeds of the revolution when the British Government wanted to go from warehouse to warehouse looking for smuggled goods. So it is not an easy situation.

I do have this question, though. Apparently, some

researchers recently published the results of a survey of over 600 encrypted products that are available online, and basically they found that about 2/3 of them are foreign products.

So the question would be, given that so many of the encrypted products could in fact be from companies not located or headquarters within the United States of America, if we force the companies that we do have jurisdiction over to weaken the security of their products, are we doing little more than hurting American industry and then sending the really bad actors like Mr. Fletcher, who is the child pornographer, just to a different format that we don't have control over? That is one question that I would ask all three of you.

Mr. Cohen. Right now, Google and Apple act as the gatekeepers for most of those encrypted apps, meaning the app is not available on the App Store for an iOS device. If the app was not available in Google Play for an Android OS device, a customer in the United States cannot install it. So while some of the encrypted apps like Telegram are based outside the United States, U.S. companies act as gatekeepers as to whether those apps are accessible here in the United States to be used.

Mr. Griffith. Chief?

Chief Galati. I would agree exactly what the captain said. And, you know, certain apps are not available on all devices, so

if the companies that are outside the United States can't comply with the same rules and regulations of the ones that are in the United States, then they shouldn't be available on the app stores. For example, you can't get every app on a BlackBerry that you can on an Android or a Google.

Ms. Hess. Yes, sir, what you stated is correct. And I think that certainly we need to examine how other countries are viewing the same problem because they have the same challenges as we speak and are having similar deliberations as to how their law enforcement might gain access to these communications as well.

So as we move toward that, the question for us is what makes consumers want to buy American products? Is it because they are more secure? Is it because they actually cover the types of services that the consumers desire? Is it just because of personal preference? But at the same time, we need to make sure that we balance that security as well as the privacy that the consumers have come to expect.

Mr. Griffith. And I appreciate that.

Captain Cohen, I am curious. You talked about the Fletcher case and indicated that the judge ordered that he give the password to the computer, but then you didn't get access to the thumb drive. Was the judge asked to force him to do that as well or --

Mr. Cohen. The judge -- in that instance, the judge

compelled him to provide it. He said it was not encrypted; the thumb drive is not encrypted. His defense expert disagreed with him and said it was encrypted. He then provided a password and failed a stipulated polygraph as to whether he knew the password and failed to disclose it. So every indication is he intentionally chose to not give the second password for that device.

Mr. Griffith. And was he held in contempt for that?

Mr. Cohen. Not that I -- I do not believe he was.

Mr. Griffith. I mean, look, obviously, if you can get the images, you have a better chance of finding the victim, but it is true that even before encryption, there was a great difficulty in finding victims even if you found a store of photographs in a filing cabinet? It is sometimes hard to track down the victims, isn't that correct?

Mr. Cohen. It is always very difficult to find child victims.

Mr. Griffith. It is. It is just a shame.

I like the concept, the visual of you are able to drill into the safety deposit box but you can't get into the encrypted computer or telephone. Is there a product out there that would be that limited? Because one of the problems that I know Apple has had is that they don't want to have a back door to every single

phone that other folks can get a hold of and that the government could use at will, particularly governments maybe not as conscious of civil liberties as the United States. Do you know of any such a product that would give you that kind of specificity?

Mr. Cohen. Again, the specificity would be similar to what we had prior to Apple changing where the encryption key is kept, meaning that the legal process served on Apple, as an example, and Apple is the one to use the drill, not law enforcement. That helps provide another layer of protection against abuses by government other than ours, meaning while they have that capability because they're inside the firewall, those outside the firewall, outside the vault, would have no ability to get access.

Mr. Griffith. Right. I appreciate it, and I yield back, Mr. Chairman.

Mr. Murphy. The gentleman yields back.

I now recognize Mr. Welch for 5 minutes.

Mr. Welch. Thank you very much.

First of all, I want to thank each of you for the work you and your departments do. It is astonishing times when the kind of crimes that all America is exposed to are happening and the expectation on the part of the public is somehow, someway you are going to make it right and you are going to make us safe. So I think all of us really appreciate your work.

This issue, as you have acknowledged, is very, very difficult. I think if any of us were in your position, what we would want is access to any information that the Fourth Amendment allowed us to get in order for us to do our job.

But there are three issues that are really difficult. One is the law enforcement issue that you have very clearly enunciated. You have got probable cause, you go through the process of getting a warrant, you are entitled to information that is in the cabin or on the phone or in the house. Yet because of technology, we have these impediments to getting what you are legally authorized to get. I think all of us want you to be able to get the information that you rightfully can obtain.

But the second issue that makes it unique almost is that in order for you to get the information, you have to get the active participation of an innocent third party who had nothing to do with the events, but who potentially can get the information for you. That is the whole Apple case.

But it is a very complicated situation because it is not as though if you came with a warrant to my house for me to turn over information that I had, it is one thing if I just go in my drawer and give it to you. It is another thing if it is buried in the backyard and the order is that I have got to buy a backhoe or rent a backhoe and go out there and start digging around until I find

it. Normally, that would be the burden on the law enforcement agency. So that is the second issue. How much can the government require a third party, a company or an individual, to actually use their own resources to assist in getting access to the information?

And then the third issue that is really tough that Mr. Griffith was just acknowledging, we get a back door key, we trust you, but we have other governments that our companies are doing business with, and they get pressured to provide the same back door key, the key is lost, and then things happen with respect to privacy and security that you don't want to happen and that we don't want to happen. So this is a genuinely tough situation where, frankly, I am not sure there is an "easy@ balance on this.

So just a couple of questions. Ms. Hess, what would you see as the answer here? I know you want the information, but if the getting of the information requires me to hire a few people to work in the yard with the backhoe or Apple to really deploy high-cost engineers to come up with an entry key, are you saying that that is what should be required now?

Ms. Hess. Yes, sir. I think that the best solution is for us to work cooperatively with technology, with industry, and with academia to try to come up with the best possible solution. But with that, I would say that no investigative agency should forgo

that for all other solutions. They should continue to drive forward with all solutions available to them.

Mr. Welch. All right. And, Chief, I will ask you. I mean, you are on the frontline there in New York all of the time, and is it your view that the right policy now would be for you, when you have probable cause to protect us -- and, you know, we are all on the same page there -- to force a technology company, at significant effort and expense, to assist in getting access to the information?

Chief Galati. So I would say up until a couple of years ago most of the technology companies -- and they still do -- have a law enforcement liaison that we work very closely with. For example, if it's Facebook or Google, even Apple where, you know, we have, you know, the ability to go to them with legal process, and they're providing us with the --

Mr. Welch. Right.

Chief Galati. -- search warrant results --

Mr. Welch. Yes. My understanding from talking to those folks is that if it is information like that is stored in the cloud, I mean, this is a situation with San Bernardino. There was a lot of stuff that was relatively easy to retrieve, and they do provide that. They do cooperate as long as you have the warrant. They do everything they can to accommodate those lawful requests from

law enforcement. Has that been your experience?

Chief Galati. Yes. The cloud does have some issues because things can be deleted from the cloud and then never recovered. If the phone is not uploaded to the cloud, then --

Mr. Welch. Right.

Chief Galati. -- things are lost. There's a very interesting --

Mr. Welch. Would you just acknowledge this? There is a significant distinction between a company turning over information that is easily retrievable in the cloud comparable to me going in my house and opening the drawer and giving you the information you requested versus a company that has to have engineers try to somehow crack the code so that they are very energetically involved in the process of decryption. That is a difference, you would agree?

Chief Galati. Yes, it is a difference, and I believe when they create the operating system, that's where they have to make that key available so that they don't have to spend the resources to crack a code rather have a new operating system that --

Mr. Welch. Thanks. Just one last thing. By the way, thank you for --

Mr. Murphy. Out of time.

Mr. Welch. Oh, I am over. All right. I just want to say

I thought what Representative Clarke said about resources for you to let you do some of this work on your own really makes an awful lot of sense, but some of these conflicts are going to be -- frankly --

Mr. Murphy. Thank you.

Mr. Welch. -- as much as we want to say they are resolvable, they are tough to resolve. I am sorry. Thank you, Mr. Chairman.

Mr. Murphy. All right. I now recognize Mr. Mullin for 5 minutes.

Mr. Mullin. Well, as you can see that I think both sides up here in this committee, you can see we want to get to the real problem. We want to be helpful, not a hindrance. Obviously, all of us want to be safe, but we also want to make sure that we operate within the Constitution. And the technology is changing at such a pace that I know law enforcement has to do their job in staying with it because the criminals are always doing their job, too, like it or not. And if it changes, crimes change, we have to change the way we operate.

The concern is privacy obviously, and getting into that, Ms. Harris, some have argued that the expansion of connected devices through the Internet of Things with new surveillance tools and capabilities. Recently, the Berkman Center at Harvard University argues that the Internet of Things could potentially

offset the government's inability to access encrypted technology for providing new paths for surveillance and monitoring. My question is, what is your reaction to the idea that the Internet of Things presents a potential alternative to accessing encrypted devices?

Ms. Hess. Certainly, sir, I do think that the Internet of Things and associated metadata presents us with opportunity to collect information and evidence that will be helpful to us in investigations. However, those merely provide us with leads or clues, whereas the real content of the communications is what we really seek in order to prove beyond a reasonable doubt in court in order to get a conviction.

Mr. Mullin. Could you expand a little bit on the content to what is in the device --

Ms. Hess. The actual content of communication.

Mr. Mullin. -- or the conversation that happens between the devices?

Ms. Hess. What the people are saying to each other as opposed to just who's communicating or at what location they were communicating. It's critically important to law enforcement to know what they said in order to prove intent.

Mr. Mullin. Is there something that we on this panel need to be -- or, I say this panel, this committee should be looking

at to help you to be able to gain access to that? Or since it is connected, do we need take any extra steps for you to be able to access that information?

Ms. Hess. Yes. And exactly to the point of the discussion here today is that we need to work with industry and with academia in order to come up with solutions so that we can access that content or so they can access it and provide it to us.

Mr. Mullin. So is the FBI exploring the options, I am assuming?

Ms. Hess. We are, yes, sir.

Mr. Mullin. Okay. Are there challenges or concerns using the growth of connected devices that you can see going down the road? Obviously, with the technology changing rapidly today, what are some of the challenges that you are facing?

Ms. Hess. Certainly, as more and more things in today's world become connected, there's also an increasing demand for encrypting those particular services, those particular devices and capabilities, and that's well-warranted and well-merited.

But again, it presents a challenge for us. As metadata is increasingly encrypted, that presents a challenge for us as well. We need to be able to access the information, but more importantly, the content. In other words, if a suspect's toaster is connected to their car so that they know it's going to come on at a certain

time, that's helpful, but it doesn't help us to know the content of the communication when it comes to --

Mr. Mullin. Sure.

Ms. Hess. -- developing plots.

Mr. Mullin. So is there a difference between, say, the FBI, the way you have to operate, Captain Cohen, and the way that you have to operate?

Mr. Cohen. There's not much of a difference because, quite candidly, we work very well together. But you asked additional challenges, in February Apple announced that it plans to tie the same encryption key to the iCloud account. So, as an example, the content that's currently in that cloud system, iCloud, Apple has announced publicly they plan to make that encrypted and inaccessible with the service of legal process. So that's one of the challenges that you asked about that we're looking at is we're going to lose that area of content as well.

Mr. Mullin. So I just assume that everything I do online for some intended purpose is out there and people are going to be able to retrieve it. I don't assume any privacy really when it is on the internet. Could that analogy hold up true or should we be expecting a sense of privacy when it is on the internet? I mean, we put it out there.

Mr. Cohen. Sir, I believe we should all expect a sense of

privacy on the internet, a sense of privacy when we talk in a restaurant, when we talk on the telephone, landline or cellular, that privacy cannot be completely absolute. We need to have, when we serve a legal process -- a search warrant is an example -- have the ability. The Constitution protects us from unreasonable searches and seizures, not all searches and seizures. So we have our private companies without checks and balances protecting everyone against all searches.

Mr. Mullin. Chief, do you have an opinion on this?

Chief Galati. Yes. I agree also. You know, on the internet you have a right to privacy, and most of these apps and programs give you privacy settings so nobody can get at it.

I think when you get into the criminal world or the malicious criminal intent, that's when law enforcement has to have the ability to go in and see what you have on there.

Mr. Mullin. Thank you. I yield back.

Mr. Murphy. Thank you. Mr. Pallone is recognized for 5 minutes.

Mr. Pallone. Thank you, Mr. Chairman.

I never seem to be amazed to that, you know, how complex an issue this is and it requires, you know, balancing various competing values and societal goals, yet much of the public debate is focused on simplified versions of the situation. They are

painted in black and white, and there seems to be some misunderstanding that we have to either have cybersecurity or no protection online at all.

We have heard that the limitations encryption places on law enforcement access to information puts us in danger of going dark. By contrast, we have heard that law enforcement now has access to more information than ever, the so-called golden age of surveillance.

At Harvard at the Berkman Center there was a report titled "Don't Panic: Making Progress on the 'Going Dark' Debate@ that concludes, "The communications of the future will neither be eclipsed in the darkness or illuminated without shadow." And I think that is a useful framework to view the issue, not as a binary choice between total darkness or complete illumination, but rather a spectrum.

I think it is fair to say there have been and always will be areas of darkness where criminals are able to conceal information, and no matter what, law enforcement has a tough job. But the question is how much darkness is too much?

So I wanted to ask you all -- you know, this is for any of you -- about, you know, some key questions on this spectrum if you will. Where are we on the spectrum? Currently, where should we be on the spectrum? If we are not in the right place, how do

we get there?

Let me start with Ms. Hess and then whoever else wants to say something.

Ms. Hess. Yes, sir. As far as the amount of information that we can receive today, I think, yes, it is true we do receive more information today than we received in the past, but I would draw the analogy to the fact that the haystack has gotten bigger but we're still looking for the same needle.

And the challenge for us is to figure out what's important and relevant to the investigation. We're now presented with these volumes -- this volume of information. And the problem additionally with that is that what we are collecting, what we are able to see is, for example, who's communicating with who or potentially what IP addresses are communicating with each other, the location, the time, perhaps the duration, but not the content of what they were actually saying.

Mr. Pallone. Chief, did you want to add to that?

Chief Galati. I do agree that, you know, the internet has provided a lot more information to police that we can go out and we can find public records, we can find, you know, records within police departments throughout the country. So to police, the internet has made things a little bit easier. However, the encryption is taking all of those gains away, and I think the more

and more we go towards encryption, the harder it's going to be to really investigate and conduct long-term cases.

We do a lot of cases in New York about gangs, drug gangs. We call them crews. And it's very vital, all the information that we get from people on the internet that sometimes are very public out there. Now they're switching over to encrypted, and it's making those long-term cases -- or those, I guess, to call them similar to RICO cases -- very, very difficult to put together because we're in the blind.

Mr. Pallone. All right. Captain, did you want to --

Mr. Cohen. I see it where we have a lack of information that I've not seen before in my 20 years of investigations, to be able to do criminal investigations not solely by encryption but also as it interrelates to retention of information and the lack of legislation related to data retention with internet service providers similar to what there is with the banking industry, as well as our inability to serve legal process on companies that are either located out of the United States or some that store data outside the United States. I see it as all interrelated issues, which together conspire to make it more difficult than ever before for me to gather the information I need to functionally conduct a criminal investigation.

So on the spectrum that you asked about, I see it far to the

extent of we're losing the ability to access information that we need to rescue victims and solve crimes.

Mr. Pallone. Thank you. I think my second question I think to some extent you already answered, but if anybody wants to, the second question is where do you see the trend moving? Are we comfortable with where we are headed or are the technological trends such as increasing a stronger encryption leaving us with too much darkness? But you kind of answered that unless anybody wants to add to what they said.

Yes, Ms. Hess?

Ms. Hess. Yes, sir. I do see that with increasing -- increasingly, technology platforms continue to change and they continue to present challenges for us that I provided in my opening statement.

In addition to that, we try to figure out how we might be able to use what is available to us, and we are constantly challenged by that as well. For example, some companies may not know what exactly or how to provide the information we are seeking. And it's not just a matter of needing that information to enable us to see the content or enable us to see what people are saying to each other, it's also a matter of being able to figure out who we should be focusing on more quickly so that if we could get that information, we're able to target our investigations more

appropriately and be able to exonerate the innocence -- the innocent as well as identifying the guilty.

Mr. Pallone. Thank you. I am going to end with that, but I just wanted to, you know, ask obviously that you continue to engage with us to help us answer these questions, I mean, not just, you know, with what you are saying today but, you know, a constant dialogue is what we need.

Thank you, Mr. Chairman.

Mr. Murphy. Thank you. I now recognize Dr. Burgess for 5 minutes.

Mr. Burgess. Thank you. And thank you all for being here.

I just acknowledge there is another hearing going on upstairs, so if some of us seem to be toggling back and forth, that is exactly what is happening.

So, Ms. Hess, let me just ask you a couple of questions if I could. There is another subcommittee at the Energy and Commerce Committee called the Commerce, Manufacturing, and Trade Subcommittee. And we are working very closely with the Federal Trade Commission, which is under our jurisdiction, that subcommittee, on the issue of data breach notification and data security. A component of that effort has been the push for companies to strengthen data security. One of those ways perhaps could be through encryption, and the FTC will look at a company's

security protocols for handling data when it reviews whether or not the company is fulfilling its obligations, protecting its customers.

So has the FBI had any discussions with the Federal Trade Commission over whether the back doors or access points might compromise the secured data?

Ms. Hess. Yes, sir. We've engaged in a number -- a number of conversations among the interagency, with other agencies, with industry, with academia. I can get back to you as far as whether we specifically met with the Federal Trade Commission.

Mr. Burgess. That would be helpful as, again, we are actually trying to work through the concepts of more in the retail space bit of data security. Data security is data security, regardless of who is harmed in the process, and data security is national security writ large. So that would be enormously helpful.

Let me just ask you a question that is probably a little bit off-topic, but I can't help myself. One of the dark sides for encryption is if someone comes in and encrypts your stuff and you didn't want it encrypted, and then they won't give it back to you unless you fork over several thousand dollars in bit coins to them in some dark market. So what is it that the committee needs to understand about that ransomware concept that is going on

currently?

Ms. Hess. Yes, sir, ransomware is an increasing problem that we're seeing and investigating on a regular basis now. And I think that certainly to exercise good cybersecurity hygiene is important, to be able to backup systems, to have the capability to access that information is important, to be able to talk to each other about what solutions might be available, to be able to fall back to some other type of backup solutions so that you aren't beholden to any particular ransom demands.

Mr. Burgess. And of course that is critically important.

I am a physician by background. Some of the ransomware has, of course, occurred in hospitals and medical facilities. And I will just offer an editorial comment for what it is worth. I just cannot imagine going into an ICU some morning and asking to see the data on my patient and being told it has been encrypted by an outside source, we can't have it, Doctor. When you catch those people, I think the appropriate punishment is shot at sunrise, and I wouldn't put a lot of appeals between the action and the reaction.

Thank you, Mr. Chairman. I will yield back.

Mr. Murphy. I now recognize Mr. Yarmuth for 5 minutes.

Mr. Yarmuth. Thank you, Mr. Chairman.

Thanks to the witnesses for your testimony.

I find it hard to come up with any question that is going to elicit any new answers from you, and I think your testimony and the discussion that we have had today is an indication of how difficult the situation is. It sounds to me like there is a great business opportunity here somewhere, but probably you don't have the budget to pay a business what they would need to be paid to get the information that you are after, so that may not be such a good business opportunity after all.

I do want to ask one question of you, Ms. Hess. In your budget request for fiscal year '17, you request more than $38 million to deal with the going-dark issue, and your request also says that it is non-personnel. So it seems to me that personnel has to be a huge part of this effort, so could you elaborate on what your budget request involves and what you plan to do with that?

Ms. Hess. Yes, sir, at a higher level, essentially, we're looking for any possible solutions, any possible tools we might be able to throw at the problem, all the different challenges that we encounter, and whether that's giving us the ability to be better password-guessers or whether that's the ability to try to develop solutions where we might be able to perhaps exploit some type of vulnerability, or maybe that's perhaps a tool where we might be able to make better use of metadata. All of those things go into

that request so that we can try to come up with solutions to get around the problem we're currently discussing.

Mr. Yarmuth. Okay. Well, I don't know enough to ask anything else, so unless anyone else is interested in my time, I would yield back. Thank you, Mr. Chairman.

Mr. Murphy. Thank you. The gentleman yields back.

I now recognize Mr. McKinley for 5 minutes.

Mr. McKinley. Thank you, Mr. Chairman.

I have been here in Congress for 5-1/2 years now, and we have been talking about this for all 5-1/2 years. And I don't see much progress being made with it. And I hear the frustration in some of your voices, but I was hoping we were going to hear today more specifics. If you could pass the magic wand, what would it be? What is the solution? I think you started to hint towards it, but we didn't get close enough.

So one of the things I would like to try to understand is how we differentiate between privacy and national security. I don't feel that we have really come to grips with that. I don't know how many people are on both sides of that aisle. I really don't care. I am very concerned about national security as it relates to encryption.

We have had -- just this past weekend there was a very provocative TV show. Sixty Minutes came out about the hacking

into cell phones. About a year ago we all were briefed. It wasn't classified. It was where Russia hacked in and shut down the electric grid in Ukraine, the impact that could have, that a foreign government could have access to it. And just this past week at town hall meetings back in the district, twice people raised the issue about hacking into and shutting down the electric grid.

And it reminded me of some testimony that had been given to us about a year ago on the very subject when one of the presenters like yourself said that, within 4 days, a group of engineers in America or kids could shut down the grid from Boston down through -- I am trying to think; where was it -- from Boston to New York you could shut down in just 4 days. I am very concerned about that, that where we are going with this, this whole issue of encryption and protection.

So, Mr. Galati, if I could ask you the question. Just how confident are you that the adequacy of the encryption is protecting our infrastructure in your jurisdiction?

Chief Galati. Well, sir, cybersecurity and infrastructure is very complicated, and we have another whole section in the police department and in the city that monitors, works very closely with all the agencies such as Con Ed, DEP, and so on. We also work very closely with the FBI and their joint cyber task

force to monitor cyber threats --

Mr. McKinley. Okay. But my question really is, how do you feel, because everyone comes in here, and when I have gone to the power companies with -- I don't need to elicit their names, but all of them has said we think we have got it. But yet during that discussion on 60 Minutes, this hacker that was there, he is a professional hacker, he said I can break into any system, any system. So my question more, again, back to you is how confident are you that this system is going to work, that it is going to be protected?

Chief Galati. Well, I think with all the agencies that are involved in trying to protect critical infrastructure, and I think that there is a big emphasis in New York -- I'll speak about New York -- working with multiple, multiple agencies. We're looking at vulnerabilities to the system. I do think that is an encryption issue, but again, I think what I was speaking about more when it came to encryption is more about communications and investigating crimes or terrorism-related offenses.

Mr. McKinley. It is beyond your jurisdiction then on that. How about --

Chief Galati. That is not an area that I would comment.

Mr. McKinley. Okay. How about you in Indiana?

Mr. Cohen. What are you talking about? Control systems

being compromised? Again, we're talking about firewalls, not encryption. We're talking about the ability for someone to get inside the system, to have the password, to have the passphrase, something like that to get the firewall. So encryption of data in motion as an example would not protect us from the types of things you're talking about to be able to shut down a power grid.

It's noteworthy that I saw that 60 Minutes piece, and what that particular hacker was able to exploit would not have been fixed by encryption. That is a separate system related to how the cellular -- how our cell system works essentially, completely separate, unrelated from the issue of encryption. So what I can say is having more robust encryption would not fix either of those problems.

Mr. McKinley. Thank you.

Mr. Cohen. And I lack the background to be able to tell you specifically do I feel confident or not confident about how the firewalls are right now in the systems you asked about.

Mr. McKinley. Ms. Hess, boiler up, by the way. And so --

Ms. Hess. Yes --

Mr. McKinley. -- and so my question back to you is same to you. How would you respond to this?

Ms. Hess. Yes, sir. I think that, first off, I don't think there's any such thing as 100 percent secure --

Mr. McKinley. Right.

Ms. Hess. -- anything as a truly secure solution. With that said, I think that it is incumbent upon all of us to build the most secure systems possible, but at the same time, we're presenting to you today the challenge that law enforcement has to be able to get or access or be provided with the information we seek pursuant to a lawful order, a warrant that has been signed by a judge, be able to get the information we seek in order to prove or to have evidence that a crime has occurred.

Mr. Yarmuth. Thank you. I yield back my time.

Mr. Murphy. Thank you.

I now recognize Mr. Tonko for 5 minutes.

Mr. Tonko. Thank you, Mr. Chair, and thank you to our witnesses.

I am encouraged that here today we are developing dialogue which I think it is critical for us to best understand the issue from a policy perspective. And there is no denying that we are at risk with more and more threats to our national security, including cyber threats, but there is also a strong desire to maintain individual rights and opportunity to store information and understand and believe that it is protected. And sometimes those two are very difficult. There is a tender balance that needs to be struck.

And so I think, you know, first question to any of the three of you is, is there a better outcome in terms of training? Do you believe that there is better dialogue, better communication, formalized training that would help the law enforcement community if they network with these companies that develop the technology? I am concerned that we don't always have all of the information we require to do our end of the responsibility thing here. Ms. Hess?

Ms. Hess. Yes, sir. I do think that certainly in today's world we need people who have those specialized skills, who have the training, who have the tools and the resources available to them to be able to better address this challenge. But with that said, there is still no one-size-fits-all solution to this.

Mr. Tonko. Anything, Chief or Captain, that you would like to add?

Chief Galati. I would just say that, you know, we do work very closely with a lot of these companies like Google, and we do, you know, share information and also, you know, at times work on training amongst the two -- the agency and the company. So there is cooperation there, and I think that it can always get better.

Mr. Tonko. And, Ms. Hess, in this encryption debate, what specifically would you suggest the FBI is asking for, asking of

the tech community?

Ms. Hess. That when we present an order signed by an independent, neutral judge, that they are able to comply with that order and provide us with the information we are seeking in readable form.

Mr. Tonko. Okay. And also to Ms. Hess, is the FBI asking Apple and possibly other companies to create a back door that would then potentially weaken encryption?

Ms. Hess. I don't believe the FBI or law enforcement in general should be in the position of dictating to companies what the solution is. They have built those systems. They know their devices and their systems better certainly than we do and how they might be able to build some type of the most secure systems available or the most secure devices available, yet still be able to comply with orders.

Mr. Tonko. Do you believe that that type of assistance that you are requesting from tech companies would lead to any unintended consequences such as a weakened order of encryption?

Ms. Hess. I believe it's best for the tech companies to answer that question because, as they build the solutions to be able to answer these orders, they would know what those vulnerabilities are or potentially could be.

Mr. Tonko. I thank you. Another potential unintended

consequence of U.S. law enforcement gaining special access may be the message that they are sending to other nations. Other countries that seek to stifle dissent or oppose their citizens may ask for such tools as well. Right now, even if other countries start to demand such a workaround, Apple and other technology companies can legitimately argue that they do not have it.

So, Ms. Hess, how would you respond to this argument that requiring tech companies to help subvert their own encryption establishes precedence that could endanger people around the world who rely on protected communications to shield them from despotic regimes?

Ms. Hess. Yes, sir. I would say, first, that in the international community -- and we've had a number of conversations with our partners internationally -- that this is a common problem among law enforcement throughout the world. And so as we continue to see this problem, obviously, there are international implications to any solutions that might be developed. But in addition to that, what we seek is through a lawful order with the system that we've set up in this country for the American judicial system to be able to go to a magistrate or a judge to get a warrant to say that we believe -- we have probable cause to believe that someone or some entity is committing a crime.

I believe that if other countries had such a way of doing

business, that that would probably be a good thing for all of us.

Mr. Tonko. And Chief Galati or Captain Cohen, do you have anything to add to what was shared here by Ms. Hess?

Mr. Cohen. In preparing for the testimony, I saw several news stories that said that Apple provided the source code for iOS to China as an example. I don't know whether those stories are true or not. I also tried to find an example of Apple answering a question under oath and did not find that.

I noted that Apple said they could not -- did not provide a back door to China but did not talk about the source code. The source code for the operating system would be the first thing that would be needed to hack into an iPhone as an example. And I know that they have not provided that source code to U.S. law enforcement.

Mr. Tonko. Okay. Thank you. My time is exhausted, so I yield back, Mr. Chairman.

Mr. Murphy. Yield back. Thank you. Mr. Hudson, you are recognized for 5 minutes.

Mr. Hudson. Thank you, Chairman.

I would like to thank the panel for being here today. Thank you for what you do to keep us safe.

Ms. Hess, as more and more of our lives become part of the digital universe, everything from communications to medical

records, home security systems, the need for strong security becomes all that more important. At the same time, however, it naturally suggests a massive increase in our digital footprint and the amount of information about individuals that becomes available on the internet. Does this present an opportunity for law enforcement to explore new, creative ways to conduct investigations? I know we have talked a little bit about metadata, and while that may not be a good solution, but new forms of surveillance or other options that maybe we haven't discussed yet.

Ms. Hess. Yes, sir. I do believe that we should make every use of the tools that we've been authorized by Congress, the American people to use. And if that pertains to metadata or other types of information we might be able to get from new technologies, then certainly we should take advantage of that in order to accomplish our mission.

But at the same time, clearly, these things have presented challenges to us as well, as previously articulated.

Mr. Hudson. Well, have you and others in the law enforcement community engaged with the technology community or others to explore these other types of opportunities or look at potential ways to do this going forward?

Ms. Hess. Yes, sir, we're in daily contact with industry

and with academia in order to try to come up with solutions, in order to try to come up with ways that we might be able to get evidence in our investigations.

Mr. Hudson. And what have you learned from those conversations?

Ms. Hess. Clearly, technology changes on a very, very rapid pace. And sometimes, the providers or the people who build those technologies may not have built in or thought to build in a law enforcement solution, a solution so that they can readily provide us with that information even if they want to. And in other cases, perhaps it's the way they do business, that they might not want to be able to readily provide that information or they just may not be set up to do that either because of resources or just because of the proprietary way that their systems are created.

Mr. Hudson. I see. The other members of the panel, do you have any opinion on this?

Chief Galati. I would just say that as technology advances, it does create a lot of new tools for law enforcement to complete investigations. However, as those advances, as we start using them, we also see them shrinking away, you know, for -- with encryption especially, locking things that we recently were able to obtain.

Mr. Hudson. Got you. You don't have to -- okay. To all

of you, I recently read about the CEO of MSAB, a technology company in a Detroit News article. It says there is a way for government to access data stored on our phones without building a back door to encryption. His solution is to build a two-part decryption system where both the government and the manufacturer possess a unique decryption key, and then only with both keys, as well as the device in hand, could you access the encrypted data on the device.

I am not an expert on decryption so I must ask, is such a solution achievable? And secondly, have there been any discussions between you all, the law enforcement community, with the tech community or tech industry regarding a proposal like this or something similar that would allow safe access to the data without giving a key so to speak to one entity? Is that --

Mr. Cohen. To answer your question, that paradigm would work. That's very similar to that paradigm of the safety deposit box in a bank where you have two different keys. And that would work, but it would require the cooperation of industry.

Mr. Hudson. Anything to add?

Ms. Hess. What I was going to say --

Mr. Hudson. Okay.

Ms. Hess. -- yes, sir.

Mr. Hudson. Well, we will get a good chance to hear from

industry on our next panel, but I was trying to explain this to one of my staffers and I said did you see the new Star Wars movie? Well, you know, the map to find Luke, you know, BB-2 had part of it -- or BB-8 and R2-D2 had the other half so you got to put them together. They were like, oh, I get it now.

Anyway, I think it is important that law enforcement and technology work together, continue to have these discussions. So I want to thank the chairman for giving us this opportunity to do that. And I thank you all for being here.

And with that, I will yield back.

Mr. Murphy. The gentleman yields back.

I recognize the vice chair of the full committee, Mrs. Blackburn, for 5 minutes.

Mrs. Blackburn. Thank you, Mr. Chairman, and thank you to the witnesses. I am so appreciative of your time. And I am appreciative of the work product that our committee has put into this. Mr. Welch and I, with some of the members that are on the dais, have served on a privacy and data security task force for the committee looking at how we construct legislation and looking at what we ought to do when it comes to the issues of privacy and data security and going back to the law and the intent of the law.

I mean, Congress authorized wiretaps in 1934, and then in '67 you come along and there is the language, you have got Katz

v. the U.S. that citizens have a reasonable expectation of privacy. And we know that for you in law enforcement you come up upon that with this new technology that sometimes it seems there is the fight between technology and law enforcement and the balance that is necessary between that reasonable expectation and looking at your ability to do your job, which is to keep citizens safe. So I thank you for the work that you are doing in this realm.

And considering all of that, I would like to hear from each of you, and, Ms. Hess, we will start with you and just work down the panel. Do you think that at this point there is an adversarial relationship between the private sector and law enforcement? And if you advise us, what should be our framework and what should be the penalties that are put in place that will help you to get these criminals out of the virtual space and help our citizens know that their virtual "you,@ their presence online is going to be protected but that you are going to have the ability to help keep them safe? So kind of a loaded question. We have got 2 minutes and 36 seconds, so it is all yours, and we will move right down the line.

Ms. Hess. Yes, ma'am. As far as whether there is an adversarial relationship, my response is I hope not. Certainly, from our perspective in the FBI we want to work with industry, we want to work with academia. We do believe that we have the

same values. We share the same values in this country, that we want our citizens to be protected. We also very much value our privacy, and we all do.

I think, as you noted, for over 200 years we -- this country has balanced privacy and security. And these are not binary things. It shouldn't be one or the other. It should be both working cooperatively together. And how do we do that? And I don't think that's for the FBI to decide, nor do I think it's for tech companies to decide unilaterally.

Mrs. Blackburn. No, it will be for Congress to decide. We need your advice.

Chief Galati. I think that it's not an adversarial relationship either. I mean, there are so many things that we have to work with all the big tech companies, you know, Twitter, Google, Facebook, on threats that are coming in on a regular basis. So they are very cooperative and we do work with them in certain areas. This is a new area that we're going into, but right now, I would say it's not adversarial. They're actually very cooperative.

Mr. Cohen. I agree with the other two that it's not an adversarial relationship, but as you mentioned, some of these statutes that authorize wire tap, lawful interception, authorize the collection of evidence, they have not been updated recently.

And as technology at an exponential pace evolved, some of the statutes have not evolved to keep up with them. And we just lack the technical ability at this point to properly execute the laws that Congress has passed because the technology has bypassed the law.

Mrs. Blackburn. Okay. And we would appreciate hearing from you as we look at these updates. The physical space statutes are there, but we need that application to the virtual space. And this is where it would be helpful to hear from you. What is that framework? What are those penalties? What enables you to best enforce? And so if you could just submit to us. I am running out of time, but submit to us your thoughts on that. It would be helpful and we would appreciate it.

Mr. Chairman, I yield back.

Mr. Murphy. The gentlelady yields back.

I now recognize Mr. Cramer for 5 minutes.

Mr. Cramer. Thank you, Mr. Chairman, and thank all of you. It is refreshing to participate in a hearing where the people asking the questions don't know the answer until you give it to us. That is really cool.

I want to go in real specifically on the issue of breaking modern encryption by brute force as we call it, and that is the ability to apply multiple passcodes and, you know, perhaps an

unlimited number of passcodes until you break it. That is sort of the trick here, and with the iPhone specifically, there is this issue of the data destruction feature. Would removing the data destruction feature sort of be at least a partial solution to your side of the formula? In other words, you know, we are not creating the back door but we are removing one of the tools. And I am just open-minded to it and looking for your out-loud thoughts on that issue.

Ms. Hess. Yes, sir, if I may. Certainly, that is one potential solution that we do use and we should continue to use. To be able to guess the right password is something that we employ in a wide variety and number of investigations. The problem and the challenge is that sometimes those passcode lengths may get longer and longer. They may involve alphanumeric characters. They may present to us special challenges that it would take years, if ever, to actually solve that problem, regardless of what type of computing resources we might apply.

And so to that point, we ask our investigators to help us be better guessers in order to come up with information or intelligence that might be able to help us make a better guess. But that's not always possible.

Mr. Cramer. But if I might, with the "you get 10 tries and you are out@ data destruction feature that iPhone utilizes, that

makes your job all the more difficult. It would be expanding that from 10 to 20 or unlimited or is there some -- I am not looking for a magic formula, but it seems to me there could be some way to at least increase your chances.

Ms. Hess. Yes, sir, and that's one of the things that does quite clearly present to us a challenge is that usually it takes us more than 10 guesses before we get the right answer, if at all. And in addition to that, many companies have implemented services or types of procedures so that there is a time delay between guesses. So after five guesses, for example, you have to wait a minute or 15 minutes or a day in order to guess between those passcodes.

Mr. Cramer. Others?

Mr. Cohen. I don't think personally that the brute-force solution would provide a substantive solution to the problem. As Ms. Hess mentioned, oftentimes that delay is built in. iOS, as an example, went from a four-digit pin to a six-digit pin so what you're doing is increasing the number of guesses to guess it right. So if you were to, as an example, legislate that it would not wipe the data and override the data after a specific period of time, you would also have to write in that passcodes could only be of a certain complexity, a certain length --

Mr. Cramer. Sure.

Mr. Cohen. -- and that would degrade security. What is important to understand is we want security, we want hard encryption but also need a way to quickly be able to access that data because the investigations I work, oftentimes, I'm running against the clock to try to identify a child victim. And being able to brute force that --

Mr. Cramer. Sure.

Mr. Cohen. -- even a matter of days, let alone weeks or months, that's not fast enough.

Mr. Cramer. Yes. Wow. Well, thanks for your testimony and all that you do. I yield back.

Mr. Murphy. Our tradition is to allow someone outside the committee if they want to ask questions. Mr. McNerney, you are recognized for 5 minutes.

Mr. McNerney. I thank the chairman for his courtesy, and I thank the witnesses for your service to our country.

I heard at least one of you state in your opening testimony that Congress is the correct forum to make decisions on data security, and I agree with that. However, encryption and related issues are technical, they are complicated. Most Members of Congress aren't really experts in these areas. Therefore, it is appropriate that Congress authorize a panel of experts from relevant fields to review the issues and advise the Congress.

The McCaul legislation does exactly that. Do each of you agree with that approach, the McCaul legislation?

Ms. Hess. I believe we do need to work with industry and academia and all the relevant parties in order to come up with the right solution, yes, sir.

Mr. McNerney. So you would agree that that is the right approach, to convene a panel of experts in cybersecurity, in privacy, and so on?

Ms. Hess. I believe that construct, we -- I -- there are varying aspects of that construct, but yes, that premise I would agree with.

Mr. McNerney. Okay. Captain, Chief?

Chief Galati. Sir, I really couldn't comment because I haven't seen that bill.

Mr. McNerney. Okay. Basically, it would --

Chief Galati. I do agree with Ms. Hess that, you know, we need to work together. I think we need to have, you know, a panel of experts that can advise and work with Congress. I do believe that the answer is in Congress, so I do agree with the principle of it.

Mr. McNerney. Okay. Thank you. Captain?

Mr. Cohen. Whatever paradigm helps Members of Congress feel comfortable that they are properly balancing civil liberties and

security versus the ability for law enforcement to do proper investigations. Whatever paradigm serves that purpose I fully support.

Mr. McNerney. Thank you. Chief Galati and Captain Cohen, you have illuminated some of the information that has been available before in cell phones but no longer is available because of encryption and I thank you fro doing that. I was a little in the dark about that. What haven't we heard, though, about information that is now available that wasn't available in the past because of technology?

Mr. Cohen. Sir, I'm having problems thinking of an example of information that's available now that was not before. From my perspective, thinking through investigations that we previously had information for, when you combine the encryption issue along with shorter and shorter retention periods for internet service providers -- I mean, keeping their records, both metadata and data for shorter periods of time available to legal process. I mean, I can definitely find an example of an avenue that's available that was not before.

Chief Galati. Sir, I would only say I've been in the police department for 32 years, so technology really has opened up a lot of avenues for law enforcement. So I do think there is a lot of things that we are able to obtain today that we couldn't obtain

10 or 20 years ago. So -- and technology has helped law enforcement. However, the encryption issue and I think the issue that we're speaking on today is definitely eliminating a lot of those gains we've made.

Mr. McNerney. Thank you. Ms. Hess, requiring back-door or exceptional access would drive customers to overseas suppliers, and if so, we would gain nothing by requiring back-door or exceptional access. Do you agree or disagree with that?

Ms. Hess. I disagree from the sense that I think many countries are having the same conversation, the same discussion currently because law enforcement in those countries has the same challenges that we do. And so I think this will just continue to be a larger and larger issue.

So while it may temporarily drive certain people who may decide that it's too much of a risk to be able to do business here in this country, I don't think that that's the majority. I think the majority of consumers actually want good products, and those products are made here.

Mr. McNerney. Well, thank you for calling out the quality of American products. I appreciate that, especially since my neighbor here and I represent the part of California where those products are developed. But I think there is always going to be countries where products are available that would superseded

whatever requirements we make.

Also, requiring back-door access would alert potential bad actors that there are weaknesses designed into our system and motivate them to try to find those weaknesses. Do you agree with that or not?

Ms. Hess. I don't believe there's anything such as a 100 percent secure system, so I think there will always be people who are trying to find and exploit those vulnerabilities.

Mr. McNerney. But if we design weaknesses into the system and everybody knows about it, they are going to be looking for those and those are design weaknesses. I mean, I don't see how that could further security of critical infrastructure and so on. Well, I guess my time is expired, Mr. Chairman.

Mr. McKinley. [Presiding] Thank you. And the chair recognizes Congressman Bilirakis for his 5 minutes.

Mr. Bilirakis. Thank you, Mr. Chairman. I appreciate it so very much.

Ms. Hess, thanks for participating in today's much-needed hearing. I appreciate the entire panel.

We are certainly at a crossroads of technology and the law, and having you and the FBI perspective is imperative in my opinion.

I have a question about timing. The recent debate has been revived as technology companies are using strong encryption, and

you described the problem as growing. What will a hearing like this look like a year from now, 2 years from now? What do you perceive is the next evolutionary step in the encryption debate so we can attempt to get ahead of it? And as processers become faster, will the ability to encrypt keep increasing?

Ms. Hess. Yes, sir. My reaction to that is that if things don't change, then this hearing a year from now, we would be sitting here giving you examples of how we were unable to solve cases or find predators or rescue victims in increasing numbers. And that would be the challenge for us is how can we keep that from happening and how might we be able to come up with solutions working cooperatively together.

Mr. Bilirakis. Thank you. Again, next question is for the entire panel, please. What have been some successful collaboration lessons between law enforcement and software or hardware manufacturers dealing with encryption? And are there any building blocks or success stories we can build upon, or have the recent advancements in strong encryption made any previous success obsolete? For the entire panel. Who would like to go first? Ms. Hess?

Ms. Hess. Yes, sir. I apologize but could I ask you to -- I'm not 100 percent clear on that question.

Mr. Bilirakis. Okay. Let me repeat it. For the entire

panel again, what have been some successful collaboration lessons between law enforcement and software or hardware manufacturers dealing with encryption? That is the first question. Are there any building blocks or success stories we can build upon, or have the recent advancements in strong encryption made any previous success obsolete?

Ms. Hess. Yes, sir. Certainly, we deal with industry on a daily basis to try to come up with the most secure ways of being able to provide us with that information and still be responsive to our request and our orders. I think that building on our successes from the past, clearly, there are certain companies, for example, as has already been stated here today that fell under CALEA and those CALEA-covered providers have built ways to be able to respond to appropriate orders. And that's provided us with a path so that they know when they build those systems what exactly we're looking for and how we need to receive that information.

Mr. Bilirakis. Sir?

Chief Galati. I'm sorry, sir. I really couldn't comment on that. That's not really an area of expertise of mine.

Mr. Cohen. I concur with what Ms. Hess said. There are a few technology companies that have worked with law enforcement to provide a legal solution, and they've done that voluntarily. So we know the technological solution. They provide a legal

solution such that we can access data.

Mr. Bilirakis. Thank you.

Mr. Cohen. And building on those collaborations and having other industry members follow in that path would be of great help.

Mr. Bilirakis. Thank you. Next question for the panel, what percentage of all cases are jeopardized due to the suspect having an encrypted device, whether it is a cell phone, laptop, desktop, or something else? I recognize that some cases such as pornography, it may be 100 percent impossible to charge someone without decrypting their storage device, but what about the other cases where physical evidence or other evidence might be available? Does metadata fill in the gaps? And for the entire panel, let's start with Ms. Hess, please.

Ms. Hess. Yes, sir, we are increasingly seeing the issue. Currently, in just the first six months of this fiscal year starting from last October we're seeing of -- in the FBI the number of cell phones that we have seized as evidence, we're encountering passwords about 30 percent of the time, and we have no capability around 13 percent of that time. So we're seeing those numbers continue to increase, and clearly, that presents us with a challenge.

Mr. Bilirakis. Thank you.

Chief Galati. Sir, just I'll give you some numbers. We

have approximately 102 devices that we couldn't get in, and these are 67 of them being Apple devices. And if I just look at the 67 Apple devices, 10 of them are related to a homicide, two to rapes, one to a criminal sex act, and two are related to two members of the police department that were shot. So we are seeing an increase as, you know, we go forward of phones not -- you know, not getting the information out of the phones.

One thing I will say is it doesn't always prevent us from making an arrest. However, it just doesn't present all the evidence that's available for the prosecution.

Mr. Cohen. And to expand on what the chief said, that can be incriminating evidence or that can be exculpatory evidence, too, that we don't have access to. On the Indiana State Police, the sad part is when our forensic examiners get called, we ask a series of questions now of the investigator, is it an iPhone, which model? And if we're told it's a model, as an example, 5S or newer or on a 64-bit operating system and it's encrypted, we don't even take that as an item of evidence anymore because we know that there is no technical solution.

So the problem is we never know what we don't know. We don't know what evidence we're missing, whether that is again on a suspect's phone or on a victim's phone where the victim is not capable of giving us that passcode.

Mr. Bilirakis. Well, thank you very much. I appreciate it, Mr. Chairman. I yield back the time.

Mr. McKinley. And I think we have one last question for the first panel, and that is from the gentlelady from California, Ms. Eshoo.

Ms. Eshoo. Thank you very much, Mr. Chairman, for extending legislative courtesy to me to be here to join in on this hearing because I am not a member of this subcommittee. But the rules of the committee allow us to, and I appreciate your courtesy.

I first want to go to Captain Cohen. I think I heard you say that Apple had disclosed its source code to the Chinese Government. I believe that you said that, and that is a huge allegation for the NYPD to base on some news stories. Can you confirm this? Did you --

Mr. Cohen. Yes, ma'am. I'm with the Indiana State Police, by the way, not NYPD.

Ms. Eshoo. I am sorry.

Mr. Cohen. What I said was in preparing for my testimony I had found several news stories but I was unable to find anything to either confirm or deny that assertion --

Ms. Eshoo. Did you say that in --

Mr. Cohen. -- by the media.

Ms. Eshoo. I didn't hear all of your presentation around

that allegation, but I think it is very important for the record that we set this straight because that takes my breath away. That is a huge allegation. So thank you.

To Ms. Hess, the San Bernardino case is really a illustrative for many reasons. But one of the more striking aspects to me is the way in which the FBI approached the issue of gaining access to that now-infamous iPhone. We know that the FBI went to court to force a private company to create a system solely for the purpose of the Federal Government, and I think that is quite breathtaking. It takes my breath away just to try and digest that, and then to use that information whenever and however it wishes.

Some disagree, some agree, but I think that this is a worthy and very, very important discussion. Now, this came about after the government missed a key opportunity to back up and potentially recover information from the device by resetting the iCloud password in the days following the shooting.

Now, the Congress has appropriated just shy of $9 billion with a B for the FBI. Now, out of that $9 billion and how those dollars are spread across the agency, how is it that the FBI didn't know what to do?

Ms. Hess. Yes, ma'am.

Ms. Eshoo. How can that be?

Ms. Hess. If I may, the -- in the aftermath of San Bernardino, we were looking for any way to identify whether or not --

Ms. Eshoo. But did you ask Apple? Did you cal Apple right away and say we have this in our possession, this is what we need to get, how do we do it because we don't know how?

Ms. Hess. We did have discussion with Apple --

Ms. Eshoo. When?

Ms. Hess. I would --

Ms. Eshoo. After --

Ms. Hess. I would have to get --

Ms. Eshoo. After it was essentially destroyed because more than 10 attempts were made relative to the passcode?

Ms. Hess. I'm not sure. I will have to take that as a question for the record.

Ms. Eshoo. I would like to know, Ms. Hess, your response to this. I served for almost a decade on the House Intelligence Committee, and during my tenure, Michael Hayden was the CIA director. Now, as the former director of the CIA, he has said that America is safer, safer with unbreakable end-to-end encryption. Tell me what your response is to that?

Ms. Hess. My response would --

Ms. Eshoo. I think cyber crime, I might add, excuse me, is

embedded -- if I might use that word -- in this whole issue, but I would like to hear your response to the former director of the CIA.

Ms. Hess. Yes, ma'am. And from what I have read and heard of what he has said, he certainly, I believe, emphasizes and captures what was occurring at the time that he was in charge of those agencies.

Ms. Eshoo. I mean, has his thinking stopped from the time he was CIA director to being former and he doesn't understand encryption any longer? What are you --

Ms. Hess. No, ma'am --

Ms. Eshoo. -- suggesting?

Ms. Hess. -- as technology proceeds as such a rapid pace that one must be constantly in that business in order to keep up with the iterations.

Ms. Eshoo. Let me ask you about this. Once criminals know that American encryption products are open to government surveillance, what is going to stop them from using encrypted products and applications that fall outside of the jurisdiction of American law enforcement? I have heard you repeat over and over we are talking to people in Europe, we are talking -- I don't know. Is there a body that you are working through? Has this been formalized? Because if this stops at our border but doesn't

include others, this is a big problem for the United States of America law enforcement and American products.

Mr. McKinley. The gentlelady's time is expired.

Ms. Eshoo. Could she respond?

Mr. McKinley. Thank you very much.

Ms. Hess. Yes, ma'am, we are working with the international community and our international --

Ms. Eshoo. How?

Ms. Hess. -- partners on that issue.

Mr. McKinley. Thank you.

Ms. Eshoo. Do you have a national body? Is there some kind of international body that you are working through?

Mr. McKinley. Thank you.

Ms. Eshoo. Can she answer that?

Mr. McKinley. Do you want to finish your remark?

Ms. Hess. There is no one specific organization that we work through. There are a number of organizations we work through to that extent.

Ms. Eshoo. Thank you, Mr. Chairman.

Ms. DeGette. Mr. Chairman, I would ask unanimous consent that all of the members of the committee, as well as the members of the full committee who have been asked to sit in be allowed to supplement their verbal questions with written questions of

the witnesses.

Mr. McKinley. So approved.

Without seeing any more members seeking to be recognized for questions, I would like to thank the witnesses once again for their testimony today.

Now, I would like to call up the witnesses for our second panel to the table. Thank you again.

Okay. We will start the second panel. First, I would like to introduce the witnesses of our second panel for today's hearing, starting with Mr. Bruce Sewell will lead off on the second panel. Mr. Sewell is Apple's general counsel and senior vice president of legal and global security. He serves on the company's executive board and oversees all legal matters, including corporate governance, global security, and privacy. We thank Mr. Sewell for being with us today and look forward to his comments.

We would also like to welcome Amit Yoran -- is that close enough -- Mr. Yoran, president of RSA Security. RSA is an American computer and network security company, and as president, Mr. Yoran is responsible for developing RSA's strategic vision and operational execution across the business. Thanks to Mr. Yoran for appearing before us today, and we appreciate this testimony.

Next, we welcome Dr. Matthew Blaze, associate professor of computer and information science at the University of Pennsylvania. Dr. Blaze is a researcher in the area of secure systems, cryptology, and trust management. He has been at the forefront of these issues for over a decade, and we appreciate his being here today and offering his testimony on this very important issue.

Finally, I would like to introduce Dr. Daniel Weitzner, who is director and principal research scientist at the Computer Science and Artificial Intelligence Laboratory, Decentralized Information Group at the Massachusetts Institute of Technology. Mr. Weitzner previously served as United States deputy chief technological officer for internet policy in the White House. We thank him for being here with us today and look forward to learning from his expertise.

I want to thank all of our witnesses for being here and look forward to the discussion.

Now, as we begin, you are aware that this committee is holding an investigative hearing, and when doing so, it has had the practice of taking testimony under oath. Do any of have objection to testifying under oath?

Okay. Seeing none, the chair then advises you that under the rules of the House and the rules of the committee, you are

entitled to be advised by counsel. Do any of you desire to be represented or advised by counsel during your testimony today?

Seeing none, in that case, if you would please rise and raise your right hand, I will swear you in.

[Witnesses sworn.]

Mr. McKinley. Thank you. You are now under oath and subject to the penalties set forth in title 18, section 1001 of the United States Code. Each of you may be able to give a 5-minute summary of your written statement, starting with Mr. Sewell.

STATEMENTS OF BRUCE SEWELL, GENERAL COUNSEL, APPLE, INC.; AMIT YORAN, PRESIDENT, RSA SECURITY; MATTHEW BLAZE, ASSOCIATE PROFESSOR, COMPUTER AND INFORMATION SCIENCE, SCHOOL OF ENGINEERING AND APPLIED SCIENCE, UNIVERSITY OF PENNSYLVANIA; AND DANIEL J. WEITZNER, PRINCIPAL RESEARCH SCIENTIST, MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LAB, AND DIRECTOR, MIT INTERNET POLICY RESEARCH INITIATIVE

STATEMENT OF BRUCE SEWELL

Mr. Sewell. Thank you, Chairman Murphy --

Ms. DeGette. You need to --

Mr. Sewell. Better? Great. Thank you, Chairman Murphy, Ranking Member DeGette, and members of the subcommittee. It's my pleasure to appear before you today on behalf of Apple. We appreciate your invitation and the opportunity to be part of this important discussion on encryption.

Hundreds of millions of people trust Apple products with the most intimate details of their daily lives. Some of you might have a smartphone in your pocket right now, and if you think about it, there's probably more information stored on that phone than a thief could get by breaking into your home. And it's not just a phone. It's a photo album, it's a wallet, it's how you communicate with your doctor, your partner, and your kids. It's

also the command central for your car and your home. Many people also use their smartphone to authenticate and to gain access into other networks, businesses, financial systems, and critical infrastructure.

And we feel a great sense of responsibility to protect that information and that access. For all of these reasons, our digital devices, indeed our entire digital lives, are increasingly and persistently under siege from attackers. And their attacks grow more sophisticated every day. This quest for access fuels a multibillion dollar covert world of thieves, hackers, and crooks.

We are all aware of some of the recent large-scale attacks. Hundreds of thousands of Social Security numbers were stolen from the IRS. The U.S. Office of Personnel Management has said as many as 21 million records were compromised and as many as 78 million people were affected by an attack on Anthem's health insurance records.

The best way that we and the technology industry know how to protect your information is through the use of strong encryption. Strong encryption is a good thing. It is a necessary thing. And the government agrees. Encryption today is the backbone of our cybersecurity infrastructure and provides the very best defense we have against increasingly hostile

attacks.

The United States has spent tens of millions of dollars through the Open Technology Fund and other programs to fund strong encryption. And the administration's Review Group on Intelligence and Communications Technology urged the U.S. Government to fully support and not in any way to subvert, undermine, or weaken generally available commercial encryption software.

At Apple, with every release of hardware and software, we advance the safety, security, and data protection features in our products. We work hard to also assist law enforcement because we share their goal of creating a safer world.

I manage a team of dedicated professionals that are on call 24 hours a day, 365 days a year. Not a day goes by where someone on my team is not working with law enforcement. We know from our interaction with law enforcement officials that the information we are providing is extremely useful in helping to prevent and solve crimes. Keep in mind that the people subject to law enforcement inquiries represent far less than 1/10 of 1 percent of our hundreds of millions of users. But all of those users, 100 percent of them, would be made more vulnerable if we were forced to build a back door.

As you've heard from our colleagues in law enforcement, they

have the perception that encryption walls off information from them. But technologists and national security experts don't see the world that way. We see a data-rich world that seems to be full of information, information that law enforcement can use to solve and prevent crimes. This difference in perspective, this is where we should be focused. To suggest that the American people must choose between privacy and security is to present a false choice. The issue is not about privacy at the expense of security. It is about maximizing safety and security. We feel strongly that Americans will be better off if we can offer the very best protections for their digital lives.

Mr. Chairman, that's where I was going to conclude my comments, but I think I owe it to this committee to add one additional thought, and I want to be very clear on this. We have not provided source code to the Chinese Government. We did not have a key 19 months ago that we threw away. We have not announced that we are going to apply passcode encryption to the next-generation iCloud. I just want to be very clear on that because we heard three allegations. Those allegations have no merit.

Thank you.

[The prepared statement of Bruce Sewell follows:]

This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.

**********INSERT 6**********

Mr. McKinley. Thank you. And we turn now to the second panelist, Mr. Yoran.

STATEMENT OF AMIT YORAN

Mr. Yoran. Chairman Murphy, Ranking Member DeGette, and members of the committee, thank you for the opportunity to testify today on encryption. This is a very complex and nuanced issue, and I applaud the committee's efforts to better understand all aspects of the debate.

My name is Amit Yoran, and I'm the President of RSA, the security division of EMC. I would like to thank my mom for coming to hear my testimony today. In case things go sideways, I assure you, she's much tougher than she looks.

I've spent over 20 years in the cybersecurity field. In my current role, I strive to ensure that RSA provides-industry leading cybersecurity solutions. RSA has been a cybersecurity industry leader for more than 30 years. The more than 30,000 global customers we serve represent every sector of our economy.

Fundamental to RSA's understanding of the issues at hand is our rich heritage in encryption, which is the basis for cybersecurity technology. Our cybersecurity products are found in government agencies, banks, utilities, retailers, as well as hospitals and schools. At our core, we at RSA believe in the power of digital technology to fundamentally transform business and society for the better, and that the pervasiveness of our

technology helps to protect everyone.

Let me take a moment to say that we deeply appreciate the work of law enforcement and the national security community to protect our nation. I commend the men and women of law enforcement who have dedicated their lives to serving justice.

Private industry has long partnered with law enforcement agencies to advance and protect our nation and the rule of law. Where lawful court orders mandate it or where moral alignment encourages it, many tech companies have a regular, ongoing, and cooperative relationship with law enforcement in the U.S. and abroad. Simply put, it is in all of our best interests for the laws to be enforced.

I have four points I'd like to present today, all of which I've extrapolated on in my written testimony. First, this is no place for extreme positions or rushed decisions. The line connecting privacy and security is as delicate to national security as it is to our prosperity as a nation. I encourage you to continue to evaluate the issue and not rush to a solution.

Second, law enforcement has access to a lot of valuable information they need to do their job. I would encourage you to ensure that the FBI and law enforcement agencies have the resources and are prioritizing the tools and technical expertise required to keep up with the evolution of technology and meet their

important mission.

Third, strong encryption is foundational to good cybersecurity. If we lower the bar there, we expose ourselves even further to those that would do us harm. As you know, recent and heinous terrorist attacks have reinvigorated calls for exceptional access mechanisms. This is a call to create a back door to allow law enforcement access to all encrypted information.

Exceptional access increases complexity and introduces new vulnerabilities. It undermines the integrity of internet infrastructure and reduces -- and introduces more risk, not less, to our national interests. Creating a back door into encryption means creating opportunity for more people with nefarious intentions to harm us. Sophisticated adversaries and criminals would not knowingly use methods they know law enforcement could access, particularly when foreign encryption is readily available. Therefore, any perceived gains to our security from exceptional access are greatly overestimated.

Fourth, this is a basic principle of economics with very serious consequences. Our standard of living depends on the goods and services we can produce. If we require exceptional access from U.S.-based companies that would make our information economy less secure, the market will go elsewhere. But worse than that, it would weaken our power and utilities, our

infrastructures, manufacturing, health care, defense, and financial systems. Weakening encryption would significantly weaken our nation.

Simply put, exceptional access does more harm than good. This is the seemingly unanimous opinion of the entire tech industry, academia, the national security community, as well as all industries that rely on encryption and secured products.

In closing, I would like to thank all the members of the committee for their dedication in understanding this very complex issue.

[The prepared statement of Amit Yoran follows:]

**********INSERT 7**********

Mr. McKinley. Thank you.

Dr. Blaze?

STATEMENT OF MATTHEW BLAZE

Mr. Blaze. Thank you, Mr. Chairman, and members of the committee for the opportunity to testify before you today.

The encryption issue which, as you know, I've been involved with for over two decades now, has been characterized as a question of whether we can build systems that keep the good guys -- a lot of the good guys in but keep the bad guys out. And much of the debate has focused on questions of whether we can trust the government with the keys for data.

But before we can ask that question, and that's a legitimate political question that the political process is well-equipped to answer, there's an underlying technical question of whether we can trust the technology to actually give us a system that does that. And unfortunately, we simply don't know how to do that safely and securely at any scale and in general across the wide range of systems that exist today and that we depend on. It would be wonderful if we could. It would solve -- if we could build systems with that kind of assurance, it would solve so many of the problems in computer security and in general computer systems that have been with us since really the very beginning of software-based systems. But unfortunately, many of the problems are deeply fundamental.

The state of computer and network security today can really only be characterized as a national crisis. We hear about large-scale data breaches, compromises of personal information, financial information, and national security information literally on a daily basis today. And as systems become more interconnected and become more relied upon for the function of the fabric of our society and for our critical infrastructure, the frequency of these breaches and their consequences have been increasing.

If computer science had a good solution for making large-scale robust software, we would be deploying it with enormous enthusiasm today. It is really at the core of fundamental problems that we have. But we are fighting a battle against complexity and scale that we are barely able to keep up with. I wish I -- my field had simpler and better solutions to offer, but it simply does not.

We have only two good tools, tried-and-true tools that work for building reliable, robust systems. One of those is to build the systems to be as simple as possible, to have them include as few functions as possible, to decrease what we call the attack surface of these systems. Unfortunately, we want systems that are more complex and more integrated with other things, and that becomes harder and harder to do.

The second tool that we have is cryptography, which allows us to trust fewer components of the system, rely on fewer components of the system, and manage the inevitable insecurity that we have. Unfortunately, proposals for exceptional access methods that have been advocated by law enforcement and we heard advocated for by some of the members of the previous panel work against really the only two tools that we have for building more robust systems, and we need all the help we can get to secure our national infrastructure across the board.

There's overwhelming consensus in the technical community that these requirements are incompatible with good security engineering practice. I can refer you to a paper I collaborated on called "Keys Under Doormats@ that I referenced in my written testimony that I think describes the consensus of the technical community pretty well here.

It's unfortunate that this debate has been so focused on this narrow and very potentially dangerous solution of mandates for back doors and exceptional access because it leaves unexplored potentially viable alternatives that may be quite fruitful for law enforcement going forward.

One of -- there's no single magic bullet that will solve all of law enforcement problems here or really anywhere in law enforcement, but a sustained and a committed understanding of

things like exploitation of data in the cloud, data available in the hands of third parties, targeted exploitation of end devices such as Ms. Hess described in her testimony will require significant resources but have the potential to address many of the problems law enforcement describes, and we owe it to them and to all of us to explore them as fully as we can.

Thank you very much.

[The prepared statement of Matthew Blaze follows:]

**********INSERT 8**********

Mr. McKinley. Mr. Weitzner, you have 5 minutes.

STATEMENT OF DANIEL J. WEITZNER

Mr. Weitzner. Thank you, Vice Chairman McKinley, Chairman Murphy, and Ranking Member DeGette. Thank you for having me.

I think this hearing comes at a very important time in the debate about how to best accommodate the very real needs of law enforcement in the digital age.

I want to say that I don't think there's any sense in which law enforcement is exaggerating or overstating the challenges they face, and I don't think we should be surprised that they have big challenges. We think about the introduction of computers in our society, in our workplace, and our homes, and it -- to be colloquial, it throws everyone for a loop for a little while, and our institutions take a while to adjust. So we shouldn't expect this problem is going to be solved overnight.

I do think what's happening at this point in the debate, however, is that, as some of the previous witnesses said, we are, I think, seeing a growing consensus that introducing mandatory infrastructure-wide back doors is not the right approach. I'm going to talk about some ways that I think we can move forward, but I want to say why I think it is, and it comes back to the safe deposit box analogy that we heard.

We all do think it's reasonable that banks should have a

second key to our safe deposit boxes, and maybe even you should have drills that can drill through those locks in the event you can't find one of the keys. But the problem here is that we're all using the same safe, every single one of us, so if we make those safe deposit boxes so that they're a little too easy to drill into or if someone gets a hold of the key, then everyone is at risk, not just the couple thousand customers who happen to be at the one bank.

That's why we see political leaders really from all around the world now rejecting the idea of mandatory back doors. Recently, Secretary of Defense Ash Carter said, "I'm not a believer in back doors or a single technical approach. I don't think it's realistic,@ he said.

Robert Hannigan, who is the director of the U.K. surveillance agency GCHQ, said in a talk he delivered at MIT last month that "mandatory back doors are not the solution.@ He said "encryption should not be weakened, let alone banned, but neither is it true that nothing could be done without weakening encryption.@ He said, "I'm not in favor of banning encryption, nor of asking for mandatory back doors.@

And very tellingly, the vice president of the European Commission, who was the former Prime Minister of Estonia and famous for digitizing almost the entire country and the

government, said if people know there are back doors, how could people who, for example, vote online trust the results of the election if they know their government has a key to break into the system?

Two very quick steps that I think we should avoid going forward, and then a few suggestions about how to approach this challenge that you face, number one, I think you've heard us all say that we have to avoid introducing new vulnerabilities into an already quite vulnerable information infrastructure. It would be nice if we could choose that only the bad guys got weak encryption and the rest of us all got strong encryption, but I think we understand that's simply not possible.

You've also heard reference to CALEA, a piece of legislation in this committee's jurisdiction. There have been calls to address the difficult question -- this very difficult question by simply extending CALEA to apply to internet companies. But if you look closely at CALEA, it shows just how hard it will be to solve this problem with a one-size-fits-all solution. CALEA was targeted to a very small group of telecommunications companies that provided basically all the same product and were regulated in a then-pretty-stable way by the Federal Communications Commission. The internet and platform industry and the mobile apps and device and history is an incredibly diverse, global

industry, and there's no single regulatory agency that governs those services and products. That's very much by design, and so I think trying to impose a top-down regulatory solution on this whole complex of industries in order to solve this problem simply won't work.

What can we do going forward? Number one, I think that's in the efforts of the encryption working group that this committee and the Judiciary Committee had set up, I think it's very important to look closely at the specific situations that law enforcement faces, at the specific court orders, which have been successfully satisfy, which haven't, which introduce system-wide vulnerabilities that they were followed through, and which actually could be pursued without system-wide risk. I think there's a lot to be learned about the best practices both of law enforcement and technology companies, and there are probably some law enforcement agencies and technology companies that could up their game a little bit if they had a better sense of how to approach this issue.

I also think it's awfully important we make sure to preserve public trust in this environment, in this internet environment. I think we understand in the last 5 years that there's been significant concern from the public about the powers both of government and private sector organizations. I think it's a

great step that the House Judiciary Committee is moving forward amendments to the Electronic Communications Privacy Act that will protect data in the cloud, and I think if we can do more of that and assure the public that their data is protected, both in the context of government surveillance and private sector use, that we'll be able to move forward with this issue more constructively.

Thanks very much, and I'm looking forward to the discussion.

[The prepared statement of Daniel J. Weitzner follows:]

**********INSERT 9**********

Mr. McKinley. And thank you very much for your testimony.

And for the whole panel, if I might recognize myself for the first 5 minutes with some questions.

Mr. Sewell, you made quite a point that you have not provided the source codes to China. And it had come up from the earlier panel. Were you ever asked to provide anyone --

Mr. Sewell. By the Chinese Government or anyone?

Mr. McKinley. Yes.

Mr. Sewell. We have been asked by the Chinese Government. We refused.

Mr. McKinley. How recent were you asked?

Mr. Sewell. Within the past 2 years.

Mr. McKinley. Okay. Mr. Yoran, I have got a couple of questions for you. First, I was a little taken back. You said don't rush on the solution or whatever that might be. And as I said earlier, this has been 5 1/2 years. I have been hearing everyone talk about it, and they are not getting anything done. I don't know what we are waiting for. There has got to be a solution. I am just one of three licensed engineers in Congress, and by now, we would have the solution if there were more engineers and fewer attorneys here perhaps.

But if I might, with your question, I understand your company was founded by the original creators of a critical algorithm in

public key cryptography. Needless to say, encryption is your company's DNA. If anyone understands the importance of protecting encryption keys, it is your company. Yet apparently, several years ago, someone stole your seed keys, and as I understand, these are the keys that generate keys that are used for remote access, much like those used by Members and their staff.

If a company like yours, as sophisticated as it is and with the securities you have, it can lose control of encryption keys, how could we have confidence in others, especially smaller companies, the ability to do the same?

Mr. Yoran. Mr. Chairman, I think that you bring up two great points. The first statement I would make is that I'd like to highlight the fact that a tremendous amount of cooperation happens currently between law enforcement and the tech community, so that characterization that we've made no progress over the past 5 years is -- I think understates the level of effort put forth by the tech community to reply to and support the efforts of law enforcement.

I think what's occurring is -- and I won't call it a line in the sand -- but I think the current request from law enforcement have now gotten to the point where they're requesting a mandate that our products be less secure and will be -- have a tremendous and profound negative impact on our society and public safety,

as has already been made the point earlier.

The second point regarding RSA's own breach, I think, you know, that highlights the very critical role that encryption plays in the entire cybersecurity puzzle. The fact that sophisticated threat actors, nation, state, or cyber criminals are going to target the supply chain and where strong encryption and strong cybersecurity capabilities come from.

We're dealing with an incredibly sophisticated adversary and one that would put forth a tremendous effort to find any back doors if they were embedded in our security systems. It highlights the value of encryption to society in general, and I think it also highlights the importance of transparency around cyber breaches and cybersecurity issues.

Mr. McKinley. Thank you. In the first testimony, first panel -- I will stay with you, Mr. Yoran -- talked a little bit about the security of our infrastructure. And I think the response was along the line that it is not an encryption problem; it is a firewall problem. I am not sure that the American public understands the difference between that, and so I am going to go back to how comfortable should we be or can we be that we have proper protection on our security firms like yours that are energy or transportation system, particularly our grid? As I said, we have been hacked -- we are subject to it. We know we already have

been attacked once. So what more should we be doing?

Mr. Yoran. Mr. Chairman, I think the -- you know, the point made by the -- the response provided by the earlier panel was wrong. I think encryption plays an incredibly important role in protecting critical infrastructure. It is not a this is a firewall solution or this is an encryption solution. Most organizations that truly understand cybersecurity have a diverse set of products, applications, and many layers of defenses, knowing that adversaries are going to get in through firewalls. Not only adversaries but important openings are created in firewalls so that the appropriate parties can communicate to them as well. And those paths are frequently leveraged by adversaries to do nefarious things.

Mr. McKinley. So are you acknowledging, then, that we still are very vulnerable to someone shutting down our electric grid?

Mr. Yoran. I believe we are extremely vulnerable in any infrastructure that leverages technology, you know, how much of it is the entire grid, how much of it is localized. I certainly believe that utilities are exposed.

Mr. McKinley. Thank you. And let me just say in closing to all four of you, if you have got some suggestions how we might be able to address this, I am hearing time and time again in the districts with our grid system. I sure would like to hear back

from you about what we might be able to do.

With that, I yield the next question from the ranking member from Colorado, Ms. DeGette.

Ms. DeGette. Thank you so much.

Well, following up on the last question, I would like to stipulate that I believe, as most members of this panel believe, that strong encryption is really critical to our national security and everything else. But, as I said in my opening statement, I also recognize that we need to try to give law enforcement the ability to apprehend criminals when criminals are utilizing this technology to be able to commit their crimes and to cover up after the crimes.

So, first of all, Mr. Sewell, I believe you testified that your company works with law enforcement now, is that correct?

Mr. Sewell. That is correct.

Ms. DeGette. Thanks. And I think that you would also acknowledge that while encryption really does provide benefit both for consumers and for society for security and privacy, we also need to address this thorny issue about how we deal with criminals and terrorists who are using encrypted devices and technologies, is that correct?

Mr. Sewell. I think this is a very real problem. And let me start by saying that the conversation we're engaged in now,

I think, has become something of a conflict, Apple v. the FBI --

Ms. DeGette. Right. And I don't --

Mr. Sewell. -- and that's just the wrong approach.

Ms. DeGette. And you don't agree with that, I would hope.

Mr. Sewell. I absolutely do not.

Ms. DeGette. And, Mr. Yoran, you don't agree with that, that it is technology versus law enforcement, do you? Yes or no will work.

Mr. Yoran. No, I don't agree it's technology --

Ms. DeGette. Okay. And I am assuming that you, Dr. Blaze?

Mr. Blaze. No.

Ms. DeGette. And how about you, Mr. Weitzner?

Mr. Weitzner. [Nonverbal response.]

Ms. DeGette. No.

Well, that is good. So here is another question, then. And I asked the last panel that. Do you think it is a good idea for the FBI and other law enforcement agencies to have to go to third-party hackers to get access to data for which they have court orders to get?

Mr. Weitzner. I don't think that's a good idea.

Ms. DeGette. Do you think so, Mr. Yoran?

Mr. Yoran. No, ma'am.

Ms. DeGette. Dr. Blaze?

Mr. Blaze. No, I think it -- if I could just clarify, the fact that the FBI had to go to a third party indicates that the FBI either had or devoted insufficient resources to --

Ms. DeGette. Right.

Mr. Blaze. -- finding a solution --

Ms. DeGette. And they couldn't --

Mr. Blaze. -- in advance of the problem.

Ms. DeGette. -- do it on their own. Right. I am going to get to that in a second. So it is just really not a good model. So here is my question. Mr. Yoran, do you think that the government should enhance its own capabilities to penetrate encrypted systems and pursue workarounds when legally entitled to information they cannot obtain either from the user directly or service providers? Do you think that they should develop that?

Mr. Yoran. Yes, ma'am.

Ms. DeGette. Do you think they have the ability to develop that?

Mr. Yoran. Yes, ma'am.

Ms. DeGette. Professor, do you think that they have the ability to develop that?

Mr. Blaze. It requires enormous resources, and they probably -- with the resources they currently have, I think it's likely that they don't have the ability to --

Ms. DeGette. One thing Congress has, we may not be internet experts but we have resources.

Mr. Blaze. Right. And I think this is a soluble problem.

Ms. DeGette. Mr. Weitzner?

Mr. Weitzner. I think that they certainly should have the resources, and I think really the key question is whether they have the personnel. And I think it will take some time to build up a set of personnel expertise --

Ms. DeGette. Well, I understand it will take time --

Mr. Weitzner. Yes.

Ms. DeGette. -- but do you think they can develop those resources?

Mr. Weitzner. I think so. Absolutely. The only thing --

Ms. DeGette. Thank you. Okay. So, Mr. Yoran, I want to ask you another question. Do you think that all of us supporting the development of increased capability within the government can be a reasonable path forward, as opposed to either relying on third parties or making companies write new software or redesign systems?

Mr. Yoran. Yes, ma'am.

Ms. DeGette. You think that is a better approach? Okay. And I assume, Mr. Sewell, you probably agree with that, too?

Mr. Sewell. I'd agree that we ought to spend more money,

time, resources on the FBI and on local law enforcement training --

Ms. DeGette. And would Apple be willing to help them develop those capabilities?

Mr. Sewell. We actively do participate in helping them.

Ms. DeGette. So your answer would be yes?

Mr. Sewell. That we would participate in training, we would --

Ms. DeGette. And helping them develop those in new capabilities?

Mr. Sewell. We -- what we can do is to help them understand our ecosystem.

Ms. DeGette. Right.

Mr. Sewell. That's what we do on a --

Ms. DeGette. So I guess --

Mr. Sewell. -- daily basis.

Ms. DeGette. Right. I am not trying to trick you.

Mr. Sewell. No, and I'm not --

Ms. DeGette. Yes. Okay.

Mr. Sewell. -- responding either.

Ms. DeGette. So I guess, then, your answer would be yes, you are willing to help us in conjunction with law enforcement and Congress to solve this problem. Is that correct, Mr. Sewell?

Mr. Sewell. I want to solve the problem just like everyone else.

Ms. DeGette. And are you willing to work with law enforcement and Congress to do it? Yes or no?

Mr. Sewell. Congresswoman, we work with them every day. Yes, of course --

Ms. DeGette. A yes or no will work.

Mr. Sewell. Of course we will. Of course we are.

Ms. DeGette. Thank you.

Mr. Sewell. Yes.

Ms. DeGette. Mr. Yoran?

Mr. Yoran. Yes, ma'am.

Ms. DeGette. Professor Blaze?

Mr. Blaze. Absolutely?

Ms. DeGette. And Mr. Weitzner?

Mr. Weitzner. Yes.

Ms. DeGette. Thank you so much. Thank you, Mr. Chairman.

Mr. McKinley. Thank you. And I now recognize Mr. Griffith from Virginia.

Mr. Griffith. Thank you, Mr. Chairman. I greatly appreciate that.

My background, I am just a small college history major that then went into law, and as a part of that, Mr. Sewell, I would

have to ask, would you agree with me that, in the history of mankind, it took us thousands of years to come up with the concept of civil liberties and that perhaps 5 1/2 years isn't such a long time to try to find a solution to this current issue? And likewise, that it was -- the answer was in the affirmative for those who might not have --

Mr. Sewell. It was, yes.

Mr. Griffith. -- heard that. And that it was lawyers who actually created the concept of individual liberty and one that our country has been proud to be the leader in the world in promoting. Would that also be true?

Mr. Sewell. That's very true, sir, yes.

Mr. Griffith. That being said, I was very pleased to hear in answers to Ms. DeGette that all of you are willing to help us solve this problem because there is no easy answer. I liked the safety deposit box analogy. Mr. Weitzner, thanks for ruining it for me in your analysis.

But I would ask Mr. Sewell if there isn't some way -- and again, I can't do what you all do so I have to simplify it to my terms. Is there some way that we can create the vault that the banks have with the safety deposit box in it, and then once you are inside of there, if you want that security -- because not everybody has a safety deposit box -- but if you want that

security, that then there is a system of a dual but separate keys with companies like yours are others holding one of the two keys and then the individual holding the other key and then having the ability to, with a proper search warrant, have law enforcement be able to get in? I mean, I am trying to break it down into a concept I can understand where I can then apply what we have determined over the course of the last several hundred years is the appropriate way to get at information. And it is difficult in this electronic age.

Mr. Sewell. It is very difficult, Congressman. I agree. We haven't figured out a way that we can create an access point and then create a set of locks that are reliable to protect access through that access point. That is what we struggle with. We can create an access point and we can create locks, but the problem is that the keys to that lock will ultimately be available somewhere, and if they're available anywhere, they can be accessed by both good guys and bad guys.

Mr. Griffith. So you would agree with Mr. Weitzner's position or his analysis, which I thought was accurate, is that the problem is we are not giving a key and a drill to one safety deposit box; it is everybody in the bank who suddenly would have their information in the open. And I saw that you wanted to make a comment, Mr. Weitzner?

Mr. Weitzner. I just want to -- since this analogy seems to be working, you know, we don't put much stuff in our safe deposit boxes, right? I mean, I actually don't have one to be honest.

There's this core concern, back to your civil liberties framework, that somehow we have a warrant-free zone that's going to take over the world. I think that if you follow the safety deposit box analogy, what we know is that the information that's important to law enforcement exists in many places. And I don't question that there will be some times when law enforcement can't get some piece of information at once.

But I think what you're hearing from a number of us and from the technical community is that this information is very widely distributed, and much of it is accessible in one way or the other or inferable from information that's produced by other third parties. And I think that part of the path forward is to really understand how to exploit that to the best extent possible in investigations so that we're not all focused on the hardest part of the problem where the hardest part of the problem is what do you do if you have very strongly encrypted data? Can you ever get it? It may not be the best place to look all the time because it may not always be available.

Mr. Griffith. And, of course, historically, you are never able to get a hold of everything.

Dr. Blaze, you wanted to weigh in?

Mr. Blaze. So I just wanted to caution that the split-key design, as attractive as it sounds, was also the core of the NSA-designed clipper chip, which was where we started over two decades ago.

Mr. Griffith. I appreciate that.

Mr. Yoran, I have got to tell you, I did think your testimony and your written testimony in particular was enlightening in regard to the fact that if we do shut down the U.S. companies, then there may even be safe havens created by those companies that are not our friends and are specifically our enemies. And unfortunately -- I wanted to ask a series of questions on that, but I see that my time has expired, and so I am required to yield back, Mr. Chairman.

Mr. McKinley. Looking at the other panel members, we have Mrs. Brooks from Indiana, your 5 minutes.

Mrs. Brooks. Thank you, Mr. Chairman.

I would like to start out with a comment that was made in the first panel, and I guess this is to Mr. Sewell, whether or not you can share with us. Does Apple plan to use encryption in the cloud?

Mr. Sewell. We've made no such announcement. I'm not sure where that statement came from, but we've made no such

announcement.

Mrs. Brooks. Okay. I understand you've made no such announcement, but is that being explored?

Mr. Sewell. I think it would be irresponsible for me to come here and tell you that we are not even looking at that, but we have made no announcement. No decision has been made.

Mrs. Brooks. And are these discussions helping inform Apple's decisions? And is Apple communicating with any law enforcement about that possibility?

Mr. Sewell. These discussions are enormously, enormously helpful, and I'd be glad to go further into that. I've learned some things today that I didn't know before, so they're extremely important. We are considering, we are talking to people, we are being very mindful of the environment in which we are operating.

Mrs. Brooks. And I have certainly seen and I know that Apple and many companies have a whole set of policies and procedures on compliance with legal processes and so forth. And so I assume that you have regular conversations with policymakers and law enforcement, whether it is FBI or other agencies, on these policy issues. Is that correct?

Mr. Sewell. That's very correct. I interact with law enforcement at two very different levels. One is a very operational level. My team supports daily activities in response

to lawful process, and we worked very closely on actual investigations. I can mention at least two where we've recently found children who've been abducted. We've been able to save lives working directly with our colleagues in law enforcement. So at that level we have a very good relationship, and I think that gets lost in the debate sometimes.

At the other side, I work at a -- perhaps a different level. I work directly with my counterpart at the FBI. I work directly with the most senior people in the Department of Justice, and I work with senior people in local law enforcement on exactly these policy issues.

Mrs. Brooks. Well, and I thank you and all the others for cooperating with law enforcement and working on these issues, but it seems as if most recently there have not been enough of that discussions. Hence, that is why we are having these hearings and why we need to continue to have these hearings.

But I think that we have to continue to have the dialogue on the policy while continuing to work on the actual cases and recognize that obviously technology companies have been tremendously helpful, and we need them to be tremendously helpful in solving crimes and in preventing future crimes. I mean, it is not just about solving crimes already perpetrated, but it is always, particularly with respect to terrorism, how do we ensure

that we are keeping the country safe?

I am curious with respect to a couple of questions with respect to legal hacking and the types of costs that are associated with legal hacking, as well as the personnel needed. And since the newer designs of iPhones prevent the bypassing of the built-in encryption, does Apple actually believe that lawful hacking is an appropriate method for investigators to use to assess the evidence in investigations?

Mr. Sewell. So I don't think we have a firm position on that. I think there are questions that would have to be answered with respect to what the outcome of that lawful hacking is, what happens to the product of that lawful hacking. So I don't have a formal corporate position on that.

Mrs. Brooks. So then, because that has been promoted, so to speak, as far as a way around this difficult issue, are you having those policy discussions about Apple's view and the technology sector's view on lawful hacking? Are those discussions happening with law enforcement?

Mr. Sewell. I think this is a very nascent area for us, but particularly the question is what happens to the result. Does it get disclosed? Does it not get disclosed? That, I think, is an issue that has not been well explored.

Mrs. Brooks. Mr. Yoran, do you have an opinion on that

lawful hacking?

Mr. Yoran. Not an opinion on lawful hacking in specific, but I would just point out that doing encryption properly is very, very hard. Trying to keep information secret in the incredibly interconnected world that we live in is very, very hard. And I would suggest that it's getting harder, not easier.

So the information, the data that law enforcement has access to, I think, is certainly much more than the metadata that they've had over the past several years. But now, as applications go into the cloud, those cloud application providers need to access the data. So the sensitive information is not just on your iPhone or other device, it's sitting in the cloud, and law enforcement has access there because it cannot be encrypted. It needs to be accessed by the cloud provider in order to do the sophisticated processing and provide the insight to the consumer that they're looking for.

Mrs. Brooks. My time is expired. I have to yield back.

Mr. McKinley. Thank you. And now seeing no other members of the subcommittee here with us, we can then go --

Mr. Bilirakis. Mr. Chairman? I am sorry.

Mr. McKinley. Oh, okay. You are on the subcommittee?

Mr. Bilirakis. No.

Mr. McKinley. Okay. We are going to -- none on the

subcommittee, so now we are going to members that have been given privileges to speak. And I was advised I was to go to the other side, like this ping-pong game. And Ms. Eshoo from California, your 5 minutes.

Ms. Eshoo. Thank you, Mr. Chairman.

First of all, to Mr. Yoran, I love your suit and tie. It brings a little of the flavor of my district into this big old hearing room. And a warm welcome to your mother. I don't know where she is, but it is great to have your mother here, great, wonderful.

I know that Associate Professor Blaze talked about the crisis of the vulnerability in our country relative to, you know, how our systems, how vulnerable our systems are. I would just like to add for the record that up to 90 percent of the breaches in our system in our country are due to two major factors. One is systems that are less than hygiene, unhygienic systems. Number two, very poor security management.

So I think the Congress should come up with at least a floor relative to standards so that we can move that word crisis away from this. But we really can do something about that. I know it costs money to keep systems up, and there are some that don't invest in it, but that can be addressed.

The word conversation has been used, and I think very

appropriately. And this is a very healthy hearing. Unfortunately, the first thing the American people heard was a very powerful Federal agency, you know, within moments of the tragedy in San Bernardino demand of a private company that they must do thus and so, otherwise, we will be forever pitted against one another, and there is no other resolution except what I call a swinging door that people can go in and out of. When I say people, in this case, it is the government.

Now, they American people have a healthy suspicion of Big Brother, but they also have a healthy suspicion of big corporations. They just do. It is in our DNA, and I don't think that is an unhealthy thing. But that first snapshot, I think, we need to move to the next set of pictures on this. And I am heartened that the panel seems to be unanimous that this weakening of our overall system by having a back door, by having a swinging door is not the way to go.

So in going past that, I would like to ask Mr. Sewell the following. Whether introducing a third-party access, and that has been talked about, I think that would fundamentally weaken our security. How does third-party access impact security? How likely do you think it is that law enforcement could design a system to address encrypted data that would not carry with it the unanticipated weaknesses of its own?

I am worried about law enforcement in this, and I want to put this on the record as well. I think that it says something that the FBI didn't know what it was doing when it got a hold of that phone, and that is not good for us. It is not going to attract smart young people to come into a Federal agency because what it says to them is it doesn't seem to us they know what they are doing.

So can you address this third-party access and what kind of effect it would have on overall security?

Mr. Sewell. Thank you very much for the question, Congresswoman.

If you allow third-party access, you have to give the third party a portal in which to exercise that access. This is fundamentally the definition of a back door or a swinging door as you've, I think, very aptly described it.

There is no way that we know of to create that vulnerability, to create that access point and more particularly to maintain it. This was the issue in San Bernardino was not just give us an access point but maintain that access point in perpetuity so that we can get in over and over and over again.

That for us -- we have no way of doing that without undermining and endangering the entire encryption infrastructure. We believe that strong, ubiquitous encryption is the best way that we can maintain the safety, security, and

privacy of all of our users. So that would be fundamentally a problem.

Ms. Eshoo. Thank you very much.

Thank you, Mr. Chairman, for your legislative courtesy again. Thank you to the witnesses. You have been, I think, most helpful.

Mr. Murphy. I thank the witnesses, too. I apologize I had to run out for a while, but I am going to get to ask a few questions here and I want to make sure to follow up.

So, Mr. Sewell --

Mr. Sewell. Sir.

Mr. Murphy. -- we can all understand the benefits of strong encryption, whether it is keeping someone's own bank statement, financial records encrypted so we didn't have to worry about hackers there. We already heard some pretty compelling testimony in the first, challenges about law enforcement, criminal activity, child predators, homicides, et cetera. Based on your experience, what we heard today, can you acknowledge that the spread of default encryption does present a challenge for law enforcement?

Mr. Sewell. I think it absolutely does. And I would not suggest for a moment that law enforcement is overstating the same claim that has been made by other panelists. I think the problem

is that there's a fundamental disconnect between the way we see the world and the way law enforcement sees the world, and that's where I think we ought to be focusing.

Mr. Murphy. And what is that disconnect? What is that two different world views?

Mr. Sewell. The disconnect has to do with the evolution of technology in society and the impact of that technology in society. What you've heard from our colleagues in law enforcement is that the context in which encryption occurs reduces the scope of useful data that they have access to, this going-dark problem.

But if you talk to technologists, we see the world in a very different way. We see the impact of technology is actually a burgeoning of information. We see that there's an abundance of information, and this will only increase exponentially as we move into a world where the Internet of Things becomes part of our reality.

So you hear on one side we're going dark, and you hear on the other side there's an abundance of information. That circle needs to be squared. And the only way that I think we can do that is by cooperating and talking and engaging in the kind of activity that Madam DeGette was suggesting. We need to work together --

Mr. Murphy. So let me bring this --

Mr. Sewell. -- so we understand their perspective, they understand ours.

Mr. Murphy. I appreciate that, but I am not -- it is a very compelling argument you gave, but I have no idea what you just said. So let me --

Mr. Sewell. Sure.

Mr. Murphy. -- try and put this into terms that we can all talk about.

Mr. Sewell. Sure.

Mr. Murphy. We heard testimony from the first panel of child predators who are able to hide behind this invisible cloak, from a murder scene where they could have perhaps caught who did this. We know that when it comes to crimes, there are those who just won't commit crimes because they have a good moral compass. We have those who will commit them anyway because they have none. We also have those who can be deterred because they think they might get caught. And when it comes to other issues such as terrorist acts where you can get into a cell phone or something from someone who has committed an act, you can find out if they are planning more and save other lives.

So what do you tell a family member who has had their child abused and assaulted in unspeakable forms, what do you tell them about burgeoning technology? I mean, tell me what comfort we can

give someone about the future?

Mr. Sewell. I think in situations like that, of course, they're tragic. I'm not sure that there's anything which I or any one of us could say that would help to ease that pain.

On the other hand, we deal with this every day. We deal with cases where children have been abducted. We work directly with law enforcement to try to solve those crimes. We had a 14-year-old girl from Pennsylvania just recently that was abducted by her captor. We worked immediately with the FBI in order to use IP logs to identify the location where she had been stashed. We were able to get feet on the ground within a matter of hours, find that woman, rescue her, and apprehend --

Mr. Murphy. And that is good and I appreciate that, but what about -- I look at this case that was presented, though, when someone may have a lot of information hidden, and if they could get in there, whether it is child predators or it is a terrorist where we could prevent more harm --

Mr. Sewell. And we're missing the point of technology here. The problems that we're trying to solve don't have an easy fix --

Mr. Murphy. I know that. I know that. But tell me, I need to know --

Mr. Sewell. So --

Mr. Murphy. -- you are working in a direction that helps here.

Mr. Sewell. Absolutely.

Mr. Murphy. That is what I am trying to help you elicit.

Mr. Sewell. Photo DNA, hashing images so that when those images move across the internet we can identify them, we can track them. The work that we do with Operation Railroad is exactly that. It's an example of taking technology, taking feet-on-the-ground law enforcement techniques and marrying them together in a way that fundamentally changes --

Mr. Murphy. And for people who are using encrypted sources, whether it is by default or intention to hide their data and their intention and their harmful activity that they are planning on hurting more, what do we tell the public about that?

Mr. Sewell. We tell the public that, fundamentally, we're working on the problem and that we believe strong, ubiquitous encryption provides the best and safest --

Mr. Murphy. So does that mean Apple is going to be working with the FBI and law enforcement on this problem? I know that the response of Apple was we ought to have a commission. You are looking at the commission, the Energy and Commerce Committee Oversight and Investigation Committee, and we want to find solutions. We want to work with you. And I am pleased you are

here today.

And you heard many of us say we don't think there is right or wrong absolutes. This is not black and white.

Mr. Sewell. Yes.

Mr. Murphy. We are all in this together, and we want to work on that. I need to know about your commitment, too, in working with law enforcement. Could you make a statement on that?

Mr. Sewell. Can I tell you a story, Congressman?

Mr. Murphy. Sure.

Mr. Sewell. Can I actually do that? I sat opposite my counterpart at the FBI, a person that I know very well. We don't talk frequently but we talk regularly. We're on a first-name basis. I sat opposite from him and I said amidst all of this clamor and rancor, why don't we set aside a day. We'll send some smart people to Washington or you send some smart people to Cupertino, and what we'll do for that day is that we'll talk to you about what the world looks like from our perspective. What is this explosion of data that we can see? Why do we think it's so important? And you, talk to us about the world that confronts your investigators from the moment they wake up in the morning. How do they think about technology? How do they think about the problems that they're trying to solve?

And we were going to sit down together for a day. We were

planning that at the time that the San Bernardino case was filed. That got put on hold. But that offer still exists. That's the way we're going to solve these problems.

Ms. DeGette. Mr. Chairman?

Mr. Murphy. Yes.

Ms. DeGette. Will you yield for one second?

Mr. Murphy. Yes.

Ms. DeGette. You know, Mr. Sewell, if we can facilitate that meeting in any way, I am sure the chairman and I would be more than happy to do that. And we have some very lovely conference rooms that are painted this very same color, courtesy of Chairman Upton, and we will have you there.

Mr. Sewell. Madam, if we can get out of the lawsuit world --

Ms. DeGette. You know what --

Mr. Sewell. -- let's start cooperating.

Ms. DeGette. That would be great.

Mr. Sewell. Yes.

Ms. DeGette. Thank you.

Mr. Sewell. Great.

Mr. Murphy. We want that to be facilitated. We have too many lives at stake and the concerns of many families and Americans. This is central. This is core.

Mr. Sewell. I agree.

Mr. Murphy. So thank you. I know I am out of time.

Mr. Bilirakis is going to be recognized now for 5 minutes.

Mr. Bilirakis. Thank you, Mr. Chairman. I appreciate it so very much. I want to thank everyone here on the panel for your technology leadership that helps keep us safe because that is what our priority here is in the United States Congress. At least it is mine and I know many others on this panel.

We are here to find a balance between security and privacy and not continue to pit them against each other. I think you will agree with that.

Mr. Yoran, how quickly does one lifecycle of encryption last as a secure system until vulnerabilities are found and exploited? Will this continually be a game of cat-and-mouse or are we at a level now where software and the processes are strong enough to make end-to-end encryption a stable system?

Mr. Yoran. Systems are attacked and vulnerabilities are exploited almost instantaneously once computer systems, mobile devices are put on the internet. Once crypto methods are published, there's an entire research community that goes to work. Depending on the strength of the encryption, vulnerabilities may be discovered immediately, or they may be discovered decades down the road, in which case all of the information may have been at

risk while that crypto system was in use.

And frequently, the exposure and the exploitation of crypto systems isn't necessarily based on the strength of the algorithms themselves but on how they're implemented and how the systems are interconnected. I might not have the key to get information off of a particular device, but because I can break into the operating system because I have physical access to it, because I can read the chips, because I can do all sorts of different things. I can still get information or I can get the key while it was resident in memory. It's just a very complex system that all has to work perfectly in order for the information to be --

Mr. Bilirakis. Thank you.

Mr. Yoran. -- protected.

Mr. Bilirakis. The next question is for the entire panel. We have known for the past few years that any significant threat to our homeland will likely include a cyber attack. Will you agree on that?

Can you elaborate on the role that encryption plays in this process of continuing national security? Certainly, the military has used forms of encryption for decades, but can you give us a contemporary snapshot of how encryption use by government or nongovernment users protect us against cyber attacks today? We can start over here, please.

Mr. Sewell. I will answer the question, but I am not at all the expert in this space. I think the other panelists are much more expert than I am in the notion of encryption and protecting our infrastructure.

The one point that I will say that I tried to emphasize in my opening statement was that we shouldn't forget about some of the changes that are happening in terms of the way that infrastructure can be accessed. I think we sometimes lose sight of the fact that phones themselves now are being used as authentication devices. If you can break the encryption and you can get into the phone, that may be a very easy way to get into the power grid, to get into our transport systems, into our water systems.

So it's not just a question of the firewalls or the access; it's how -- what is the instrumentality that you used to get into those things that we also have to be concerned about.

Mr. Bilirakis. Thank you. Mr. Yoran?

Mr. Yoran. I believe fundamentally that security is actually on the same side as privacy and our economic interest. It's fundamental. It's fundamental in the national security community. But it's also mandated by law to protect all sorts of other data in other infrastructures and systems such as financial services, health care records, so on and so forth, such

that even folks who might not gain an advantage by having strong encryption available like General -- I'm sorry, Admiral Rogers, the director of the NSA; and James Clapper, the director of National Intelligence, are on the record saying that they believe it's not in the U.S. best interest to weaken encryption.

Mr. Bilirakis. Anyone else wish to comment, please?

Mr. Blaze. I mean, encryption is used in protecting critical infrastructure the same way it's used in protecting other aspects of our society. It protects sensitive data when it's being transmitted and stored, including on mobile devices and over the internet and so on.

I just want to add that critical infrastructure systems are largely based and built upon the same components that we're using in consumer and business devices as well. There aren't -- you know, critical infrastructure systems essentially depend upon mobile phones and operating systems that you and I are using in our day-to-day life. And so when we weaken them, we also weaken the critical infrastructure systems.

Mr. Bilirakis. Sir?

Mr. Weitzner. Could I just add very briefly that I actually thought Mr. Sewell's answer was pretty good. But -- and what's critical about those systems that we rely on to protect our critical infrastructure is that when we find flaws in them, we

have to patch them quickly. We have to fix them quickly. As Mr. Yoran said, you know, these systems are constantly being looked at.

I'm concerned that if we end up imposing requirements on our security infrastructure, on our encryption tools, if we impose CALEA-like requirements, the process of identifying flaws, fixing them, putting out new versions rapidly is going to be slowed down to figure out whether those comply with whatever the surveillance requirements are. And I think that's the wrong direction for us to go in. We want to make these tools as adaptive as possible. We want them to be fixed as quickly as possible, not be caught in a whole set of rules about what they have to do and not do to accommodate surveillance needs.

Mr. Bilirakis. Thank you very much. Thank you, Mr. Chairman, for allowing me to participate. I appreciate it, and I will yield back.

Mr. Murphy. Thank you. I ask unanimous consent that the letter from CTA be admitted to the record. Without objection, that will be so.

[The information follows:]

**********COMMITTEE INSERT 10**********

Mr. Murphy. And I believe, Ms. DeGette?

Ms. DeGette. I would ask unanimous consent -- Ms. Eshoo has a letter from TechNet dated April 19 that we would like to have put in the record.

Mr. Murphy. Thank you.

[The information follows:]

**********COMMITTEE INSERT 11**********

Mr. Murphy. And I also ask unanimous consent that the contents of the document binder be introduced in the record and authorize staff to make any appropriate redactions. Without objection, the documents will be entered in the record with any redactions the staff determines are appropriate.

[The information follows:]

**********COMMITTEE INSERT 12**********

Mr. Murphy. And in conclusion, I want to thank all the witnesses and members that participated in today's hearing.

I remind members they have 10 business days to submit questions for the record. I ask that the witnesses all agree to respond promptly to the questions.

Thank you so much. We look forward to hearing from you more, and we will get you together. Thank you.

Mr. Sewell. Good. Thank you, Mr. Chairman.

Mr. Murphy. This committee is adjourned.

[Whereupon, at 1:14 p.m., the subcommittee was adjourned.]