

**DECIPHERING THE DEBATE OVER ENCRYPTION:
INDUSTRY AND LAW ENFORCEMENT PERSPEC-
TIVES**

HEARING
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND
INVESTIGATIONS
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED FOURTEENTH CONGRESS
SECOND SESSION

APRIL 19, 2016

Serial No. 114-136



Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

20-696

WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan

Chairman

JOE BARTON, Texas

Chairman Emeritus

ED WHITFIELD, Kentucky

JOHN SHIMKUS, Illinois

JOSEPH R. PITTS, Pennsylvania

GREG WALDEN, Oregon

TIM MURPHY, Pennsylvania

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

Vice Chairman

STEVE SCALISE, Louisiana

ROBERT E. LATTA, Ohio

CATHY McMORRIS RODGERS, Washington

GREGG HARPER, Mississippi

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

DAVID B. MCKINLEY, West Virginia

MIKE POMPEO, Kansas

ADAM KINZINGER, Illinois

H. MORGAN GRIFFITH, Virginia

GUS M. BILIRAKIS, Florida

BILL JOHNSON, Ohio

BILLY LONG, Missouri

RENEE L. ELLMERS, North Carolina

LARRY BUCSHON, Indiana

BILL FLORES, Texas

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

RICHARD HUDSON, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

FRANK PALLONE, JR., New Jersey

Ranking Member

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DeGETTE, Colorado

LOIS CAPPs, California

MICHAEL F. DOYLE, Pennsylvania

JANICE D. SCHAKOWSKY, Illinois

G.K. BUTTERFIELD, North Carolina

DORIS O. MATSUI, California

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

JERRY McNERNEY, California

PETER WELCH, Vermont

BEN RAY LUJAN, New Mexico

PAUL TONKO, New York

JOHN A. YARMUTH, Kentucky

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

KURT SCHRADER, Oregon

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

TIM MURPHY, Pennsylvania

Chairman

DAVID B. MCKINLEY, West Virginia

Vice Chairman

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

H. MORGAN GRIFFITH, Virginia

LARRY BUCSHON, Indiana

BILL FLORES, Texas

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

RICHARD HUDSON, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

JOE BARTON, Texas

FRED UPTON, Michigan (*ex officio*)

DIANA DeGETTE, Colorado

Ranking Member

JANICE D. SCHAKOWSKY, Illinois

KATHY CASTOR, Florida

PAUL TONKO, New York

JOHN A. YARMUTH, Kentucky

YVETTE D. CLARKE, New York

JOSEPH P. KENNEDY, III, Massachusetts

GENE GREEN, Texas

PETER WELCH, Vermont

FRANK PALLONE, JR., New Jersey (*ex*

officio)

CONTENTS

	Page
Hon. Tim Murphy, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	2
Prepared statement	3
Hon. Diana DeGette, a Representative in Congress from the state of Colorado, opening statement	4
Hon. Fred Upton, a Representative in Congress from the state of Michigan, opening statement	6
Prepared statement	8
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	8
Prepared statement	9

WITNESSES

Ron Hickman, Sherriff, Harris County, Texas	
Prepared statement	12
Amy Hess, Executive Assistant Director for Science and Technology, Federal Bureau of Investigations	20
Prepared statement	22
Answers to submitted questions ¹	144
Thomas P. Galati, Chief, Intelligence Bureau, New York City Police Department	26
Prepared statement	28
Answers to submitted questions	150
Charles Cohen, Commander, Office of Intelligence and Investigative Technologies, Indiana State Police	32
Prepared statement	34
Answers to submitted questions	156
Bruce Sewell, General Counsel, Apple, Inc.; Amit Yoran, President, RSA Security	72
Prepared statement	74
Answers to submitted questions	165
Amit Yoran, President, RSA Security	77
Prepared statement	79
Answers to submitted questions	175
Matthew Blaze, Associate Professor, Computer and Information Science, School of Engineering and Applied Science, University of Pennsylvania	87
Prepared statement	89
Answers to submitted questions	183
Daniel J. Weitzner, Principal Research Scientist, MIT Computer Science and Artificial Intelligence Lab, and Director, MIT Internet Policy Research Initiative	100
Prepared statement	102
Answers to submitted questions	189

SUBMITTED MATERIAL

Subcommittee memorandum	135
Statement of the Consumer Technology Association, submitted by Mr. Murphy	140
Statement of TechNet, submitted by Ms. Eshoo	142
Document binder ¹	

¹ The information can be found at: <http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104812>.

**DECIPHERING THE DEBATE OVER
ENCRYPTION: INDUSTRY AND LAW EN-
FORCEMENT PERSPECTIVES**

TUESDAY, APRIL 19, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

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.

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.

OPENING STATEMENT OF HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. MURPHY. It is chaos, OK. 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.

[The prepared statement of Mr. Murphy follows:]

PREPARED STATEMENT OF HON. TIM MURPHY

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 commu-

nications, but would also provide the government with a key to access those communications, if necessary. This so-called “backdoor” sparked intense debate between the government and the technology community about the benefits—and risks—of government access to encrypted technology.

One of the principle arguments of the technology community was that such a backdoor 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 backdoor more akin to a front door.

As a partial solution, Congress passed the Communications Assistance for Law Enforcement Act (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. 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—the default. This 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.

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 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, a choice between black-and-white. If we take that approach, the only possible 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 vs. 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 to this issue.

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.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

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 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 Congress 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.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. 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.

[The prepared statement of Mr. Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON

For months 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 much bigger than any one entity, device, application, or piece of technology. At its 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 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.

This 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 devastating effects 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 ignoble purposes. 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 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. As we will hear today, this cannot always be offset by alternative means such as meta-data 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 do not have that answer nor do I expect we will find it during this hearing. This is a complex issue and it is going to require some 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 away and they will only get more difficult with time.

Identifying a solution to this problem may involve trade-offs 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 Congress to “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 issue.

In order for Congress to successfully “confront this issue,” however, it will require patience, creativity, courage, and most 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. Therefore, I hope those who were unprepared to participate in this hearing take this to heart and will be part of the solution moving forward.

Mr. MURPHY. The gentleman yields back.
I now recognize Mr. Pallone for 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

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 e-mail 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.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

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 de-

bate. 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. 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 a key to that information. When the tech community tells us that providing backdoors will make their job of protecting our information that much more difficult, we should heed that warning and work toward 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’m happy to work with Congress, with our partners in the private sector, 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 e-mail 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.” He wrote that “Apple would gladly participate in such an effort.”

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 cannot 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.

I would like to yield my remaining time to Rep. 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 cliché 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.

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:]

April 11, 2015

The Honorable Tim Murphy
 Chairman
 Subcommittee on Oversight and Investigation
 Committee on Energy and Commerce
 U.S. House of Representatives

Ref: Hearing Entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives"

Dear Congressman Murphy,

First, let me introduce myself to your committee and provide some basic background and qualifications. I am a forty-five year peace officer and currently the Sheriff of the third largest Sheriff's Office in the Country. I currently serve as Chairman of the Local Executive board for the Greater Houston Regional Computer Forensic Labs and sit on the FBI's National Advisory Board providing local input for the network of seventeen regional computer forensic labs across the country. I have been supervising technical investigators and been involved in such cases for at least twenty years.

In general, the issue at hand is about how to gain access to data stored on electronic devices, ie a cell phone or other portable device with a unique operating system. The government's approach in the case of the phone belonging to the San Bernardino shooters seems to seize the opportunity of a high profile incident with a compelling public interest and a nexus to terrorism to compel technology companies to provide a tool or back door access to the device and its data. Such a tool would seem to bypass the device's immediate limitations to access or locks on the user interface, or front end of the operating system, and gain access to the phone's functionality. Encryption of the actual data layer may be another issue entirely.

Law enforcement has always followed a set of rules surrounding access to evidentiary data authorized under court order on a case by case basis, based solely on the justification provided to a qualified member of the judiciary. Should the justification rise to the level of the issuance of a search warrant in any case, that warrant is always limited to the circumstances specified. This tool would bypass that level of judicial scrutiny. Many believe that the 4th Amendment tenets should remain inviolate and in bypassing this requirement and requiring companies to provide such access would erode the delicate trust we try to maintain with the public. In researching the issue with my staff experienced in the matter, we provide the following:

- 1) Should US Technology companies be forced to install backdoors on their products to permit government access to encrypted data?
 - a) In reference to requiring companies create a product is a very sensitive subject and I know of no place in the constitution which allows for the government to require a

company create a product. This would create a situation in which the company creating the product/back door could arguably be considered an agent of the State. At which point does the 'product' become the Intellectual Property of the State? Will the Government then require the company provide unlimited free updates and new versions? Based on previous records, how will the Government ensure the safety and privacy of the product as it will be disseminated to the various law enforcement agencies? Who will be the keeper of the Key?

- 2) Should Congress weigh in on this matter? Should Congress pass legislation to prohibit a government mandated backdoor?
 - a) There are currently two States (New York and California) in the process of introducing laws which would ban the sale of phones with "full-disk encryption". This piecemeal approach would only serve to create confusion and conflict within the United States. This is one area where a Federal legislative preemptive approach would be better suited. The legislation would be well suited to prohibit States from requiring manufacturer's compromise their product offerings by weakening encryption.
 - b) The Federal Government issues standards and requirements for motor vehicle safety, not the States. By allowing the States to address this issue in different manners would only serve to create a new genre of laws concerning the exportation of encrypted devices among States. By addressing this issue on the Federal level would serve to keep a consistency across States for all manufactures and serve to create a more secure and competitive environment. How would a State disallow a cell phone from say, Texas, to work in a State like California which would require the compromise? Is this something the carrier would be required to monitor and maintain and at what cost to the carrier?
- 3) Should Congress mandate that a backdoor be installed under certain, limited circumstances, such as a warrant requirement?
 - a) This would presume the technology already exist in order to implement, post act, the backdoor on a device. To initiate the inclusion of a backdoor on a device would require the device ALREADY be configured to accept the backdoor. This would mean the device was already in a compromised state. Prior to the issue presented by the FBI, and after the exposure of intelligence agencies acquisition of cellular/digital phone data through the extended use of the FISA courts beyond their initial mandated roles, this issue was a moot point. The fact the court is ultra-secret and has relatively no oversight and no truly viable method to appeal a ruling has created a situation in the public of extreme distrust and 'conspiracy theories' are constantly voiced by the public. Local law enforcement, have taken a direct hit in the ability to obtain information and records due to those actions. While we in local law enforcement have always strived to be transparent and open as to the content and scope of our search warrants for data/access through the accepted use of search warrants, it would seem the DOJ has not and this has created a very real backlash within the realm of privacy. Again, the concept of forcing a company to create a 'back door' is not one path the Congress should tread. By doing so would foster distrust not just between the public and the Government but also between the private sector manufacturers and law enforcement. We must address the issue in a collaborative effort and not in an adversarial one.

- 4) How would the inclusion of a backdoor affect the competitiveness of U.S. technology abroad?
- a) By requiring the creation of a back door to software places American companies in a weaker position in the very competitive global market. This requirement would place our companies in a position of not being providing their customers a truly secure and mature product when overseas competitors in overseas markets are not burdened with this mandate. This would serve to create a situation where companies already struggling to differentiate themselves from the competition would find it difficult not to relocate out of the United States in order to stay competitive in the global economy. The current projected growth in overseas markets is substantially more progressive as global population densities change. Legislating the inclusion of a security compromise erodes the trust in corporate America as those in other countries will always be left wondering if American made products are just an extension of the American Government's intrusion into private communications.
 - b) Another issue which must be discussed is what happens if another Nation State obtains the process and procedures put in place by the US Government. This would now provide those countries with the ability to obtain information from our communications. This does not include the bad actors, including Nation States, from obtaining the information thereby placing US interests in substantial risk.
 - c) By forcing technology companies to provide backdoor access to devices and processes would only serve to weaken the systems in place to protect consumers from identity theft and other technology facilitated crimes. This includes the online market in which all data transmitted across the networks of the carriers is encrypted to protect the end user. To weaken this process only serves to provide a target for criminals and hackers alike. Many users have transitioned to using mobile devices for their banking and financial transactions and rely heavily on the high level of encryption
- 5) What would the implications of a Government-mandated backdoor mean for the U.S. technology in other countries? Would other countries be given the key to the backdoor as well?
- a) Given the current accelerating trend towards more and more secure private communications, technology created in the US would be substantially more vulnerable to outside hacking. If our devices and technology are not secure due to a designed in compromise, other countries and entities will not allow our devices on their networks to process financial transactions. Something as simple as checking your bank account with your phone could theoretically be denied due to a weakness in the platform. For many years, several banks forced the end users to update their computer's web browser because the encryption technology was not sufficient to provide adequate protection against compromise. What will happen when all U.S. Technology providers are required to build in a compromise to their system? Think of it this way, if you take a cell phone from the US with our technology, which includes a built in back door, to another country, it would be like painting a giant red X on it and advertising it as a device with a known weakness which has been built in by the manufacturer. With our devices in a constantly connected state, it is not difficult to envision bad actors spending large amounts of resources and money in order to identify those devices on the network in order to compromise the entire

system. This act of actively seeking those devices could lead to slower networks as they are flooded with traffic probing for their presence.

All of the above answers to the proposed questions are based around mobile device technology. What happens when the Government decides to address these issues in encryption technology in general? Does the Government provide for itself an exemption to the rule of law if one is passed? How does this type of approach directly affect the U.S. financial market as everything transmitted is done with a very high level of encryption to protect the data. Encryption is used in everyday communication both in the mobile telecommunications world and on the Internet. Something as simple as going to www.google.com ends up with encryption technology being employed to prevent others from seeing your web traffic.

From an article on Engadget.com written by Ms. Violet Blue (tinynibbles.com, [@violetblue](https://twitter.com/violetblue)) is a freelance investigative reporter on hacking and cybercrime at Zero Day/ZDNet, CNET and CBS News

<http://www.engadget.com/2015/11/19/lets-have-an-argument-about-encryption/>

"..... even before the Paris attacks, Tim Cook had to patiently explain like a seasoned parent that "any backdoor is a backdoor for everyone. Opening a backdoor can have very dire consequences."

An excellent article from Tech Times

<http://www.techtimes.com/articles/129680/20160202/myth-busters-harvard-edition-harvard-study-makes-compelling-argument-on-encryption-and-going-dark-government-fears.htm>

"A new Harvard study stands by companies that use software encryption in products, explaining that authorities will have abundant amounts of data to feed their surveillance hunger.

The study shows that the ever-growing Internet of Things gives law enforcers access to a myriad of information pertaining to the user of the connected devices. The transformation of traditional households into Smart Homes gave birth to the Internet of Things, which comprises everything from vehicles and smart TVs to IP video cameras, all of which are Internet connected.

"Law enforcement or intelligence agencies may start to seek orders compelling Samsung, Google, Mattel, Nest or vendors of other networked devices to push an update or flip a digital switch to intercept the ambient communications of a target," the report says (PDF)."

Suffolk County DA Daniel Conley has a written testimony, which when researched online, does hold validation even though many in the media world would like to discredit his assertions. He brings to light some of the issues which Law Enforcement face when dealing with encryption on cellular devices.

<http://motherboard.vice.com/read/the-latest-argument-against-apples-new-encryption-its-for-perverts>

"But a Massachusetts prosecutor, who is scheduled to testify at a House hearing on encryption on Wednesday, is taking the arguments a step further into bizarre territory.

If encryption becomes widespread, according to Daniel Conley, the Suffolk County District Attorney in Massachusetts, perverts that take surreptitious pictures of women's intimate parts on public transportation—also known as "upskirting"—will never be prosecuted.

"If the offender's phone can't be searched pursuant to a warrant, then the evidence won't be recovered and this practice will become absolutely un-chargeable as a criminal offense," Conley, who is also a board member of the National District Attorneys Association, will tell the House Committee on Oversight and Government Reform, according to the written testimony he submitted ahead of the hearing.

Conley, however, doesn't mention that the pictures might be in the pervert's cloud storage (phones sometimes have cloud backups turned on by default), which would potentially put them at the reach of police forces. He also doesn't explain how often his district prosecutes these types of cases."

The author of the article obviously has never had to walk in the shoes of an investigator seeking information for a case. He presumes law enforcement would know which cloud storage service to request the information. He apparently has never asked for information from a cloud storage service. Many of the services are now encrypted so the data in the cloud is also not accessible even with a court order. The DA is accurate if the data is not obtainable then the charges may not be considered since there is insufficient evidence to support a charge. This not only happens in 'upskirting' scenarios but many categories of offenses as well. This is the type of misconceptions which are furthered by the media which only serve to make this issue more difficult to bring to a mutually satisfactory conclusion for all parties. Balancing privacy with security has always been difficult.

In relation to the above article with DA Conley we can also add to this list several cases here within the HCSO which have been directly affected by the use of Encryption. One of our investigators is working a case very similar to the above in which a deputy is called out to a scene where the suspect had been observed taking photographs of a young girl under the divider of a dressing room. The deputy arrives on scene and speaks with the suspect and looks at the suspects cell phone. The deputy sees images which would be considered Invasive Visual Recordings (a State Jail Felony) and files the appropriate charges. The deputy then drops the phone as evidence and after an extended period of time the High Tech Crime Unit is notified about the case. An HTCUC investigator retrieves the phone only to find it is locked and running encryption so all the evidence the deputy saw on scene is no longer available for the court. It is an Apple iPhone 4S running IOS 9.

Other notable cases

We have currently have a laptop in relation to a possible suicide/homicide in which the laptop was submitted as evidence. The laptop is a Macbook Pro 15 inch (late 2012) and when we attempted to image the drive using the newest and latest tools designed specifically for Apple products it was noted the laptop is running the newest version of Apples FileVault2. According to the FBI it will take approximately 34 years to brute force the laptop's encryption key using today's supercomputers.

Another case of note is U.S. vs Todd Ewanko. This is the airline pilot whom we arrested in 2010 for the possession of Child Pornography via file sharing networks. When the search warrant was executed we were extremely fortunate the suspect was awake and using his computer at the time. This means he had 'mounted' the drives in his computer – a total of 7 hard drives in one machine – and had opened his encryption program he was using. He finally provided the encryption keys for the hard drives and we discovered more than 26 million images of child sexual assault on his computers. If he had simply turned the computer off prior to answering the door, we would not have any of the evidence.

We also worked a case with the Houston Metro ICAC in which the suspect had only one image of child sexual assault on his main hard drive in his computer and it was only a thumbnail. The suspect refused to provide the password and it was only after the forensics examiner noted a document with a password in it were we able to access the external hard drive which was running encryption and was able to identify the person was sexually assaulting a child inside the residence and taking photos of the assaults. (Pasadena ISD PD Case)

We currently have a homicide case (15-133875) in which the phone is of the suspect who is an unknown but the phone is running IOS 9 or higher and is locked so no access can be made at this time. There are no other viable leads in this case other than data which may be on the phone.

I spoke with the Greater Houston Regional Computer Forensics Lab Quality Assurance Manager on 4-13-2016 and learned 20 percent of the devices presented to the Lab (this includes the devices submitted and those identified at the door as not viable and retained by the lab) are not accessible due to encryption running on the device. Just yesterday (4/12/2016) two devices were declined at the intake process on a very significant case out of Austin due to them being locked and being IOS devices.

The High Tech Crime Unit has processed 247 devices since 08-31-2015 from our own investigators and also outside agencies with approximately 17 devices considered as significant value to the investigation running either encryption or locked beyond our capability to access the underlying data. Significant value means the device is the only viable piece of evidence relative to the case. There were substantially more devices which were locked but ancillary to the investigation and not the main focal point.

During the time period of 2015-2016 (which I could locate in FileOnQ as "phones" in our reporting system since due to coding mismatches I am sure not all phones are listed correctly so

this is a conservative number) the HCSO as a whole took in 1457 phones in reference to cases under some form of investigation. Of the 1457 phones, the HTCUC has processed 125 devices presented to us from HCSO investigators.

It should be noted the number of cases where we expect to see phones locked beyond our current capability to unlock them will substantially increase. This is due in part, our unit at the HCSO is new and the training for processing phones was recently completed. Also of concern is it was with IOS 8 where encryption began to be pushed out "enabled" by default and Apple placed most of the user data under the encryption of the passcode. With IOS 9 a new longer pin code was allowed along with a passcode if desired. This created a more robust security feature and complicated the attempts to brute force a pin code. With IOS 9 Apple initiated the 10 and your done rule where the phone would wipe or brick itself with 10 incorrect pass attempts. The older iPhones were easier to obtain access with the right tools and the right training. As of this year, that is no longer possible.


The chart below is for your reference to the cases where the phone is of significant value to the case.

Device Make	Device Model	Is Phone Unlocked	Password If Provided	Type Of Investigation
ZTE	Z432	YES	N/A	ICAC
APPLE	6 S PLUS	YES	NONE PROVIDED/12399	Death Investigation
APPLE	I-PHONE(A1549)	NO	N/A	Death Investigation
APPLE	I-PHONE 6	NO	N/A	Auto Theft
SAMSUNG	SM-G386T	NO	N/A	Auto Theft
APPLE	A1549	YES	LOCKED	Gang
APPLE	I-PHONE 4S A1387	YES	N/A	Death Investigation
APPLE	I-PHONE 4 A1387	NO	N/A	Death Investigation
APPLE	I-PHONE A1533	NO	N/A	Sexual Assault
APPLE	6 S PLUS	YES	NONE PROVIDED/12399	Death Investigation
LG	LGMS769	NO	N/A	Death Investigation
APPLE	I-PHONE 5	NO	N/A	Death Investigation

APPLE	I-PHONE 6 A1633	NO	N/A	Robbery
APPLE	I-PHONE 5	NO	N/A	Death Investigation
SAMSUNG	SM-G920T	NO	NO	Robbery
APPLE	I-PAD 32GB	NO	NO	Robbery
RCA	RCT 6773W2	NO	NO	ICAC

In conclusion, we might point out that encryption and restricted access is an issue that will continue to confront us and what we must consider is whether the government should, or to what degree, they will play a role in preparing us for that future need for access to data, as well as our ability protect it at the same time.

Sincerely,


 Ron Hickman, Sheriff
 Harris County
 FBI NA #256

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 [continuing]. 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:]



Department of Justice

STATEMENT OF

AMY HESS
EXECUTIVE ASSISTANT DIRECTOR
SCIENCE AND TECHNOLOGY BRANCH
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATION
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

“DECIPHERING THE DEBATE OVER ENCRYPTION: INDUSTRY AND LAW
ENFORCEMENT PERSPECTIVES”

PRESENTED

APRIL 19, 2016

**Statement of
Amy Hess
Executive Assistant Director
Science and Technology Branch
Federal Bureau of Investigation**

**Before the
Subcommittee on Oversight and Investigation
Committee on Energy and Commerce
U.S. House of Representatives**

**At a Hearing Entitled
“Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives”**

**Presented
April 19, 2016**

Good morning, Chairman Murphy, Ranking Member DeGette, and members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss the ongoing challenges encryption presents to law enforcement’s ability to obtain electronic information and evidence pursuant to a court order or warrant.

In recent years, new methods of electronic communication have transformed our society, most notably by enabling ubiquitous digital communications and facilitating broad e-commerce. As such, it is important for our global economy and our national security to have strong encryption standards. The development and robust adoption of strong encryption is a key tool to secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cyber security. We have benefited immensely from digital communication and e-commerce, but with those conveniences come risks and dangers, and we have seen how criminals, including terrorists, also use advances in technology to their advantage. We as a nation are faced with trying to maximize privacy and security, both of which we value as a society.

We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance — not simply because the Constitution demands it — but because the free flow of information is vital to a thriving democracy.

We also have always investigated and prosecuted those wishing to do harm to our nation and its people. As national security and criminal threats continue to evolve, the FBI must continue to work hard to stay ahead of changing threats and changing technology. The more we as a society rely on electronic devices to communicate and store information, the more likely it is

that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. We have seen case after case — from homicides and kidnappings, to drug trafficking, financial fraud, trade secret theft, and child exploitation — where critical evidence came from smart phones, computers, and online communications. Increasingly, some technologies are prohibiting law enforcement from having access to that critical evidence.

The problem, at its base, is one of choices about how to maximize privacy and security to the greatest extent possible. We are not asking to expand the Government's surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress provided to us to keep America safe. There is not, and will not be, a single solution to address the variety of challenges we face. The FBI is pursuing multiple avenues to overcome these challenges; however, it is clear that we cannot overcome these challenges on our own.

For example, one potential approach involves the exploitation of vulnerabilities previously unknown to the device or software manufacturer in order to gain access to information contained within or protected by it. While this is possible in some instances, it is often not a viable solution for law enforcement. Identifying these vulnerabilities and developing lawful intercept or lawful access solutions can take an unacceptable amount of time, require significant skill and resources, and the results of these efforts can be ephemeral, at best.

In order to better protect this nation and its people from harm, we need to be able to access electronic information. When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to identify and stop terrorists who are using social media to recruit, plan and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence. These are not just theoretical concerns.

Malicious actors have taken advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children; and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information.

Terrorist groups, such as ISIL, also use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. Some of these conversations occur over publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters.

We have decisions to make, with our government partners, industry, and the American people. We must find solutions to ensure both the fundamental right of people to engage in private communications as well as the protection of the public. One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds legally sufficient reason to believe that certain private communications contain evidence of a crime, then the Government can conduct a limited search for that evidence. For example, by having a neutral arbiter — the judge — evaluate whether the Government's evidence satisfies the appropriate standard, we have been able to protect the public and safeguard citizens' constitutional rights.

The rules for the collection of the content of communications in order to protect public safety have been worked out by Congress and the courts over decades. Our country is justifiably proud of the strong privacy protections established by the Constitution and by Congress, and the FBI fully complies with those protections. The core question is this: once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime or intelligence that might prevent an attack?

The debate so far has been a challenging and highly charged discussion, but one that we believe is essential to have. This includes a productive and meaningful dialogue on how encryption as currently implemented poses real barriers to law enforcement's ability to seek information in authorized investigations. Mr. Chairman, we believe that the challenges posed by this problem are grave, growing, and extremely complex. At the outset, it is important to emphasize again that we believe there is no one-size-fits-all strategy that will ensure success. We must continue the current public debate about how best to ensure that privacy and security can co-exist and reinforce each other, and continue to consider all of the legitimate concerns at play, including ensuring that law enforcement can keep us safe.

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 device—the computer, the tablet, or the phone—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 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:]



NYPD
New York City Police Department

**PREPARED TESTIMONY OF
CHIEF OF INTELLIGENCE THOMAS P. GALATI
NEW YORK CITY POLICE DEPARTMENT**

**BEFORE THE HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
“Deciphering the Debate Over Encryption:
Industry and Law Enforcement Perspectives”**

APRIL 19, 2016

Thank you 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 has been 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 governmental search and seizure for the past 224 years. It now seems, however, that this legal authority is struggling to catch up with the times.

In today’s world, nearly everyone lives his or her life on a smartphone, and this includes criminals. 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

Written testimony as submitted – Delivered remarks may differ – Page 1 of 4



constraints inherent in the law, but because of limitations in accessibility imposed by technology.

When law enforcement is technologically unable to access evidence necessary to the investigation, prosecution, and prevention of crime, despite the lawful right to do so, we describe it with the term “going dark.” Every day, we deal with this evidentiary dilemma on two fronts.

First, there is what is known as “data at rest.” This is when the actual device—the computer, tablet, or phone—is in law enforcement’s possession, but the information stored within it is inaccessible.

In New York City, in just the six-month period from October, 2015 through March of this year, we have been locked out of 67 Apple devices lawfully seized pursuant to the investigation of 44 violent crimes. These incidents include 23 felonies, ten homicides, two rapes, and an instance in which two officers were shot in the line of duty. The incidents include robberies, criminal weapons possession, criminal sex acts, and felony assaults. In every case, we have the “file cabinet,” as it were, and the legal authority to open it, but we lack the technical ability to do so because encryption protects the contents of those 67 Apple devices. In every case, however, these crime victims deserve our protection.

The second type of “going dark” incident is known as “data in motion.” In these cases, law enforcement is legally permitted—through a warrant or other judicial order—to intercept and access a suspect’s communications. But the encryption built-in to applications such as “WhatsApp,” “Telegram,” “Wickr,” and others thwarts this type of lawful surveillance, because even if the information can be intercepted, it cannot be understood.

NYPD**WRITTEN TESTIMONY FOR THE ECSOI
CHIEF OF INTELLIGENCE THOMAS P. GALATI**

As a result, we may know a criminal group is communicating, but we are unable to understand why. In the past, a phone or wiretap—legally obtained through a judge—would alert the police to drop-off points, hide outs, and target locations. Now, we are literally in the dark. Criminals know it: we recently heard a defendant in a serious felony case make a telephone call from Riker’s Island in which he extolled Apple’s 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 this 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. These corporations 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 is charged with protecting eight-and-a-half million residents and tens of millions of daily commuters and tourists every day—I am confident that corporate CEOs do not hold themselves to the same public-safety standard as our elected officials and law-enforcement professionals.

Given this, how do we keep people safe? The answer cannot be warrant-proof encryption, which creates a landscape of criminal information outside the reach of a search warrant or subpoena, as well as outside the legal authority established over centuries of jurisprudence.

Until 19 months ago, Apple agreed. Until 19 months ago, Apple held the key that could override protections and open phones. Apple used this “master key” to comply with court orders in drug, kidnapping, murder, and terrorism cases. There was no documented instance of this code getting out to hackers or to the government. If they were able to comply with constitutionally legal court orders then, why not now?

NYPD**WRITTEN TESTIMONY FOR THE ECSOI
CHIEF OF INTELLIGENCE THOMAS P. GALATI**

The ramifications of this fight extend beyond San Bernardino, California, and the 14 people murdered there. It is important to recognize that more than 90 percent of all criminal prosecutions in our country are handled at the state or local level. These cases involve real people—your families, your friends, and your loved ones. They deserve police departments that are able to do everything within the law to bring them justice, and they deserve corporations that appreciate their ethical responsibilities.

I applaud you for holding this hearing today. It is critical that we work together to fight crime and disorder, because criminals are not bound by jurisdictional boundaries nor industry standards. They are increasingly aware of the safety net that warrant-proof encryption provides them, however, 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 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.

I would be happy to answer any questions.

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 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:]

Statement of Captain Charles Cohen
Commander, Intelligence and Investigative Technologies
Indiana State Police
April 19, 2016
Hearing Before the Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
United States House of Representatives
“Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives”

Chairman Murphy, Ranking Member DeGette, Members of the Subcommittee:

My name is Chuck Cohen and I am a Captain with the Indiana State Police, responsible for the Office of Intelligence and Investigative Technologies. I also serve as the Indiana Internet Crimes Against Children Task Force Commander and as the Executive Director of the Indiana Intelligence Fusion Center. I have conducted criminal investigations for 21 years. For over 15 years, those investigations have involved internet crimes against children. Internet crimes against children include the production, dissemination, and possession of child pornography, online child solicitation, and online child sexual extortion. While my testimony focuses on this narrow set of criminal activities, the implications are the same for any type of criminal investigation.

During my years as an investigator, I have not seen any impediment to rescuing child victims or identifying and prosecuting child sexual predators that even comes close to the impediment created by encryption. It is a fact that encryption prevents law enforcement from lawfully gathering evidence. Encryption is great if you are a private individual who wants to keep your tax information private, if you work at a doctor’s office and need to keep patients’ medical records safe, or if you own a business whose internal communications relate to the development of highly sensitive intellectual property. I get that, and so does everyone else in law enforcement. I want my information in my personal life to be secure from unauthorized access as much as the next person, but we must not allow ourselves to be blind to the relative harms.

Encryption is necessary, but it is also necessary for criminal investigators to have access to both stored data and data in transit when lawfully authorized.

Put yourselves in the shoes of the parents of a child whom we have just discovered is being victimized online. The victimizer has thousands of photographs of your child in a digital vault that is impossible for law enforcement to open. Your child’s abuser has ready access to the

contraband, but can possess and disseminate it with impunity. Again, the fact is that encryption puts those images of child abuse beyond the reach of law enforcement. In this case, it is the depraved individual harming a child, not society, that benefits from encryption.

Encryption is not new. What *is* new over the last three years is encryption moving from something that people could seek out and deploy if they had the specific desire to conceal information or communication, to something that is being deployed by default into data storage systems including cell phones and hard disk drives, operating systems such as iOS and Android, and communications platforms such as WhatsApp and Viber. At the same time, the encryption has reached a level of technical and mathematical sophistication that often makes it impossible to defeat.

The march to encrypt everything means that more and more evidence at rest on devices and in motion across networks is unavailable to law enforcement by default, no matter what legal demands we obtain.

I have grave concerns that within the next several years, if nothing changes, we will substantially lose our ability to conduct Internet crimes against children investigations as a direct result of the ubiquity with which encryption is being built by default into devices, operating systems, and online communication systems.

Private companies in the United States and around the world have unilaterally decided, without checks and balances, to deploy unbreakable encryption in the most widely used communications devices and computing systems. This threatens to present an insurmountable challenge to local, state, and federal law enforcement conducting a wide variety of routine criminal investigations. Nowhere is this more evident than during the investigations of internet crimes against children since these crimes rely so heavily on technology. That challenge is compounded because of the absence of requirements in the United States for Electronic Communication Service providers and Remote Computing Service providers to retain business records or transactional information.

In much the same way that some countries are viewed both by criminals and law enforcement as safe havens for money laundering and concealing proceeds of unlawful activity due to weak legislation and a lack of regulation, I am concerned that the United States may become viewed as a safe haven for those who sexually exploit and victimize children.

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. Data from the San Bernardino County iPhone was able to be accessed because it was an iPhone 5c with a 32-bit processor. iPhone models that are 5s or newer have 64-bit processors. Essentially, a faster processor can support more powerful encryption. I am aware of no current means available to law enforcement to defeat the encryption of 64-bit iPhones running iOS 8 or higher.

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 to the sensitivity of information that people keep in bank deposit boxes and their bedrooms. While criminal investigators with proper legal authorization have the technical means to access both deposit boxes and bedrooms, we lack the technical means to access new cellular phones running default hard encryption.

Under normal conditions, when there is reason to extract data from a cell phone during a criminal investigation, the first (and usually only) step is to do both logical and physical memory extractions. There are several commercial and custom tools that aid both in the extraction and indexing of the extracted data.

When the phone's data port is destroyed, nonfunctional, the data is encrypted, or the phone has been damaged, the next step is to do a JTAG examination. JTAG stands for Joint Test Action Group. These are the solder points on the motherboard that are used by the manufacturer to test the firmware. So, the examiner solders leads to the JTAG points and uses that connection to extract the data from the memory chip. This method works on many phones. But, this method does not work for encrypted iPhones or phones using encrypted Android operating systems.

When JTAG is not an option, the next step is called an In-System Programming (ISP) examination. This is conducted after determining the location of small circuits on the phone's circuit board and micro soldering hair sized wires to the circuits under microscopic examination. This method also only works on non-encrypted devices.

The forensic method of last resort is a chip-off exam. To do this, a forensic examiner disassembles the phone, de-solders the memory chip from the motherboard, repairs the chip connectors if necessary, and reads the binary data from the chip. The examiner then runs the extracted binary data through software tools to index it. This method also does not work when the memory chip is encrypted.

The only other option we currently have is to attempt brute force methods to correctly guess the passcode. But if the user has set the iPhone to overwrite the data after ten failed password attempts, this method is not possible either.

Apple, as an example, deploys an unbeatable combination of hardware and software encryption on iPhone 5S and higher running iOS 8 and higher. This combination is not found on other cell phones and requires the pairing of the unique memory chip with the unique encryption chip in combination with the key to the software encryption in order to access data. I can think of two reasons why a cell phone or mobile operating system designer would want to do this: to reduce liability and cost by making themselves technically unable to help a government agency seeking assistance; or to outright prevent extraction of data during a forensic examination when someone has physical control of the device and is using advanced hardware and software forensic tools

I have heard some people on news programs and in testimony say that companies should not have to assist the government in trying to obtain evidence on a device because "the government must have some secret way of defeating the encryption."

The short answer is: we do not. I have also heard so-called "experts" say that law enforcement can get everything we need with metadata. The short answer is: we cannot. Asking a detective to use only the metadata to solve an online crime is the equivalent of 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 would not be here today if I was not encountering serious problems that do not have easy technological fixes. We need help, and it is increasingly apparent that this help must be legislative.

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 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.

We have unfortunately reached a point where we now ask investigators for the phone type and operating system before we accept them for analysis in a case. In many instances, we need to tell the investigator that there is nothing that can be done to extract the data from newer 64-bit iPhones and encrypted Android operating system phones. While those phones sit, and while there is no solution, investigations go unsolved and victims go without justice. This challenge is exacerbated when combined with cloud storage encryption and encrypted communication. The bottom line is that we are left with fewer leads to investigate.

Earlier this year, a mother and adult son were shot to death inside their home in Indiana. Both victims had newer iPhones. I am confident that, if they were able, both would give consent for us to forensically examine their phones to help us find their killer(s). But, unfortunately, being deceased they are unable to give consent, and unfortunately for those of us trying to solve their murders, they chose to buy phones running encrypted operating systems. I need to emphasize that we are talking not just about suspects' phones, but also victims' phone; and not just about incriminating evidence, but also exculpatory evidence that cannot be recovered.

Of course we pursue all leads in any investigation, but as we push deeper into the technology and data era, an increasing percentage of the evidence that is critical to any case is in electronic storage somewhere—on a device, on electronic storage media, on a network, or in the cloud. If we cannot get it, then it is harder to generate leads and harder to solve crimes.

It is difficult to determine how many cell phones Indiana State Police forensic examiners are not able to examine due to encryption. That is because when certain combinations of devices and operating systems are encountered during an investigation, they are not even accepted for examination because investigators and examiners know they cannot defeat the encryption either technically or through the service of legal process.

What we do know is that in 2015 the Indiana State Police examined over 1,000 cell phones linked to crimes that were committed. Forensic examiners working for the Indiana State Police estimate that in excess of 40% of all cell phones encountered during the course of Internet crimes against children investigations have encryption that prohibits forensic examination. The requests received for forensic examinations that cannot be serviced due to encryption is constantly increasing. Over 80% of those phones that have been forensically examined during the course of Internet crimes against children investigations contain evidence of the sexual exploitation of children or child pornography. This means that there is a lot of evidence on a lot of phones sitting on our desks right now. And these are serial crimes: the offenders do it over and over again until they are caught. We absolutely know that we could stop pedophiles today if we had access to data on the encrypted phones sitting in our evidence rooms. But we're stuck, and children continue to be victimized.

Another example comes from Burlington County, New Jersey where police are working an active investigation into the manufacturing of child pornography. But police cannot access the data on an encrypted phone that is central to the investigation.

In Guilderland, New York, police have two iPhones that cannot be unlocked that they believe hold critical evidence in a quadruple murder case where four members of a family were killed.

Massachusetts State Police death investigators are overwhelmed with heroin overdoses right now. In several cases they have recovered locked phones which likely contain evidence regarding circumstances of death or the victim's drug supplier, but the data is unobtainable.

Also in Massachusetts, the State Police Computer Crimes Unit, which handles child pornography and physical child sexual exploitation investigations, are increasingly forced to note "phone locked and not examined" in their case reports.

These are a handful among thousands of cases around the country that are currently stymied by encrypted devices. In February 2016, Apple announced that it was going to tie the encryption of iCloud accounts to the device encryption key. It is important to note since Apple currently stores the keys, it can currently comply with the proper service of a search warrant based on probable cause for the contents of an iCloud account. Transferring the key to the device means that Apple will no longer have the technical ability to comply with the proper service of legal process related to iCloud accounts. Moving the location of the encryption key, which Apple plans to do, is different from hardening firewalls, which Apple has not announced plans to do. Hardening firewalls provides additional safeguards from malicious intrusion for customers while still allowing Apple to comply with the proper service of a search warrant.

I have heard the question asked, "Can't the FBI just help state and local law enforcement when encrypted devices or communication is encountered?" The Indiana State Police has some of the most skilled forensic examiners and most advanced hardware and software tools to conduct forensic examinations of digital devices and electronic storage media. I am very familiar with the commercial and proprietary forensic tools available to law enforcement. I can

say definitively that there is no solution for recovering data from many encrypted devices and hard drives. And, I can also say definitively that there is no way to technically obtain the transactional information or communication content from many encrypted communications platforms such as Wickr, WhatsApp, Viber, Telegram, and Skype.

As more platforms, such as Gmail, Yahoo, and WhatsApp move to robust encryption by default, those who investigate Internet crimes against children are truly "going dark."

Unlike many other crimes and contact sex offenses against children, Internet crimes against children can be perpetrated completely online and obfuscated by hard encryption. But, make no mistake, these crimes are devastating to victims and victims' families in ways that are without parallel and are difficult to fully conceive unless you routinely interact with these victim populations. They are also incredibly difficult on law enforcement investigators who spend a significant portion of their time reviewing the evidence and interacting with the victims.

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 the result of encryption. But the investigation, prosecution, and federal conviction of Randall R. Fletcher helps to shed light on the type of evidence being concealed by encryption.

Fletcher lived in Northern Indiana. During the course of an investigation in 2009 for production and possession of child pornography, a computer hard drive with an encrypted partition was seized, along with a separate encrypted hard drive and an encrypted thumb drive. The encryption was robust such that it was not possible to forensically examine the encrypted data. A federal judge compelled Fletcher to disclose his encryption key. Fletcher initially denied remembering the key but failed a polygraph examination on that question. He then provided law enforcement with a passcode that was found to open two of the encrypted containers – the encrypted partition and the additional hard drive – but which did not open 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. Fletcher denied that the thumb drive contained encryption, but his own computer forensic expert disagreed. To date, all efforts to technically break the encryption on the USB storage device have failed. And, to this day, investigators believe that 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 had previously photographed in lascivious poses.

In 1995, Fletcher was convicted of conspiracy to commit murder after he hatched a plan to shoot and kill the mother his then-15-year-old girlfriend. Seven years later, in 2004, while still on probation, Fletcher was found to be in possession of images and videos featuring minor children. By the time he was investigated again in 2009, Fletcher had downloaded encryption software and set about attempting to hide his massive collection containing thousands of child pornography images and videos from law enforcement.

Fletcher is currently serving a 30-year term of imprisonment in a federal facility, to be followed by lifetime supervised release. The encryption used by Fletcher withstood numerous examination attempts and forensic techniques attempted by several law enforcement agencies. There is good reason to believe and it is quite possible that, because of hard encryption on the USB storage device, additional crimes committed by Fletcher have not been investigated and prosecuted and additional child victims have not been provided victim services or access to the justice they so richly deserve.

Unless Congress acts soon to require compliance with a warrant, I anticipate that the choices being made today by technology companies to rapidly move to ubiquitous hard encryption will cripple investigations into the most disgusting of crimes - Internet crimes against children.

The Fourth Amendment protects people "...against unreasonable searches and seizures..." by the government, not against all searches and seizures. Since the founding of the country, if I received a warrant, issued by an impartial judge or magistrate, based on oath or affirmation, specifically describing the place to be searched, and the items authorized to be seized, as a police officer I could serve that warrant. It does not matter how well the residence or business was locked or how strong the safe is, I can gain access. Now, for the first time in the history of the United States, private companies located in the United States and elsewhere are making business decisions, without oversight or checks and balances, to create virtual safes and strong boxes that cannot be opened.

These companies have made unilateral decisions to reach beyond the protections of the 4th Amendment and place evidence of crimes, including child sex offenses, beyond not just unreasonable searches, but against all searches. And, this is clearly a business decision rather than one based on concerns about privacy or civil liberties because it has widely been reported in the media that when certain countries other than the United States require modifications to operating systems, revelation of source code, or modifications to communications platforms, the same companies make certain modifications in order to do business in those countries.

Several factors are working together to create "the perfect storm" such that those who conduct investigations involving child pornography, online child solicitation, and online child sexual extortion are "going dark". Those factors are - in order of impact:

1. data and communication encryption,
2. no U.S. federal law setting retention periods for Electronic Communication Service providers or Remote Computing Service providers,
3. the ability for sexual predators to engage in criminal communication facilitated by companies that are not required to comply with the service of U.S. legal process; and,
4. the unwillingness of service providers to comply with exigent circumstance requests when there is a child at imminent risk, often combined with the

notification of customer suspects when service providers are contacted by law enforcement to make such requests.

I hope that Congress takes the time to truly understand what is at stake with the "going dark" phenomenon and what problems are being created. In particular, please weigh the harms that an encryption scheme that allowed lawful access, even at the cost of some theoretically higher chance of lost data, against the very real human cost in failed investigations that we see across the country.

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 strongly encourage the 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 am happy to answer questions today or at any point in the future.

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 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. 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 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 workarounds 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 usually in 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 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 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. OK.

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 [continuing]. 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 solu-

tions 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 scaleable 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 employ 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. OK.

Ms. HESS [continuing]. 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 DeBrotta, 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. OK. 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 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 unserved.

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 [continuing]. 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, 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 $\frac{2}{3}$ 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 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 bal-

ance 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. 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. 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 governments 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, somehow 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. 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 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 we have the ability to go to them with legal process, and they're providing us with the—

Mr. WELCH. Right.

Chief GALATI [continuing]. 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, 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 [continuing]. 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 [continuing]. 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 ca-

pabilities. 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 opportunities 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 [continuing]. 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 the FBI is exploring the options, I am assuming?

Ms. HESS. We are, yes, sir.

Mr. MULLIN. OK. 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 [continuing]. 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 about 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. 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 cease to be amazed at how complex an issue this is and it requires 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—this is for any of you—about some key questions on this spectrum. 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 an 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 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 the Internet has provided a lot more information to police that we can go out and we can find public records, we can find 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 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 answered that, unless anybody wants to add to what they said.

Yes, Ms. Hess?

Ms. HESS. Yes, sir. I do see that 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 ask obviously that you continue to engage with us to help us answer these questions, not just with what you are saying today but 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 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. OK. 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 5½ years now, and we have been talking about this for all 5½ 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 toward 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.

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. OK. 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 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. OK. 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 [continuing]. 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 [continuing]. 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 we do work very closely with a lot of these companies like Google, and we do share information and also at times work on training among 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 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. OK. 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 the 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 estab-

lishes 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. OK. 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, for—with encryption especially, locking things that we recently were able to obtain.

Mr. HUDSON. Got you. You don't have to—OK. 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. OK.

Ms. HESS [continuing]. 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, the map to find Luke, 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, 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. OK. 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, 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, 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 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 [continuing]. 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 [continuing]. 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—there are varying aspects of that construct, but yes, that premise I would agree with.

Mr. MCNERNEY. OK. Captain, Chief?

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

Mr. MCNERNEY. OK. Basically, it would—

Chief GALATI. I do agree with Ms. Hess that we need to work together. I think we need to have 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. OK. 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 for 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 processors 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. OK. 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 6 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, 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 we go forward of 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 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 [continuing]. 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 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 call 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 a 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. 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 [continuing]. Suggesting?

Ms. HESS [continuing]. 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 gentelady'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 [continuing]. 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.

OK. 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?

OK. 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, 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 $\frac{1}{10}$ 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:]

Statement for the Record

“Deciphering the Debate Over Encryption: Industry and
Law Enforcement Perspectives”

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

Bruce Sewell

Senior Vice President and General Counsel

Apple Inc.

April 19, 2016

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 about encryption.

Hundreds of millions of people trust Apple's 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 steal by breaking into your house.

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 central command center for your car or your home. Many people also use their smartphone to authenticate and gain access to other networks, businesses, financial systems and critical infrastructure. And we feel a great sense of responsibility to protect that information and 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 multi-billion 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 said as many as 21 million people had their records compromised and as many as 78 million people were affected by an attack on Anthem's health insurance records.

The best way we, and the technology industry, know how to protect your information is through the use of strong encryption. Strong encryption is a good thing, 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 subvert, undermine, or weaken generally available commercial encryption software.

At Apple, with every new release of hardware and software, we advance the safety, security and data protection features in our products. We work hard to 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 interactions 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 one-tenth of one percent of our hundreds of millions of users. But all of those users — 100% of our users would be made more vulnerable if we were forced to build a back door.

As you heard from our colleagues in law enforcement, they have the perception that encryption walls off information to 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 is the difference in perspective that we should be focused on resolving. 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.

Thank you for your time. I look forward to answering your questions.

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:]



Written Testimony
U.S. House Committee on Energy & Commerce
Subcommittee on Oversight and Investigations
Amit Yoran
President, RSA, The Security Division of EMC
April 19, 2016

Introduction

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 am the President of RSA, The Security Division of EMC. I have spent over twenty years in the cyber security field. I received a Master of Science in computer science from the George Washington University and Bachelor of Science degree in computer science from the United States Military Academy. I served as the national cyber czar from 2003-2004 and as the founding Director of the US-CERT program. I served on the CSIS Commission on Cyber Security advising the 44th Presidency and am serving on the current Commission developing advice for the next Administration. As an innovator and entrepreneur in the security space, I founded, led and sold two major security companies: Riptech, acquired by Symantec; and NetWitness, acquired by RSA. I also serve as a director and advisor to security startups and sit on several industry advisory boards.

In my current role as President of RSA, I strive to ensure that we provide industry leading cyber security solutions for organizations worldwide.

RSA has been a cyber industry leader for more than 30 years. Our legacy is rooted in tirelessly helping customers solve their most challenging and pressing security problems. The more than 30,000 global customers we serve represent every sector of the economy. Our business enables those we work with to effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately reduce IP theft, fraud, and cybercrime. With a world-class incident response team with expertise, battle-tested processes and sophisticated tools, we have helped hundreds of customers investigate and respond to security incidents and, more importantly, recover from advanced attacks. On a broader scale, we also regularly and rapidly disseminate threat intelligence to our customers in order to empower them to take appropriate measures to protect their company assets from the ever-changing landscape of advanced threats.

Fundamental to RSA's understanding of the issues at hand is our rich heritage in encryption, which is the basis of all security technology, and reflected in our name. RSA solutions work to protect almost every industry and many nations. Our 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.

Industry and Law Enforcement Cooperation

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. My heartfelt sympathy goes to the families and victims of the San Bernardino attacks and the victims of other unspeakable terrorist and criminal acts.

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 technology 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 our laws to be enforced.

A growing number of companies are publishing Transparency Reports that show the number of national security and law enforcement requests they receive and the frequency with which the companies provide the data¹. The data shows tremendous cooperation between industry and law enforcement. Transparency Reports from six companies show they received over 88,000 requests over a one-year period and complied with over 70,000 of them, for a compliance rate of 80 percent.

“Security versus Privacy” Misnomer

The security versus privacy label is sensationalist and emotion provoking. It makes for great headlines, and acts as a looming battle-cry to rally people around the thought that we are all at grave risk if we don't empower our national security apparatus in a way that conflicts directly with our privacy. “Security versus privacy” is an incredibly inaccurate, misleading and dangerous way to describe the debate our society faces over encryption.

Today's debate needs to balance the equities of, on the one hand, the needs of law enforcement to prosecute crimes, sometimes heinous crimes, and, on the other hand, our security, privacy, and economic competitiveness. We do not face an either/or choice between security and privacy. There is a continuum of options that have to be carefully weighed as we consider the thin line that connects these issues.

To be clear, when used properly and in isolated and well-protected systems, strong encryption does make it difficult for law enforcement to access content. Encryption poses a similar challenge to our national security and intelligence community. But it also poses the same challenge to every foreign intelligence service, terrorist, criminal, hacker, industrial spy, and other bad actor attempting to affect our national security, public safety and individual rights. Strong cryptography is a foundational building block for good cybersecurity. We would simply cease to function as a technology-enabled society without it.

¹ Access Now, “Transparency Reporting Index”, <https://www.accessnow.org/transparency-reporting-index/>, (Feb 18, 2016)

Going Dark

We live in a “golden age” of surveillance, more so than in any other point in history. In just about everything we do, we leave an incredibly insightful digital breadcrumb trail. As technologies permeate every aspect of our daily lives, this trail has exploded in a robust and detailed journaling of our activities and communications. Our very interaction with the world around us produces a rich set of data that is continually being transmitted and produces an overwhelming amount of information and meta-data about that information. This meta-data, which is practically impossible to protect, includes information about who you are, where you are, who you are communicating or interacting with, the length, frequency, volume and duration of your communications, what applications you are using, and other troves of information.

While much of this information is constitutionally protected from law enforcement collection, they can, and do, legally gain access to this information, including purchasing it from data aggregators. Law enforcement has an overwhelming volume of information readily available to it, creating challenges to efficiently manage and fully leverage it.

The Cloud and New Computing Paradigms Empower and Enable Law Enforcement

In addition to the meta-data overload, law enforcement can now gain access to raw content at an unprecedented level. Business is transforming faster than ever before. Technology has become the key differentiator in just about every industry, and information is the fuel. Technology has enabled businesses to reduce cost, transform and gain competitive advantage.

The present and future belong to the businesses that have the greatest intelligence and can differentiate their insight. By gaining access to a customer’s information, or perhaps more importantly the information of a prospective customer, companies can simply comb through such data, a process known as data-mining, and produce the most targeted information of the greatest value. This is a practice that each and every one of our industry leading corporations is utilizing.

The new economy uses information to delight us. The magic of the applications we use and the utility and enjoyment we get from them are not on our computer or mobile devices. The power of modern apps and business transcends our computing platforms and occurs in the cloud.

Application providers process it, and sort the unencrypted information in order to deliver the insight we want. For information efficiency and resiliency purposes, unless you very conscientiously make the deliberate effort to evade it, the majority of content you produce or interact with is accessible in a clear text form by the organization you work for and the companies you engage with in your personal capacity. This makes such information readily accessible to law enforcement operating through proper legal channels.

Keeping Information Secret is Really Hard to Do

Good cryptography is really hard to do well, even when it is readily available; algorithms are only a small part of the puzzle. Flaws are constantly being detected in how algorithms are implemented, in key exchange mechanisms, in shared memory or storage, where keys can frequently be found. Even when good cryptography is readily available, protecting information is

incredibly hard to do. There are inevitably flaws in the other moving parts, such as hardware, protocol implementations, operating systems, authentication mechanisms and other components of the computing platform that can compromise information, even if such information is properly encrypted.

We all read about high profile cyber breaches. Thousands of individual hackers are regularly discovering buying and selling exploits that provide unfettered and complete access to computer systems. Given physical access to a device there are expectations that any credible intelligence service or sophisticated law enforcement agency should be able to gain access to the information that resides on that device. If the FBI is unable to do so, they should prioritize developing this organic technical capability to solve the problem.

Law enforcement has phenomenal access to information on an unprecedented scale and is continually increasing its visibility.

Exceptional Access Encryption Creates Exceptional Exposure

Although law enforcement has access to a wealth of insightful surveillance data already, recent and heinous terrorist acts have reinvigorated calls for *exceptional access* mechanisms. These exceptional access mechanisms would enable specified government entities to access the underlying contents of encrypted data even if a third-party encrypted that data. Simply put, this is a call to create a “back door” to allow law enforcement access to encrypted information.

While this request ostensibly sounds simple, it is not only infeasible to achieve, but it fundamentally weakens the security of the Internet infrastructure upon which we all continuously rely, impacting both national security and public safety.

As with any cryptosystem, the greatest challenges exist in implementation and in maintaining effective operational security. The concept of exceptional access encryption directly conflicts with the fundamental design principles of modern encryption and cybersecurity in several ways:

– *Exceptional access mechanisms increase complexity.*

As system complexity increases, so too do the risks of a compromise. In their purest form, security and complexity are typically antithetical to each other. The more complex the system the less safe it is. Each time we add a level or layer of complexity, we add potential for vulnerability. Bear in mind that it can take a significant amount of time and vetting before systems are considered to be secure enough in practice. An exceptional access system will therefore require a more significant incubation period.

– *Exceptional access mechanisms incur operational and procedural risks.*

How would access work? Compromises of even the most sensitive and well-protected systems occur on a regular basis. These are the breaches we see on the news and the world of breaches that we do not even know about. The technical controls and procedures which would be required to govern and audit legitimate access introduce an even greater complexity.

- *Exceptional access mechanisms introduce an extra point of failure.*

Whoever possesses the capability of gaining exceptional access now carries the largest target on their back. They have a need of the greatest magnitude to safeguard their own infrastructure and protect the exceptional access. We have not seen the government demonstrate this exceptional capability to date. A compromise of the “Exceptional Access” method would compromise the effectiveness of the entire system. The result might be massively destructive to society.

- *Exceptional access mechanisms aren't compatible with authenticated encryption.*

The idea behind authenticated encryption is not only to preserve the confidentiality of the underlying data, but also to ensure its authenticity and integrity; i.e., it was encrypted only by the person who had knowledge of the encryption key and no one else could have modified the data. Authenticated encryption is considered a best practice when applying encryption techniques.

- *Exceptional access mechanisms aren't compatible with perfect forward secrecy.*

In other words, if the key is compromised, then all of the data ever encrypted with this key becomes compromised. A more common practice is to negotiate a new key per transaction and use your longer-term key to help ensure the authenticity and integrity of the negotiation process. Each transaction is then encrypted with a fresh key that is discarded shortly after the transaction is completed. An adversary who compromises a given key only learns the contents of a given transaction and not the transactions that preceded it (or any subsequent transactions for that matter).

These are not esoteric or theoretical risks and there are numerous examples of significant systems being exploited as a result of poor cryptographic implementations, even without the added vulnerability of exceptional access. Such “back door” access is significantly more complex and introduces massive additional complexity and risk to our technology infrastructure.

To this end, the entirety of the cryptographic, cyber security, and technology communities has spoken with one unified voice in an unequivocal and unprecedented fashion. Our individual and collective experiences have taught us that from a security perspective, “Exceptional access is an exceptionally terrible idea.”

Requiring Exceptional Access Cryptography Would Likely Harm, Not Improve Our National Security, Intelligence, or Public Safety Capabilities.

Very strong cryptography is readily available outside the United States. A recent [survey](#)² by Bruce Schneier, a fellow at Harvard’s Berkman Center for Internet & Society, demonstrates this very fact: of the 619 entities Schneier identified as selling encrypted products, more than 65 percent are based outside of the U.S., and of the products offered by the non-U.S. companies, nearly half are available for free.

² Bruce Schneier, Kathleen Seidel, Saranya Vijayakumar, “A Worldwide Survey of Encryption Products”, <https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf> (February 11, 2016)

Restricting encryption technology in the U.S. will not make these technologies or known cryptographic methods unavailable. Sophisticated adversaries and criminals, anyone capable of impacting our security, will just create or buy encrypted devices abroad. It is highly unlikely that any credible terrorist or foreign intelligence service would ever use technology that was knowingly weakened or that U.S. intelligence or law enforcement agencies have access to.

If U.S.-based organizations lose customers and market share as a result of enabling some form of exceptional access, U.S. agencies would lose significant visibility into that customer's use cases, meta-data and potential for content. Making matters worse, some countries that historically do not cooperate with U.S. law enforcement and intelligence agencies might purposefully become digital safe havens for end users.

The current Director of the National Security Agency, as well as his predecessors, have stated they do not support a national policy requiring exceptional access encryption.

Weakening Encryption Would Catastrophically Weaken our Nation.

Good encryption is a foundational building block for good cyber security. Without the availability of good encryption, those defending vital U.S. networks and systems would be at a massive disadvantage. We live an era where cyber is consistently cited as the single greatest threat to our way of life. The National Intelligence Estimate and repeated testimonies by James Clapper, the Director of National Intelligence, reinforce this point.

How can we justify a policy that would undermine and disadvantage the already challenging and frequently failing efforts of our cybersecurity practitioners and expect them to keep our industries and us safe? The negative impacts would not only affect tech companies, but every industry, including our critical infrastructures, our audit and law firms, power and utilities, automotive, manufacturing, healthcare, banking and financial industries. An exceptional access policy also runs the risk of further harming U.S. interests on an already suspicious post-Snowden world stage.

While I believe the civil liberties and privacy losses would be significant in the presence of exceptional access, I will leave the articulation of those societal trade-offs for others to expound upon.

Technology and Cyber Industry Engagement

I want to acknowledge the many accomplishments of the Department of Commerce in cyber, including updating the privacy framework, enabling better cooperation between the E.U. and the U.S., the continuous assessment of the NIST Cybersecurity Framework developed hand in glove with industry and now being adopted internationally, and the many standards and best practices that enable the cybersecurity community to build interoperable tools.

Likewise, the Department of Homeland Security has been putting forth a genuine effort to collaborate better with industry and is implementing more efficient information sharing mechanisms.

Policy Considerations

I urge caution with any legislation that would require technology companies to weaken security protocols or provide data to law enforcement in an unencrypted format. The Information Technology Industry Council responded to the discussion draft of the “Compliance with Court Orders Act of 2016,” by stating:

Our ability to constantly innovate and deploy strong security technology is key to protecting not just people’s privacy, but their security – including their physical security. We must constantly innovate to stay at least one step ahead of those who would do us harm. This proposal would actually freeze in place the technology we need for protection, leaving all of us extraordinarily vulnerable.³

Similarly, the Consumer Technology Association (CTA) called the proposed legislation an “overbroad overreaction,” stating: “...requiring access to protected communications would defeat the entire purpose of encryption - opening Americans' data to not only the U.S. government, but also hackers, contentious foreign regimes and other bad actors.” CTA also stated, “former NSA and CIA director Michael Hayden, former Homeland Security director Michael Chertoff and former NSA director Mike McConnell have spoken out against similar proposals and argue that encrypted devices are an important weapon against terrorism.”⁴

As complex and important as this issue is, I am encouraged by the creation of the House Bipartisan Encryption Working Group, which includes members of this committee and the House Judiciary Committee. I believe it is critical for Members to understand all aspects of this debate before putting pen to paper. I would welcome the opportunity to work with the task force as they consider options for ensuring law enforcement has the tools they need to protect us while preserving the benefits of strong encryption.

We also support the Digital Security Commission Act of 2016 (H.R. 4651), which would create a commission of members of the tech community, privacy advocates, and the law enforcement and intelligence communities to work on a solution. Both the Working Group and the Digital Security Commission provide industry, law enforcement, and other stakeholders with a forum to discuss the potential impact of any proposed path forward, legislative or otherwise, and balance their sometimes competing interests.

We also believe it is important for Congress to bear in mind the international precedent that is being set by this discussion. We have already seen a number of countries, including China and France, signal a strong interest in mandating companies create vulnerability in their technology for the purpose of releasing information to them. While these countries have yet to set such a mandate in statute, they are keeping a close eye on the current debate before the U.S. Congress.

As a company, we try to do our part. At RSA Conference, we bring together industry, law enforcement and national security professionals to engage in dialogue and stay abreast of

³ ITI, “ITI Statement on Discussion Draft Regarding Compliance with Court Orders on Encrypted Communications”, <https://www.itic.org/news-events/news-releases/iti-statement-on-discussion-draft-regarding-compliance-with-court-orders-on-encrypted-communications>. (April 8, 2016)

⁴ Consumer Technology Association, “Burr-Feinstein Encryption Bill Overbroad and Threatens Privacy, Says CTA”, <http://www.cta.tech/News/News-Releases/Press-Releases/2016-Press-Releases/Burr-Feinstein-Encryption-Bill-Overbroad-and-Threa.aspx>. (April 11, 2016)

relevant cyber security issues and have been doing so for 25 years. The annual RSA Conferences draw tens of thousands of attendees per year, making RSA Conference the world's largest information security event. This February, speakers at the conference included Attorney General Loretta Lynch, Assistant Attorney General John Carlin and FBI Assistant Director of Cyber Division, James Trainor.

Conclusion

In summary, 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 this issue and not rush to a solution.

Second, law enforcement has access to a lot of information they need to do their jobs. Data is readily accessible to law enforcement operating through proper legal channels. There is a need for a better strategy to manage the quantity and efficiency of the information and analysis. 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 as our society's use of technology evolves.

Third, strong encryption is the basis for good cyber security; if we lower the bar there, we expose ourselves even further to those that would do us harm. Exceptional Access increases complexity and introduces new vulnerabilities. It undermines the integrity of internet infrastructure and introduces more risk, not less, to national interests. Creating a "back door" into encryption means creating opportunity for more people with nefarious intentions to harm us. Back doors into encryption will not address advanced threat actors who pose a material threat to our security. 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 from exceptional access are overestimated.

Finally, 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 US-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, infrastructure, manufacturing, healthcare, defense and financial systems. Weakening encryption would catastrophically weaken our nation.

Simply put, Exceptional Access does more harm than good. This is the seemingly unanimous opinion of the technology industry, academia, national security, as well as all industries that rely on encryption and secured products.

Closing

In closing, I would like to thank Chairman Murphy and Ranking Member DeGette and all members of the committee for their dedication to better understand this complex issue.

I thank you for the opportunity to be here today, and EMC and RSA look forward to working with you and your colleagues in Congress as encryption and cybersecurity topics remain at the forefront of so many policy decisions we face.

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 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. 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 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.

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:]

MATT BLAZE**UNIVERSITY OF PENNSYLVANIA¹****US HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
HEARING ON “DECIPHERING THE DEBATE OVER ENCRYPTION”**

APRIL 19, 2016

Thank you for the opportunity to offer testimony on the important public policy issues raised by cryptography and other security technologies. Since the early 1990's, my research has focused on cryptography and its applications for securing computing and communications systems, especially as we rely for increasingly critical applications on relatively insecure platforms such as the Internet. My work has focused particularly on the intersection of this technology with public policy issues. For example, in 1994, I discovered some fundamental technical flaws with the ill-fated “Clipper Chip”, an encryption system designed by the National Security Agency intended to provide a government backdoor to encrypted communications.

I am currently an associate professor in the computer and information science department at the University of Pennsylvania. From 1992 until I joined Penn in 2004, I was a research scientist at AT&T Bell Laboratories. However, this testimony is not offered on behalf of any organization or agency.

**I. ROBUST DIGITAL SECURITY TECHNOLOGIES ARE VITAL TO PROTECTING
OUR NATIONAL AND CRITICAL INFRASTRUCTURE**

It is difficult to overstate the importance of robust and reliable computing and communications to our personal, commercial, and national security today. Virtually every aspect of our lives, from our health records to the critical infrastructure that keeps our society and economy running, is reflected in or supported in some way by increasingly connected digital

¹ University of Pennsylvania Computer and Information Science, 3330 Walnut Street, Philadelphia, PA 19104. *mab@crypto.com*. Affiliation for identification only.

technology. The influx of new communications and computing devices and software over the last few decades has yielded enormous benefit to our economy as well as to our ability to connect with one another. This trend toward digital systems, and the benefits we reap from them, will only accelerate as technology continues to improve. Preventing attacks against our digital infrastructure by criminals and other malicious actors is thus now an essential part of protecting our society itself.

Unfortunately, modern computing and communications technologies, for all their benefits, are also notoriously vulnerable to attack by criminals and hostile nation-state actors. And just as the benefits of increased connectivity and more pervasive computing will continue to increase as technology advances, so too will the costs and risks we bear when this technology is maliciously compromised. It is a regrettable (and yet time-tested) paradox that our digital systems have largely become *more* vulnerable over time, even as almost every other aspect of information technology has (often wildly) improved. New and more efficient communication technologies often have *less* intrinsic security than the systems they replaced, and the latest computers and similar devices are regularly found to suffer from unexpected vulnerabilities that can be exploited remotely by malicious attackers. Large-scale data breaches and similar security failures have so become commonplace that they now only make the news when their consequences are particularly dramatic.

Serious security failures have become literally a daily occurrence, and it is not an exaggeration to characterize this situation as a national crisis.

Modern digital systems are so vulnerable for a simple reason: computer science does not yet know how to build complex, large-scale software that has reliably correct behavior. This problem has been known, and has been a central focus of computing research, literally since the dawn of programmable computing. As new technology allows us to build larger and more complex systems (and to connect them together over the Internet), the problem of software correctness becomes exponentially more difficult.² Worse, as this insecure technology becomes more integrated into the systems and relationships upon which society depends, the consequences become increasingly dire.

While a general solution to the problem of software reliability and

² That is, the number of software defects in a system typically increases at a rate far greater than the amount of code added to it. So adding new features to a system that makes it twice as large generally has the effect of making it far more than twice as vulnerable. This is because each new software component or feature operates not just in isolation, but potentially interacts with everything else in the system, sometimes in unexpected ways that can be exploited. Therefore, smaller and simpler systems are almost always more secure and reliable, and best practices in security favor systems the most limited functionality possible.

correctness has eluded us (and will continue to do so absent some remarkable and unexpected breakthrough), there are two tried-and-true techniques that can, to some extent, ameliorate the inherent vulnerability of software-based systems. One is the use of encryption to protect data stored on or transmitted over insecure media. The other is to design systems to be as simple as possible, with only those features needed to support the application. The aim is to minimize the “attack surface” that any software vulnerabilities would expose.

Neither the use of encryption nor designing systems to be small and simple are perfect solutions to the software security problem. Even carefully designed, single-purpose software that encrypts data whenever possible can still harbor hidden, exploitable vulnerabilities, especially when it is connected to the Internet. For this reason, software systems must be exposed to continual (and resource intensive) scrutiny throughout their lifecycle to discover and fix flaws before attackers find and exploit them. But these approaches, imperfect and fragile as they might be, represent essentially the only proven defenses that we have.

II. LAW ENFORCEMENT ACCESS REQUIREMENTS INTRODUCE GREAT RISKS

U.S. law enforcement agencies have for at least two decades been warning that wiretaps and other forms of electronic evidence gathering are on the cusp of “going dark”. These fears have been focused chiefly on the potential for criminal use of encryption (which, properly used, can prevent eavesdroppers from recovering communications content), as well as on emerging decentralized communications paradigms, such as peer-to-peer communication, that are not easily intercepted with the same techniques that were used to wiretap traditional telephone calls. They call for developers to incorporate “lawful access”³ features into products and services in order to facilitate wiretapping.

At first blush, a “lawful access only” mechanism that could be incorporated into the communications systems used by criminal suspects might seem like an ideal technical solution to a difficult policy problem. Unfortunately, harsh technical realities make such an ideal solution

³ These law enforcement access features have been variously referred to as “lawful access”, “back doors”, “front doors”, and “golden keys”, among other things. While it may be possible to draw distinctions between them, it is sufficient for the purposes of the analysis in this testimony that all these proposals share the essential property of incorporating a special access feature of some kind that is intended solely to facilitate law enforcement interception under certain circumstances.

effectively impossible, and attempts to mandate one would do enormous harm to the security and reliability of our nation's infrastructure, the future of our innovation economy, and our national security.

A. Access Requirements Make Encryption Vulnerable and Expensive

Let us consider first the relatively narrow problem of ensuring law enforcement access to encrypted communication.⁴ This is perhaps the simplest part of the law enforcement access problem, but it is dauntingly – and fundamentally – difficult to solve in practice without creating significant risk.

Encryption systems encode messages in a way that prevents their decryption without knowledge of a secret, called a *key*. Ordinarily, only the parties to the communication know the key, which can be destroyed and forgotten as soon as the communication has ended and need never be sent to anyone else. In most well designed encrypted communications systems, third parties – including the developer of the software used to perform the encryption and the service providers who operate the infrastructure through which it traverses – do not know or have copies of these keys; the encryption is said to be *end-to-end*, meaning it is conducted entirely between the communicating parties. End-to-end encryption is an important simplifying principle that allows for secure communication even over insecure media. It means that only the endpoints (the computers or devices being directly used by the parties) need to have access to and protect the keys, and the compromise of any other part of the system has no effect on the security of the messages. Securing the endpoints can sometimes be perilously difficult in practice, but it is a much simpler problem than securing the entire path over which messages are transmitted.

Any law enforcement access scheme of the kind apparently envisioned by the FBI would, necessarily, involve a mechanism for the transmission and storage of sensitive secret keys to a third party (whether the government or some other entity that holds it). This approach is sometimes called *key escrow*, *key recovery* or *trusted-third party* encryption; the secret is held “in escrow” by a third party. Key escrow was the widely criticized approach incorporated into the Clipper Chip in the early 1990's. It destroys the end-to-end design of robust encryption systems without any benefit to the application.

There are several fundamental problems with such schemes.

The most basic problem with third-party access cryptography is simply

⁴ Decrypting encrypted communication is only one aspect of the law enforcement access problem as posed by law enforcement, but any access design mandate would, at a minimum, introduce the problems and risks discussed here, as well as others.

that we do not fully understand how to design it securely. Any key escrow or lawful access cryptography system, by its very nature, increases its number of points of failure. Unfortunately, we do not understand the problem well enough to even precisely quantify how this reduces security, let alone identify a safe level for this reduction.

The design and implementation of even the simplest encryption systems is an extraordinarily difficult and fragile process. Very small changes frequently introduce fatal security flaws. Ordinary (end-to-end, non-escrowed) encryption systems have conceptually rather simple requirements and yet, because there is no general theory for designing them, we still often discover exploitable flaws in fielded systems. Adding key escrow renders even the specification of the protocol itself far more complex, making it virtually impossible to assure that any systems using it will actually have the security properties that these systems are intended to have. It is possible, even likely, that lurking in any key escrow system will be one or more design weaknesses that allow recovery of data by unauthorized parties. The commercial and academic world simply does not have the tools to analyze or design the complex systems that arise from key recovery.

This is not simply an abstract concern. Virtually all law enforcement key recovery or key escrow proposals made to date, including those designed by the National Security Agency (the Clipper Chip⁵), have had unanticipated, serious design weakness discovered after the fact.

Frequently, subtle but devastating weaknesses in cryptographic systems and protocols are only discovered long after they are deployed in products and services, which means that sensitive data was at risk from their very first day of use. Law enforcement access requirements make such hidden flaws far more likely to exist.

Aside from cryptographic weaknesses, there are significant operational security issues. Third-party access, by its nature, makes encrypted data less secure because the third party itself creates a new target for attack.

The FBI has not stated whether the cryptographic access mechanisms they desire would be operated centrally or by the vendors of individual products. Either approach creates its own inherent risks and costs. A centralized system becomes a large and highly attractive target, while leaving the task to individual product vendors introduces the likelihood that some vendors will lack the resources to securely manage the keys for their customers or will be specialty targeted for attack by national adversaries.⁶

⁵ See M. Blaze. "Protocol Failure in the Escrowed Encryption Standard". *ACM Conference on Computer and Communications Security*, 1994.

⁶ An alternative, but equivalently risky, design approach involves incorporating a law enforcement access mechanism into the end-user devices that would respond to remote commands from law enforcement to reveal its keys. In this case, managing and securing the

Importantly from a business perspective, the infrastructure to properly support any scheme of this kind would be very expensive to operate.

Even more significant risks arise from the *operational complexity* of managing access to the access keys. Key access centers must presumably be prepared to respond to law enforcement requests for key data on an emergency basis, completing transactions within a short time of receiving each request and without alerting the target of the investigation. There are thousands of law enforcement agencies in the United States authorized to perform electronic surveillance; the escrow centers must be prepared to identify, authenticate and respond to any of them within a short time frame. Even if we imagine relaxing these requirements considerably (e.g., one day or perhaps one week response time), there are few existing secure systems that operate effectively and economically on such a scale and under such tightly constrained conditions.⁷ It is simply inevitable that lawful access systems that meet the government's requirements will make mistakes in giving out the wrong keys from time to time or will be vulnerable to unauthorized key requests. Nation-state adversaries could be expected to be particularly interested in, and adept at, fraudulent access to our law enforcement access services.⁸

B. Access Requirements Make Critical Software Vulnerable to Attack

The vulnerabilities introduced by the cryptographic and operational complexity of introducing law enforcement access are significant; by itself, this should be sufficient reason to render any policy that requires access unacceptably risky. But these are not the only problems. Even more serious, subtle, and difficult to prevent risks arise from the process of integrating the mechanism into the end-user software itself.

As noted above, computer science does not, in general, have the tools to

secret required to remotely issue such commands is essentially an equivalent problem to managing and securing cryptographic keys. The same risks and costs are present in either design.

⁷ Perhaps the closest existing analog to such a system can be found in the law enforcement service centers operated by telephone companies to service wiretap and pen register requests. But these operations do not hold sensitive cryptographic keys of their customers or similar data. They simply act as a clearinghouse and point of contact to which law enforcement agencies serve legal processes. They do not have the problem of managing, controlling access to, or distributing any data as sensitive as cryptographic keys.

⁸ In fact, there have already been several cases where hostile intelligence services have exploited the "lawful access" interfaces in telephone switches. The most famous published case involved the (still unsolved) compromise of a Greek mobile phone carrier. See V. Prevelakis and D. Spinellis, "The Athens Affair". *IEEE Spectrum*. July 2007.

build reliably correct software at scale, and any added requirements or features will increase the likelihood that the system as a whole will suffer from unintended, exploitable, vulnerabilities. Law enforcement access requirements are especially problematic in this regard because of their inherent interaction with the most security-sensitive aspects of the systems that would use them.

As of the time of this writing, the most specific proposal for access mandates is the recently circulated Feinstein-Burr “Compliance with Court Orders” discussion draft. It is exceptionally broad, and would appear to implicate the design of virtually all computing and communications software and hardware. But even under a much more narrowly tailored mandate, ensuring law enforcement access in this way would necessarily add complex requirements to a broad range of consumer, business, and infrastructure-support software. We enjoy today flourishing, heterogeneous software and service marketplace. Everything from small mobile apps that provide instant messaging services to large-scale communication and data storage platforms routinely process communication and stored data that might potentially serve as evidence in criminal cases at some point.

The design approach advocated in such proposals would affect software across the full range of modern computing, from small systems built by startups and entrepreneurs to large platforms managed by multinational corporations, be engineered to incorporate the law enforcement access features, from decentralized and standalone application to centralized, cloud-based services. In small systems, the law enforcement access mechanism could be expected to represent almost as much design and development effort as the underlying function of the software itself. In larger systems, depending on the specifics of the software architecture, the law enforcement access function would have to be designed around and interact with a large number of data management, security, and communications functions.

Compounding the difficulty is the range of different application and service architectures whose designs would have to accommodate integration with the law enforcement access features. Each application would require significant engineering effort, much of which would be highly specific to the particular piece of software. That is, much of engineering effort required to put applications in compliance would not be able to be re-applied to other systems, because each system has its own particular architectural and design constraints. And because the access features are so security sensitive, this engineering work will require the highest quality assurance, testing, and validation, making it a difficult, slow and very expensive process. Doing this properly (to the extent it can be done safely at all) will make the access feature a significant bottleneck to many projects. Given the time and budget

pressures under which many software projects operate, and because the access feature is not directly useful to users, many developers will be able to devote only the minimum engineering resources possible to meet the requirements. The result will be that while the features might work in the sense that they allow law enforcement access, they can also be expected to account for a large proportion of the potentially exploitable defects in the system as a whole.

Incorporating law enforcement access features across even a subset of the most widely used software systems is an extraordinary engineering task, the correctness of which would be crucial for the security and integrity of any data that the software might handle and of the environment in which it will run.

In other words, the risks here come not just from the potential for direct misuse or abuse of the law enforcement access mechanism itself, but from the inevitable introduction of unintentional software bugs that can be exploited by bad actors to bypass the “front door” of the access mechanism entirely and gain access to sensitive user data.

An alternative approach to requiring each software developer to design its own access mechanism is also possible, but would have even more negative effects on the software ecosystem. This would involve the government developing approved software libraries that implement the access mechanism and requiring software developers to incorporate them in their systems. Unfortunately, this scheme would have the effect of essentially outlawing software whose design and architecture is incompatible with the standard official libraries. It would hugely attenuate the innovation that has driven the software economy, and it would still carry most of the risks discussed above.

C. These Risks Would Cut Across Our Nation’s Infrastructure

An important task for policymakers in evaluating the FBI’s proposal is to weigh the risks of making software less able to resist attack against the benefits of more expedient surveillance. It effectively reduces our ability to prevent crime (by reducing computer security) in exchange for the hope of more efficient crime investigation (by making electronic surveillance easier). Unfortunately, the costs of the FBI’s approach will be very high. It will place our national infrastructure at risk.

This is not simply a matter of weighing the desires for personal privacy and for safeguards against government abuse against the need for improved law enforcement. That by itself might be a difficult enough balance for policymakers to strike, and reasonable people might disagree on where that balance should lie. But the risks here go far beyond that, because of the

realities of how modern software applications are integrated into complete systems.

Vulnerabilities in software of the kind likely to arise from law enforcement access requirements can often be exploited in ways that go beyond the specific data they process. In particular, even small hidden vulnerabilities often allow an attacker to effectively take control over an entire system, injecting its own software and compromising the platform as a whole.⁹ The unintended defects inevitably introduced by access mandates such as those discussed in the previous section are especially likely to include vulnerabilities in this category. They are difficult to defend against or contain, and they current represent perhaps the most serious practical threat to networked computer security.

For better or worse, ordinary citizens, large and small business, and the government itself all depend on the same software platforms that are used by the targets of criminal investigations. It is not just potential terrorists, members of the Mafia and local drug dealers whose software would be weakened, but everyone's, including the systems used at almost all levels of government. The stakes involve not just the potential for unauthorized leaks of inconsequential personal chitchat, but also exposure of personal financial and health information, disclosure of proprietary corporate data, and compromises of the platforms that manage and control our national critical infrastructure.

These risks are not merely speculative concerns. There is overwhelming consensus in the technical security community that requirements for "exceptional access" mechanisms such as those being advocated for by law enforcement "open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend."¹⁰

III. THE FOCUS ON DESIGNED-IN ACCESS IGNORES ALTERNATIVES

The cryptography debate is sometimes characterized as a stark, zero-sum choice between privacy and security on the one hand and effective law enforcement and evidence gathering on the other. Fortunately, there appear to be viable alternatives to that permit law enforcement to continue without weakening security.

First, much user data today is stored a multitude of places, typically

⁹ Such vulnerabilities, for example, are how so-called "botnets" used by criminals are able to take control over large numbers of computers on the Internet for sending spam and other fraudulent messages.

¹⁰ See Abelson, et al, "Keys Under Doormats". *Oxford Journal of Cybersecurity*, 2015. <http://cybersecurity.oxfordjournals.org/content/early/2015/11/17/cybsec.tyv009.article-info>

creating multiple copies of evidence in the hands of third parties, such as at “cloud” services that provide backups and remote computing services. When evidence relevant to an investigation is stored in this way, it generally can be obtained by law enforcement under conventional legal processes.

Furthermore, as noted above, the systems we use today, including those protected by cryptography, are not impenetrably secure against sophisticated attack. Indeed, they are often woefully insecure, and are frequently compromised by criminals, which is why access mandates that would make them less secure would be so dangerous. However, this inherent insecurity can, under some circumstances, create opportunities for targeted evidence collection by law enforcement by exploiting preexisting security flaws (which are virtually always present) in the devices used by investigative subjects. With sufficient resources (perhaps beyond those currently available, but well within the potential resources of a national law enforcement agency), such weaknesses can often be exploited to obtain evidence.

An example of the fruitfulness of such approaches can be found in the recent San Bernardino shooting case, in which the FBI sought to unlock an Apple iPhone model 5c used by one of the shooters. Initially, the FBI believed that the device could not be unlocked, but some time after the initial court filings in the case, a targeted technical solution was discovered that enabled the agency to obtain the data stored on the phone without assistance from Apple.

Neither the use of third-party cloud data nor the use of targeted technical attacks against devices will be “one stop shopping” solutions for law enforcement. Each technology and product will be different, and in some cases considerable resources may be required to develop a particular solution. But a systematic, broad, and up-to-date arsenal of technical forensic capabilities, while costly, can be expected to provide a viable alternative to “going dark” in many cases, even as strong cryptography (without any explicit access mechanism) is increasingly used.¹¹

Alternative approaches such as those discussed here have been largely absent from the “going dark” debate.

¹¹ See Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, “Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet,” *12 Nw. J. Tech. & Intell. Prop.* 1 (2014). <http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1>

IV. CONCLUSION

The technical vulnerabilities that would inevitably accompany design requirements for law enforcement access being proposed will harm our security far more than they will help law enforcement. They will provide rich, attractive targets not only for relatively petty criminals such as identity thieves, but also for organized crime, terrorists, and hostile intelligence services. It is not an exaggeration to understand these risks as a significant threat to our economy and to national security.

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 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 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 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 satisfied, 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:]

Before the United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

Testimony of Daniel J. Weitzner, Director
MIT Internet Policy Research Initiative
Principal Research Scientist, MIT Computer Science and Artificial Intelligence Laboratory

Hearing on "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives" -- April 19, 2016

Summary

While recognizing the legitimate needs of law enforcement and challenges raised by increasing widespread encryption, there is now a well-developed consensus among policy-makers and computer security experts that mandating infrastructure-wide back doors is the wrong approach to dealing with the complex intersection of public safety, network security and individual privacy needs. As Congress addresses this important issue, there are several cautions to observe, as well as affirmative steps that can identify positive paths forward. Scientific investigation of current computer security challenges teaches that the last thing policymakers should do is to cause new vulnerabilities to be introduced into the global Internet and mobile device infrastructure. We must also be careful to avoid any new disincentives that would discourage the best possible technical security architectures from being deployed. The challenge of keeping our information infrastructure secure is already so great. We must not put new stumbling blocks in the way.

There will be a temptation to look for a 'one size, fits all' regulatory answer to the complex question before us. The Communications Assistance for Law Enforcement Act (CALEA) was a reasonable way to address surveillance obligations of high-regulated, centralized, national telecommunications companies. However, the highly diverse, global and decentralized firms that make up the Internet platform and mobile industries are a poor fit for this top-down regulatory model. Instead, Congress can find constructive paths forward with careful analysis of specific cases in which law enforcement faces roadblocks, and recognition that any surveillance requirements imposed by courts or legislatures have to scale up to hundreds or thousands of providers. Finally, increased transparency and privacy protection under law will help assure the public that surveillance authorities are subject to effective accountability, committed to respect for user privacy and protection of the underlying security of the global information infrastructure.

Introduction

Thank you Chairman Murphy and Ranking Member DeGette, for inviting me to appear before you at this hearing on encryption, surveillance and privacy. My name is Daniel J. Weitzner. I am Founding Director of the MIT Internet Policy Research Initiative and Principal Research Scientist at the MIT Computer Science and Artificial Intelligence Lab. From 2011-2012, I was United States Deputy Chief Technology Officer for Internet Policy in the White House. My computer science research includes the development of Accountable Systems architecture to enable computational treatment of legal rules and automated compliance auditing. I teach Internet public policy in MIT's Electrical Engineering and Computer Science Department. Before joining MIT in 1998, I was founder and Deputy Director of the Center for Democracy and Technology, and Deputy Policy Director of the Electronic Frontier Foundation.

I. Phase One of the Debate is Over - Infrastructure-wide back doors are a bad idea

This hearing comes at an important time in the broad debate about how best to accommodate law enforcement's legitimate needs for investigative access to Internet platforms, mobile devices and apps. Some in the law enforcement community have suggested that mandating infrastructure-wide back doors would be a reasonable way to meet law enforcement needs. And they hoped that there would be a way to do this without unreasonable security risk. No one should doubt that law enforcement investigators face real challenges in the digital world as a result of the easy availability of strong encryption. Still, even those who are most sympathetic to law enforcement needs are joining the consensus view that infrastructure-wide back doors are too risky to implement. Therefore, the debate is shifting from looking for a "one-size, fits all" solution to a more nuanced assessment of how to address the complex challenges faced by law enforcement while supported continued strengthening of Internet security measures.

Following initial calls from FBI Director James Comey and UK Prime Minister David Cameron for infrastructure-wide back doors, a group of cryptographers and computer security experts came together to evaluate the technical security impact of such an approach. We found that mandatory, infrastructure-wide exceptional access would cause three fundamental problems. First, providing exceptional access to communications would force a U-turn from the best

practices now being deployed to make the Internet more secure.¹ These practices include forward secrecy—where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications.

Second, building in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security—every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world. One might hope that the encryption problem could be ‘solved’ with a single, top-down approach much as CALEA did for traditional telecommunications systems. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services, which tend to use similar technologies and are more likely to have the resources to manage vulnerabilities that may arise from new features. Features to permit law enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious—making security testing difficult and less effective.

Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. Moreover, law enforcement’s stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple key holders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the U.S. Government Office of Personnel Management (OPM) show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data

¹ Keys under doormats: mandating insecurity by requiring government access to all data and communications. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, Daniel J. Weitzner
Journal of Cybersecurity Nov 2015.
<http://cybersecurity.oxfordjournals.org/content/early/2015/11/17/cybsec.tyv009.full>

because OPM had insecure infrastructure. If service providers implement exceptional access requirements incorrectly, the security of all of their users will be at risk.

In response to these arguments and related views from computer security experts around the world, the new phase of the debate is characterized by a growing acceptance that mandatory, infrastructure-wide back doors are a bad idea. In the more than six months since our article was first published in a peer-reviewed journal, we have only been able to find one academic computer scientist who has questioned our finding.² In a blog post, a well-respected Dutch computer security researcher accepted most of our arguments but indicated that we had not proved that it is absolutely impossible to build secure exceptional access systems. Still, he implicitly agreed with our stated view that it is very hard and therefore very risky.

Political leaders from around the world are now publicly rejecting the idea of mandatory back doors. Recently, US Secretary of Defense Ash Carter offered his view at the RSA Conference:

As we together engineer approaches to overall human security in the information age, I know enough to recognize that there will not be some simple, overall technical solution—a so-called 'back door' that does it all.... I'm not a believer in backdoors or a single technical approach. I don't think that's realistic.

Last month, Robert Hannigan, Director of the UK's GCHQ (the lead UK government surveillance agency) gave a talk at MIT—entitled "Front Doors and Strong Locks: Encryption, Privacy and Intelligence Gathering in the Digital Era"³—on his views of the evolving issues of encryption and surveillance. His message was clear: It does not make sense to ban or weaken end-to-end-encryption, nor does he favor 'backdoors' in the infrastructure. But he believes the obstacles posed by encryption are a "moral challenge" that society, broadly speaking, must face. Hannigan's emphasis on GCHQ's information assurance mission makes clear that companies should only be required to offer assistance in a manner that avoids creating security risks. As he says,

² The second crypto war is not about crypto, Jaap-Henk Hoepman.
<https://www.cqure.nl/kennisplatform/the-second-crypto-war-is-not-about-crypto>

³
http://www.gchq.gov.uk/press_and_media/speeches/Pages/hannigan-speech-at-mit-front-doors-and-strong-locks.aspx

Much of GCHQ's work is on cyber security, and given the industrial-scale theft of intellectual property from our companies and universities, I'm acutely aware of the importance of promoting strong protections in general, and strong encryption in particular. The stakes are high and they are not all about counter terrorism.

Adding that he is "accountable to our Prime Minister just as much, if not more, for the state of cyber security in the UK as I am for intelligence collection," he is outright opposed to mandatory back doors:

The solution is not, of course, that encryption should be weakened, let alone banned. But neither is it true that nothing can be done without weakening encryption. I am not in favour of banning encryption just to avoid doubt. Nor am I asking for mandatory backdoors.

Speaking⁴ with US Secretary of Commerce Penny Pritzker, European Commission Vice President Anders Ansip repeated his opposition to weakening encryption with mandatory back doors. Ansip argued that people simply will not trust systems that have built-in governmental controls. Drawing from his experience as the Prime Minister of Estonia who famously digitized much of the government, he observed that over two-thirds of Estonian citizens vote online. "How will they trust the results of the election," VP Ansip asked, "if they know that the government has a back door into the technology used to collect citizen's votes?"

These statements from US, UK and EU government officials demonstrate that our underlying technical analysis against mandatory back doors in Keys Under Doormats has been largely accepted.

II. Cautions going forward

The debate has moved beyond the false, binary choice that would have us either aim to guarantee the success of all law enforcement surveillance requests, and ignore the broader security impact, or at the other extreme, simply declare that law enforcement is entirely on its

⁴ <http://webcast.amps.ms.mit.edu/spr2016/DOC/1610/5.html>

own in the age of strong encryption. Moving forward, how should policymakers address the important interests of law enforcement, security, privacy and global competitiveness? It will remain important to avoid mandating technical security vulnerabilities as even small security gaps can spread and cause widespread damage. And we must avoid creating undue burdens on efforts to make our infrastructure more secure, so we can meet challenge of designing and maintaining our global information infrastructure with strong confidentiality, resilience, and reliability.

A. Avoid mandating technical security vulnerabilities that can easily propagate throughout the entire global Internet infrastructure

Some law enforcement arguments calling for exceptional access suggest that that Apple and Google's increased focus on encryption is not actually about increasing the security of the device; that this push is a marketing ploy for privacy conscious users in the post-Snowden era. Mobile devices appeared to function perfectly well before the switch to full disk encryption, so why change now?

The history of computer security shows that the push to ubiquitous encryption is well motivated by the litany of systemic vulnerabilities resulting from hardware and software vendors failing to encrypt and/or cryptographically verify data. Further, the damage from failures to properly encrypt data has historically been exacerbated by the slow and arduous pace of eliminating bad code once it has been added to the overall software ecosystem. The combination of these two factors has led the security community to advocate for applying encryption and authentication to as much as is possible, since failing to do so has been repeatedly shown to cause serious damage to user security and privacy.

One of the points of contention between Apple and the FBI in the San Bernardino case is whether Apple can be compelled to 'sign' a new version of the Apple iOS operating system whose function is to enable law enforcement access to the locked phone. Code-signing is an important security technique that prevents malicious software from running on a user's device. Before the FBI found an alternative method to break into the phone, they sought a court order to force Apple to sign the code, thereby enabling that version of iOS to run on the seized phone. Apple users rely on the company to only sign code that is safe for use. While Apple's refusal to agree to sign a weakened version of iOS was a stumbling block for the FBI, it is also a means of

protecting the integrity of the code-signing mechanism is essential to the security of all iPhone users. Failing to cryptographically verify updates through this code signing process can lead to developer's software being subverted to spread malware. Flame, a sophisticated nation-state malware campaign discovered in 2012, exploited Microsoft Update's outdated cryptography to infect Windows PCs.⁵ Apple failing to cryptographically verify updates to iTunes turned the program into an infection point for the FinFisher virus,⁶ which was then found to be in use by oppressive governments spying on local dissidents.⁷ Most recently, an update framework used by hundreds of OS X apps was found to be vulnerable to these exact same sorts of attacks, leaving thousands of users at risk of losing complete control of their computers, including anything they access on that device --- bank accounts, private chat, email accounts, health records, and social media.⁹

Another class of attacks involve the interception of account information from websites or apps that do not encrypt their data in transit. For instance, as recently as 2010, major websites including Facebook, Google, LinkedIn, and Reddit failed to encrypt connections to their sites using HTTP over the TLS/SSL secure transport protocols, known as HTTPS. This failure made those sites vulnerable to "session hijacking attacks" that allowed attackers watching the network to gain access to user accounts. Such attacks were not difficult to execute, for instance, an easily installable Firefox plugin called Firesheep allowed anyone in the vicinity of an unencrypted wifi connection to gain access to unsuspecting users' email, social media, and bank accounts with a literal click of a button.¹⁰ To see how far-reaching this vulnerability could be, think of all the times users connect to an untrusted airport wifi hotspot to download an app, to check email, access health records, or converse with friends. Strong encryption makes it possible for that user to do so without needing to fully trust the myriad of devices and organizations between his or her device and the service being accessed. Conversely, without encryption, a malicious middleman such as the wifi router owner, the Internet service provider, or a disgruntled network administrator could easily gain control of an unsuspecting user's computer or bank account.

⁵ <http://arstechnica.com/security/2012/06/flame-malware-hijacks-windows-update-to-propagate/>

⁶

<http://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent-fake-itunes-flash-updates-documents-show/>

⁷ <http://www.bbc.com/news/uk-34529237>

⁸ <http://bits.blogs.nytimes.com/2012/08/13/elusive-finspy-spyware-pops-up-in-10-countries/>

⁹ <https://vulnsec.com/2016/osx-apps-vulnerabilities/>

¹⁰ The tool, called Firesheep, allowed amateur attackers to gain surreptitious access to unsuspecting users' Facebook, Reddit, Gmail, Yahoo, and Twitter accounts. <http://codebutler.com/firesheep/>

Computer security architects are inclined to advocate the widest possible deployment of cryptography in the infrastructure because it is impossible possible to know in advance what applications and services will require strong security or how the threats may evolve. For instance, even a few years ago, code signing, full-disk encryption, and HTTPS were viewed as tools only for high-security applications. Today, any company that did not use code signing for software updates, HTTPS for their ecommerce websites, or full-disk encryption for their employee laptops would be compromised in short order.

Inadequate computer security design choices, like absent or out-of-date cryptography, stick around for a long time and are hard to clean up once deployed in the infrastructure. The Flame virus infection vector, cited above, was caused by Microsoft's use of an outdated cryptographic primitive that had been shown to be flawed more than five years before.¹¹ Even when developers produce patches for bad crypto, users might not switch over for compatibility reasons --- the TJ Maxx intrusion, which cost that company upward of \$250 million, was caused by their use of a woefully outdated encryption scheme (WEP) on one of the company's wifi access points. Finally, a 2013 study by the University of Michigan found that tens of thousands of websites were using outdated cryptographic primitives such as weak keys and other easily avoidable misconfigurations.¹²

It follows that one of the major concerns with exceptional access capabilities is that the bugs they inevitably introduce will be difficult to fix. It is important to note that this is not a theoretical problem: Past forays into regulation mandating weakened encryption for foreign export during the early 90s, so-called "export-grade encryption," resulted in the 2015 FREAK class of vulnerabilities, which in turn led to roughly 12% of the top million most visited websites being interceptable, including usajobs.gov and americanexpress.com. FREAK worked because a malicious middleman could force the use of weak export grade cryptography in cases where both the browser and the server happened to still support the outdated protocol,¹³ which had unfortunately been kept around for backward compatibility even after the export cryptography regulation had been lifted.

¹¹ The first known practical break of md5 happened in 2005, and Flame was found in 2012.
<http://eprint.iacr.org/2005/067>

¹² <https://jhalderm.com/pub/papers/https-ipc13.pdf>

¹³ See FREAK and DROWN (<https://freakattack.com/>, <https://drownattack.com/>)

The damage caused by flaws in cryptographic implementations is compounded by the fact that these cryptographic systems are extraordinarily interdependent at the operating system and application level. Writing good crypto code is difficult. Correct implementation of cryptographic algorithms requires deep theoretical computer science and systems-level knowledge, applications almost always rely on third-party libraries or services to encrypt both data at rest and in transit. In fact, the difficulty in implementing cryptography has led to very few implementations of these frameworks; for instance, almost every Android device uses one of two libraries.¹⁴ Bugs introduced in such cryptographic frameworks (like Android's libraries) would therefore proliferate to vulnerabilities in seemingly unrelated apps (like your banking or email app).

These factors show that vulnerabilities introduced by weakening encryption, including mandating exceptional access, will propagate widely and could cause widespread, hard-to-measure damage. Vulnerabilities introduced by weakening encryption, including mandating exceptional access, will propagate to a wide range of security-critical applications. Therefore mandating exceptional access or other system-wide vulnerabilities is tantamount to mandating chronically vulnerable devices and services.

B. Avoid introducing disincentives to using secure systems development practices

Any proposed regulation on encryption must take into account the chilling effect on adoption and continued use of good security procedures. Incentivizing good security is already quite hard. Today, though cryptography is relatively unfettered by regulation, there are nonetheless disincentives for businesses to properly secure their users' data. It would be reasonable to assume that adding more disincentives would risk causing the rapid abandonment of these otherwise beneficial security procedures.

The difficulty of using cryptographic tools both in development and by end-users are well known in computer security research. A 2013 study of the Google Play app store found that, of 11,748 different applications tested, only 1,421 (12%) made correct use of the cryptographic libraries available, leaving many apps vulnerable to known bugs.¹⁵ Users have encountered similar

¹⁴A great paper on the state of cryptography on Android is "An Empirical Study of Cryptographic Misuse in Android Applications" by Egele et al. Indeed, the paper finds that the vast majority of app developers fail to use these libraries properly. https://www.cs.ucsb.edu/~chris/research/doc/ccs13_cryptolint.pdf

¹⁵ https://www.cs.ucsb.edu/~chris/research/doc/ccs13_cryptolint.pdf

difficulties, often making it rational to ignore encryption and security advice in order to more easily complete daily goals.¹⁶

In addition to user and developer and user error, device manufacturers must deal with physical limitations --- battery life and processing speed can be drastically affected by the use of encryption, which is only ameliorated by use of specialized, currently more expensive hardware. Google, for instance, backed away from forcing full disk encryption on all devices citing battery life and usability as concerns.¹⁷

Regulation will compound the above disincentives. Imagine a burgeoning tech startup deciding whether or not to spend the time and capital to properly encrypt their services, or to encrypt their data at rest. Without having to worry about compliance, the company's choice is somewhat straightforward --- it will be more likely to bake security in from day one since a high-profile failure will damage their brand. However, with regulation, that same company runs a risk of accidentally running afoul of government-mandated of exceptional access requirements.

Amazon, far from a struggling firm, recently decided to remove full-disk encryption from their Kindle Fire, almost immediately after the FBI brought suit against Apple in San Bernardino.¹⁸ It is unimportant whether such concessions are due to fear of government lawsuits or the technical issues --- either way they demonstrate that even the best-resourced companies have competing incentives about implementing full-disk encryption on their devices.

C. Avoid top-down regulatory approaches - they are likely to fail in the global Internet environment

As this Committee considers how to address the very real needs of federal, state and local law enforcement to conduct investigations in the digital environment, examination of existing regulatory models in the law of electronic surveillance can be helpful in identifying models to adopt and models to avoid. As a case in point, there have been calls over the last several years calls¹⁹ to address this difficult question by simply extending the Communications Assistance for

¹⁶ <http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf>

¹⁷ <http://www.theverge.com/2015/3/3/8143607/android-lollipop-default-disk-encryption-performance>

¹⁸ <http://motherboard.vice.com/read/amazon-removes-device-encryption-fire-os-kindle-phones-and-tablets>

¹⁹ <http://www.cnet.com/news/fbi-to-announce-new-net-wiretapping-push/>

Law Enforcement Act (CALEA)²⁰ to apply to Internet companies. But close examination of CALEA in the context of today's digital surveillance challenges shows just how hard it would be "solve" these problems with the top-down regulatory approach used in CALEA. CALEA was drafted to address the conduct of a very small number of traditional telecommunications companies all of which were subject to (then) stable and well-understood regulatory authority of the FCC. No such regulatory control exists for the Internet and mobile industries. The companies under CALEA's purview are all mature, US-based companies with slowly-evolving products largely focused on the domestic marketplace. By contrast, the services at the heart of the FBI's challenge today are rapidly evolving in scale, scope and location in the world. Finally, while CALEA's regulatory structure is complex, its goal is simple - preserve status quo surveillance capability. The deep uncertainty about the constitutional scope of surveillance authority in the Internet and mobile environment as a result of rapid evolution in new services means that drafters of a new law would have no stable surveillance goal around which to build a statute.

First, CALEA targeted the behavior of the traditional telecommunications industry, which was already regulated by Congress under the Communications Act under the Federal Communications Commission. Companies providing the telecommunications services regulated by CALEA had a clearly defined relationship with the regulatory agency so legislative drafters could use the FCC as a mechanism for defining rules under clear statutory guidance. Having an expert agency in place to adjudicate the scope of CALEA's applicability to evolving telecommunications services has been critical to assure that the goals of the statute are satisfied as telecommunications services evolve. The FCC has a vital role both in assuring that carriers meet their obligations so that the Congressional goals of protecting innovation, privacy and security are met in the face of changing technology. In sharp contrast, the vast majority of products and services of concern to law enforcement -- from smartphone hardware devices to operating system software to apps and web-based services -- are largely unregulated by the FCC. Broadly speaking, the Internet and mobile industries, by contrast, do not fall under the purview of any single statute or regulatory agency. So even if Congress were to extend specific law enforcement assistance requirements to Internet platforms and mobile device industries, it is not clear how those requirements could be formulated to assure the proper balance of effectiveness and flexibility.

²⁰ 47 USC 1001, *et seq.*

Second, the telecommunications industry regulated under CALEA was made up of mature companies provided stable, highly standardized and slow-to-change product offerings. The fact that all of the major telecommunications carriers offered more or less the same kind of services meant that Congress could write one common set of rules for CALEA compliance that would apply in a coherent way to all telecommunication services. CALEA drafters, including this committee, were especially concerned that Congress avoid dictating specific technology so only wrote functional requirements into the statute.²¹ However, this created some risk that neither the industry nor law enforcement would know whether a specific technology or service was actually CALEA compliant. To strike the right balance between law enforcement needs for effective access and industry needs for compliance certainty and technical flexibility, Congress created a safe harbor mechanism by which industry could work through its own technical standards bodies to develop technical standards the defined CALEA compliant services.²² Any company complying with these industry standards is presumed to be in compliance with the statute unless law enforcement specifically challenges the design of those standards. In this way, industry is free to design its own technology and still have certainty that is complying with the law. The fact that there was one main technical standards body that defined the standards for basic telecommunications services was key to statutory architecture of CALEA.

In sharp contrast to the standards-drive development of the telecommunications industry, many of the innovative new services offered by today's Internet platforms, mobile device makers and apps developers are introduced into the market long before they can be standardized. They represent a highly diverse set of companies which varied and highly competitive business models. Product and service offering change rapidly. Of course this is one of reasons way law enforcement faces real challenges in this area. While the Internet and the Web depend on technical standards for global interoperability, those standards are much more generic in nature and do not tend to define full product offerings.

Finally, CALEA was aimed solely at assuring the preservation status quo surveillance capabilities - access to voice communications service that had been functionally unchanged since the original federal wiretap laws were passed in the 1960s. By contrast, the wealth of information available on today's smartphones and other Internet communications and information

²¹ 47 USC 1002(a)(1)-(4).

²² 47 USC 1006(a).

applications is vast and still growing. Everything from exchange of photos, video, personal financial data, real time health monitoring, and location data are available in today's advanced Internet environment. Defining what data should and should not be available to law enforcement will be a complex and ever-changing task. All of these factors give rise to serious doubt as to whether it will be possible to develop and impose a single, top-down regulatory framework to address the wide range of applications and services in which law enforcement could face surveillance challenges.

Even if some regulation existed that maintained security while providing law enforcement access, it is unlikely that the US alone could limit the use and distribution of encryption software. In the years since the years since CALEA was enacted and the Internet marketplace has exploded around the world, the ability for US regulation to control the global availability of encryption software has declined dramatically. A recent study by Harvard's Berkman Center showed that a vast number of products providing cryptographic services originated overseas, including a number of secure messaging and email applications.²³ Any law enacted in the US would therefore only cover a small subset of current encryption apps and have little ability to prevent the development of strong security products abroad. Consider Github, a global social network for collaborative software development, which boasts a userbase of over 14 million developers and 35 million projects.²⁴ That same site has over 32 million visitors per month, only about a quarter of which are from the US.²⁵ Once source is shared over such services, it can easily be modified, strengthened, or examined for bugs by programmers from all over the world.

III. Finding a constructive way forward

None of the cautions above in any way diminish the real need that law enforcement has to be able to investigate crimes and gather evidence toward convicting those who break the law. As this committee and the House Judiciary Committee move forward with exploration of this issue

²³ https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html

²⁴ <https://github.com/about/press>

²⁵

<http://venturebeat.com/2015/06/17/github-by-the-numbers-32m-people-visit-each-month-74-from-outside-the-u-s-36-from-europe/>

through the encryption working group²⁶ announced last month, addressing the following issues can help identify constructive paths forward.

A. Learn from law enforcement cases

As the pace of law enforcement investigations involving smartphones and other platforms with strong encryption moves forward, there will be much to learn about the nature of the challenges faced by law enforcement, about judicial responses to law enforcement requests for assistance, and about the means chosen to collect information necessary for investigations. Most notably, there will be those cases where enhancing law enforcement technical sophistication can alleviate the need for court orders compelling company assistance. The encryption task force should learn as much as possible about this class of capabilities. Key issues to explore include:

- How can federal law enforcement agencies develop increased online digital investigative prowess? In this regard I strongly endorse the recommendations made by my colleague Susan Landau, Worcester Polytechnic Institute, in her testimony on this issue before the House Judiciary Committee on March 1 of this year. Prof. Landau calls for increased resources to assist the FBI in online digital investigations and forensics.²⁷
- In what circumstances will technical assistance from Internet platform, mobile device and apps vendors be needed?
- Of the assistance requests made through the court system or privately between law enforcement and tech companies, what types of requests create risk to the security and privacy of the infrastructure as a whole and what types of assistance can be provided with low security and privacy risk? Answering these questions requires access to detailed information about the nature of these assistance requests, much of which is under seal.
- As the locus of criminal activity moves more to Internet and mobile platforms, to what extent does good access to metadata, including location information, personal health monitoring information, and other Internet-of-Things related sensor data provide alternatives to law enforcement when they are not able to get access to the encrypted content of communications? We know from computer science research that careful automated analysis metadata can be even more revealing than content. New analytic techniques have shown that even without access to the content of communications it is

²⁶

<https://judiciary.house.gov/press-release/goodlatte-conyers-upton-pallone-announce-bipartisan-encryption-working-group/>

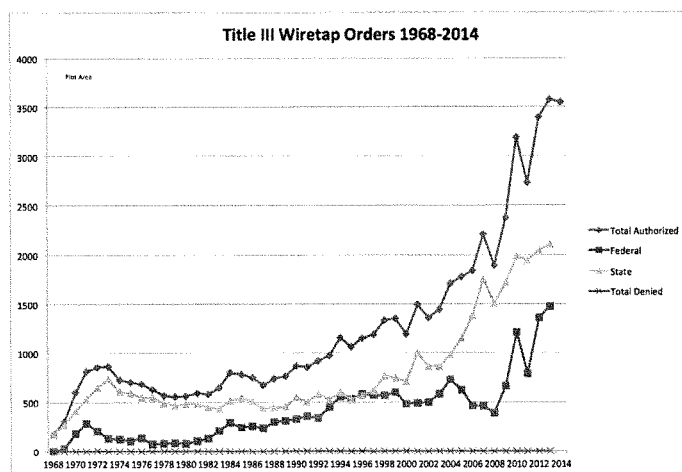
²⁷ <https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf>

possible to infer to a very high degree of accuracy a subject's close associates, the identify of intimate partners²⁸, typical patterns of daily travel,²⁹ sexual orientation,³⁰ and other details of private life.

B. Plan for scale

Any long run policy governing the scope of assistance required of tech companies must account for the likely large number of those requests across the country, and the world. As awareness of law enforcement assistance requests moves beyond the request to help with "just one phone," we must consider how an assistance request would look if it were repeated ten, one hundred, or one thousand times.

Figure 1



Source: Administrative Office of the US Courts, Electronic Privacy Information Center

²⁸ Backstrom, Lars, and Jon Kleinberg. "Romantic partnerships and the dispersion of social ties: a network analysis of relationship status on facebook." *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. ACM, 2014.

²⁹ Gonzalez, Marta C., Cesar A. Hidalgo, and Albert-Laszlo Barabasi. "Understanding individual human mobility patterns." *Nature* 453.7196 (2008): 779-782.

³⁰ Jernigan, Carter, and Behram FT Mistree. "Gaydar: Facebook friendships expose sexual orientation." *First Monday* 14.10 (2009).

The rate of growth of electronic surveillance requests as shown in Figure 1 suggests that the suitability of any policy will be judged in part based on how well it scales to large numbers of requests. Consider that most of the individual All Writs Act cases in which the FBI seeks assistance from mobile device manufacturers appear to be one-off requests. However, if those cases gave rise to a general rule requiring such assistance, then those companies would have to design systems to respond to large numbers of requests at a time. While a single order to assist might pose only low security risk, building systems to respond to repeated requests could substantially increase the risk that security sensitive software or private keys might leak out to hostile adversaries. Understanding the nature of these risks requires careful analysis of the nature of the rules derived from these court orders and the design of the systems put in place to enable expeditious response.

C. Rebuild public trust

One of the many lessons to be learned from the last few years of debate about surveillance, privacy and security policy is that the public harbors serious doubts about whether they can trust either industry or government to respect individual privacy. According to the Pew Research Center, 65% of the country believes that there should be stronger limits on government surveillance.³¹ And even before the Snowden revelations, more than half of smartphone users uninstalled an app because they were concerned about how information was going to be shared.

³² So a significant portion of the public perceives a real gap in the degree to which the legal system protects them from unwanted privacy intrusion.

Two measures can help close this trust gap and reduce the public anxiety about lawful government surveillance. First, Congress should provide for the maximum feasible transparency regarding legal surveillance orders and operations. As the scope of surveillance grows and given the likely increase in lawful hacking, it is important that the public and policymakers have full visibility into surveillance practices. That visibility is required in order to provide accountability and give policy makers the information necessary to keep surveillance law updated in the face of new technology and changing investigative practices. Second, Congress should continue its efforts to modernize civil liberties and consumer privacy protections in light of advancing technology. The House Judiciary Committee's recent action to provide greater protection for

³¹ http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf

³² <http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/>

private information stored in cloud computing services will offer the public welcome new assurances of basic digital privacy rights. And there are numerous uses of citizens' personal information by the commercial sector that deserve stronger legal privacy protections. Personal data collected from mobile devices, personal health monitor, home environmental monitoring and many of sources are being used in a growing variety of innovative new services. We should welcome these new services but also recognize that citizens deserve clear privacy protection in these arenas. By providing clear privacy rules of the road, Congress can ease individual privacy anxiety as to both commercial and government uses of personal data.

D. Strong Security, Privacy and Innovation Guarantees are Vital Complements to Surveillance Law

Finally, however surveillance law and practice evolves, Congress should continue the longstanding tradition of enjoining privacy and security protections as vital complements of surveillance law. In enacting CALEA, Congress recognized that as surveillance power grows, it is also vital extend privacy and security protections alongside. CALEA explicitly prohibits telecommunications carriers from taking steps to help law enforcement in ways that would impair customer privacy. All CALEA compliant technology is required to be designed so that it has

"...a minimum of interference with any subscriber's telecommunications service and [is designed] in a manner that protects the privacy and security of communications and call-identifying information not authorized to be intercepted."³³

Congress went even further to guarantee that CALEA surveillance requirements could not be used to block the deployment of any new technology. Under the explicit terms of the statute, if a new technology is being deployed and there is no way for it to meet CALEA requirements, then innovation takes precedence over surveillance guarantees.³⁴

³³ 47 USC 1002(a)(4)

³⁴ 47 USC 1002(b)(1)(B). "This subchapter does not authorize any law enforcement agency or officer ... to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services." As the legislative history on this section goes on to explain, "The Committee's intent is that compliance with the requirements in the bill will not impede the development and deployment of new technologies.... This means that if a service of technology cannot reasonably be brought into compliance with

None of this is to say that CALEA mandates should be extended to Internet platforms of mobile device manufactures, but rather to recognize that surveillance conducted under law must also respect the privacy of users who are not specific targets of a surveillance order.

Conclusion

While there is not likely to be a 'one size fits all' approach to the challenges that law enforcement faces today and in the future, there are a number of avenues Congress can explore to be sure that legitimate public safety needs are met to the maximum extent possible without compromising the security of Internet users.

* * * * *

the interception requirements, then the service or technology can be deployed." House Report No. 103-827, Part I .

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. OK. 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 ½ 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, 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 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, 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 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 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, 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 ter-

rorists 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 [continuing]. 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. OK. 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, 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 [continuing]. Finding a solution—

Ms. DEGETTE. And they couldn't—

Mr. BLAZE [continuing]. In advance of the problem.

Ms. DEGETTE [continuing]. 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 [continuing]. But do you think they can develop those resources?

Mr. WEITZNER. I think so. Absolutely. The only thing——

Ms. DEGETTE. Thank you. OK. 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? OK. 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. 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 [continuing]. Daily basis.

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

Mr. SEWELL. No, and I'm not——

Ms. DEGETTE. Yes. OK.

Mr. SEWELL [continuing]. 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 ½ years isn't such a long time to try to find a solution to this current issue? And likewise, the answer was in the affirmative for those who might not have—

Mr. SEWELL. It was, yes.

Mr. GRIFFITH [continuing]. 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, 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. 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. OK. 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 dis-

closed? 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, OK. You are on the subcommittee?

Mr. BILIRAKIS. No.

Mr. MCKINLEY. OK. 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.

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 [continuing]. 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 [continuing]. 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 [continuing]. 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 [continuing]. 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 [continuing]. 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 [continuing]. 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 non-government 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—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 appears at the conclusion of the hearing.]

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 appears at the conclusion of the hearing.]

Mr. MURPHY. And I also ask unanimous consent that the contents of the document binder¹ 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.

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.

¹The contents of the document binder can be found at: <http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104812>.

Mr. MURPHY. This committee is adjourned.
[Whereupon, at 1:14 p.m., the subcommittee was adjourned.]
[Material submitted for inclusion in the record follows:]



U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

April 15, 2016

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on “Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives”

On Tuesday, April 19, 2016, at 10:00 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled “Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives” This hearing will examine the balance between the benefits of strong encryption and its effect on the law enforcement and intelligence communities. Recent debate has focused heavily on a February 2016 court order that sought to compel Apple, Inc. (Apple) to assist the Federal Bureau of Investigations (FBI) in unlocking an iPhone used by one of the San Bernardino attackers. However, the issues surrounding the growing prevalence of default encryption are much broader. As such, this hearing will feature testimony from a diverse set of stakeholders, including representatives from federal and state law enforcement, as well as representatives from the device and enterprise information technology industries, and academia.

I. WITNESSES

First Panel

- Amy Hess, Executive Assistant Director for Science and Technology, Federal Bureau of Investigations;
- Thomas Galati, Chief, Intelligence Bureau, New York Police Department;
- Ron Hickman, Sheriff, Harris County Sheriff’s Office, on behalf of the National Sheriff’s Association; and
- Charles Cohen, Commander, Indiana Internet Crimes Against Children Task Force.

Second Panel

- Bruce Sewell, General Counsel, Apple, Inc.;
- Amit Yoran, President, RSA Security LLC;

Majority Memorandum for April 19, 2016, Subcommittee Oversight and Investigations Hearing
Page 2

- Daniel Weitzner, Director and Principal Research Scientist, Computer Science and Artificial Intelligence Laboratory (CSAIL) Decentralized Information Group (DIG), Massachusetts Institute of Technology; and
- Matthew Blaze, Associate Professor, Computer and Information Science, School of Engineering and Applied Science, University of Pennsylvania.

II. BACKGROUND

While concerns surrounding encryption and its effect on law enforcement has gained prominence in recent years, the debate regarding government access to encrypted data – commonly referred to as the “Crypto Wars” – has existed for decades. For example, in the mid-1990’s, intense debate over encryption prompted proposals to install a government-mandated method to permit lawful “exceptional access” capabilities into computing technologies. This so-called “Clipper Chip” was a “backdoor” that would, in theory, preserve the government’s ability to access encrypted information with legal authorization. The technology community resisted this proposal, arguing that such a system would create a vulnerability that could be exploited by actors outside of the government.¹ These concerns were ultimately validated when a critical flaw was discovered in the chip’s design.²

The growth in recent years of digital communications platforms and the spread of default encryption have rejuvenated the debate. Previously, encryption technologies – though highly effective if implemented properly – were complex, cumbersome, and hard to use. Most users, including criminals, did not possess the technical proficiency or patience to deploy strong encryption. However, mounting concerns regarding the security and privacy of digital data in recent years has incentivized companies to develop products and platforms that incorporate strong encryption by default, thus facilitating the widespread adoption of encryption technologies.

As a result, the law enforcement and intelligence communities, led primarily by the FBI, have reiterated their claims that they are losing the ability to monitor, obtain, and otherwise use the digital evidence associated with suspected terrorists, child predators, and other criminals. It is true that the deployment of strong encryption by companies like Apple and Google, and messaging apps like WhatsApp and Signal, create situations where neither the company nor the authorities can easily gain access to decrypted data – a situation commonly referred to as “going dark.”

However, technology companies have strongly rejected any calls that would force them to weaken encryption or to otherwise create backdoors in their products. They claim that doing so would significantly undermine the security of their products and the wider internet, and would leave huge swaths of data vulnerable to hacking and theft. Recent discoveries of exploitable vulnerabilities in internet products, most notably the unauthorized backdoor discovered in

¹ Steven Levy, *Battle of the Clipper Chip*, N. Y. TIMES, June 12, 1994, <http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all>.

² John Markoff, *Flaw Discovered in Federal Plan for Wiretapping*, N. Y. TIMES, June 2, 1994, <http://www.nytimes.com/1994/06/02/us/flaw-discovered-in-federal-plan-for-wiretapping.html>.

Majority Memorandum for April 19, 2016, Subcommittee Oversight and Investigations Hearing
Page 3

networking equipment provider Juniper's products,³ support the technology community's claims.⁴

The majority of the recent public debate has centered on the February 2016 court order to compel Apple to assist the FBI in unlocking a specific iPhone that was used by one of the San Bernardino attackers. In that case, the FBI eventually withdrew its request after an unidentified third-party provided an undisclosed method for gaining access into the iPhone in question.⁵ There are, however, other pending cases – including in New York where a federal magistrate judge initially ruled in Apple's favor and the government has appealed – and there will inevitably be more in the future.⁶

While these investigations provide valuable case studies, the issues implicated in the Crypto Wars debate encompass many stakeholders beyond Apple and the FBI, and many technologies beyond iPhones. For example, the messaging platform WhatsApp recently announced that it had completed its planned roll-out of strong, "end-to-end" encryption across the entirety of its products.⁷ In completing this roll-out, WhatsApp has extended the number of individuals protected by strong encryption by nearly a billion.⁸

These examples – the iPhones in each court case, and WhatsApp – represent the two primary types of data that encryption may be used to protect; data-at-rest and data-in-transit. In the recent cases involving iPhones, law enforcement is interested in obtaining access to data-at-rest in the device itself. In the case of WhatsApp's encrypted messaging, law enforcement and others are concerned about having access to communications, or data-in-transit. Data-at-rest refers to information that is statically stored, most commonly on devices such as smartphones or in the cloud. Data-in-transit, on the other hand, refers to information as it moves throughout the internet. This can refer to data that is being sent from a desktop browser to a company's server, for example, or – as in WhatsApp's case – from a smartphone to another smartphone. While the encryption technologies used to protect data-at-rest and data-in-transit are, at their core, similar,

³ 2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756), JUNIPER NETWORKS, Dec. 20, 2015, https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST.

⁴ Several cryptographic experts and government agencies, including the United States Computer Emergency Readiness Team (US-CERT), have indicated that the Juniper vulnerability could allow unauthorized actors to intercept and decrypt otherwise protected communications on a commercial scale. See: *Vulnerability Note VU#640184 Juniper ScreenOS contains multiple vulnerabilities*, COMPUTER EMERGENCY READINESS TEAM | SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY, Dec. 21, 2015, <https://www.kb.cert.org/vuls/id/640184>.

⁵ Ellen Nakashima, *FBI paid professional hackers one-time fee to crack San Bernardino iPhone*, WASH. POST, Apr. 12, 2016, https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

⁶ Ellen Nakashima, *Judge rules in favor of Apple in key case involving a locked iPhone*, WASH. POST, Feb. 29, 2016, https://www.washingtonpost.com/world/national-security/judge-rules-in-favor-of-apple-in-key-case-involving-a-locked-iphone/2016/02/29/fa76783e-db3d-11e5-925f-1d10062cc82d_story.html.

⁷ Previously, their strongest implementation applied only to smartphones running the Android mobile operating system, and did not cover group, photo, or video messages. See: moxio0, *WhatsApp's Signal Protocol integration is now complete*, OPEN WHISPER SYSTEMS, Apr. 5, 2016, <https://whispersystems.org/blog/whatsapp-complete/>.

⁸ Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED, Apr. 5, 2016, <http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/>.

the distinction between the two forms of data is important to the technical and policy discussion of this challenge.

There are three primary types of technologies that create data-in-motion and data-at-rest, each of which affects “going dark” differently:

- **Cloud Services** – Apple’s iCloud, Google’s Gmail and associated programs (Docs, Sheets, etc.), and Dropbox are some of the most well-known examples of cloud services. These services allow users to access data such as email, documents, and media over the internet through, for example, web browsers or apps.
 - **Effect on “going dark”:** **Low** – The majority of cloud services are hosted on hardware owned and operated by private companies that may analyze the associated data. While the data may be transported and stored in an encrypted format, the entity hosting the data likely possesses the ability to decrypt it.
- **Electronic Communications** – Messaging programs like WhatsApp, iMessage, and Google Hangouts, video and voice chat programs like Skype, FaceTime, and WebEx, along with more traditional methods like email, are just a few examples of the types of electronic communications that exist today. Regardless of specific features, “electronic communications” use the internet to send data between two or more users.
 - **Effect on “going dark”:** **Varies** – Different types of electronic communications vary greatly in terms of their use of encryption. Some programs like iMessage and WhatsApp are specifically designed to prevent anyone other than the message recipients from decrypting message data. Others, like Skype and Google Hangouts, encrypt data in transit, but have access to decrypted data at some point in the data’s lifetime.
- **Devices** – This category includes smartphones (like Apple’s iPhone and those running Google’s Android operating system), tablets, and laptops. As a general rule, devices tend to contain a significant amount of data pertaining to the device’s owner, including chat logs, emails, personally-identifiable information and much more.
 - **Effect on “going dark”:** **High** – Most modern devices now use operating systems that automatically employ some level of encryption. While traditional devices like laptops usually require that users manually enable higher levels of encryption, modern smartphone and tablet operating systems (including iOS and Android) are fully encrypted by default. Further, these operating systems are often designed in such a way as to make brute-forcing the encryption mathematically impossible, both for the associated companies and any interested third-parties such as law enforcement.

The growth of new technologies such as the Internet of Things (e.g. smart TVs, thermostats, baby bottles, etc.) and cyber-physical systems (smart grid, connected automobiles, medical devices, etc.) add new layers of complexity to this debate that must also be considered.

Majority Memorandum for April 19, 2016, Subcommittee Oversight and Investigations Hearing
Page 5

On the one hand, the growth of connected technologies opens new opportunities for investigation and surveillance by the law enforcement and the intelligence communities. On the other hand, many of these technologies – especially cyber-physical systems – will depend on strong encryption to ensure the security of products that could result in catastrophic or physical harm if compromised.

The unintended consequences of weakening or otherwise undermining strong encryption may range from the reduced economic competitiveness of U.S. companies, to an increased threat to the safety of products, the security of information, and the privacy of U.S. citizens. However, widespread default encryption could provide safe havens for terrorists, child predators, and other bad actors. This hearing presents an opportunity for representatives from law enforcement and the technology community to educate Congress and the public on the critical equities faced by both stakeholders, and to discuss how society may balance the law enforcement's need for access to encrypted data and the critical importance of safe, secure systems.

III. ISSUES

The following issues may be examined at the hearing:

- How has the evolution of encryption impacted law enforcement and intelligence capabilities, and how is it expected to impact those capabilities in the future?
- What are the concerns for data-in-transit and data-at-rest?
- Is a primary factor in the “going dark” phenomenon strong encryption, or is it the default application of strong encryption?
- How useful is metadata to investigations and prosecutions as compared to content data (i.e. text messages, pictures, etc.)?
- Is “legal hacking” by the government a viable option, and if so, what factors must be considered?

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact John Ohly or Jessica Wilkerson of the Committee staff at (202) 225-2927.

FOR IMMEDIATE RELEASE

Contact: Izzy Santa or Bronwyn Flores
703-907-4308 703-907-7679
isanta@CTA.tech bflores@CTA.tech
www.CTA.tech

Encryption Dialogue is About Security vs. Security, says CTA

Arlington, VA, April 18, 2016 – The following statement is attributed to Gary Shapiro, president and CEO, Consumer Technology Association (CTA)TM, regarding tomorrow’s House Energy and Commerce Committee hearing entitled, “Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives:”

“Tomorrow’s hearing continues a vital national discussion. The discussion isn’t about the tech industry versus law enforcement or privacy versus security but, rather, to quote Sen. Ron Wyden ‘more security versus less security.’ Consumers and the government both want and need encryption to protect personal data, credit information, computer systems, intellectual property and more from malicious hackers, terrorists and thieves. Right now, encryption is our best defense against cyber-attacks and ‘backdoors’. That means making sure everyone’s data is secure and tech companies need to create strong security and provide assurances to their customers without fear of legal reprisal.

“As we explore balanced approaches to keeping private digital communications and information secure, we must weigh the benefits and harms of government mandates and proposed court orders that require companies to disable security features aimed at weakening our data. Meanwhile, the tech industry will continue to help in the fight against terrorism by responding to lawful legal orders as well as developing predictive analytics, chemical-sensing devices, biometric measuring capabilities and other cutting edge innovations to keep our country safe. Market-driven innovation is best at preserving our security, our privacy and our liberty.”

About Consumer Technology Association:

Consumer Technology Association (CTA)TM is the trade association representing the \$287 billion U.S. consumer technology industry. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world’s best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES[®] – the world’s gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA’s industry services.

UPCOMING EVENTS

- CES on the Hill – [Register](#)
April 19, Washington, DC
 - Digital Patriots Dinner
April 20, Washington, DC
 - CES Asia 2016 – [Register](#)
 - May 11-13, Shanghai, China
 - CEO Summit
June 21-24, Tel Aviv, Israel
 - Innovate!
September 20-22, San Jose, CA
-

- CES Unveiled Prague
October 20, Prague, Czech Republic
- CES Unveiled Paris
October 25, Paris, France
- CT Hall of Fame Dinner
November 9, New York, NY
- CES Unveiled New York
November 10, New York, NY
- CES Unveiled Las Vegas
January 3, Las Vegas, NV
- CES 2017
January 5-8, Las Vegas, NV

###



805 15th Street, NW, Suite 708, Washington, D.C. 20005
 Telephone 202.650.5100 | Fax 202.650.5118
www.technet.org | @TechNetUpdate

April 19, 2016

The Honorable Tim Murphy
 Chairman
 Oversight and Investigations Subcommittee
 House Energy and Commerce Committee
 Washington, D.C. 20515

The Honorable Diana DeGette
 Ranking Member
 Oversight and Investigations Subcommittee
 House Energy and Commerce Committee
 Washington, D.C. 20515

Dear Chairman Murphy and Ranking Member DeGette,

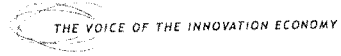
TechNet, the national, bipartisan network of innovation economy CEOs and senior executives, thanks you for holding today's hearing, "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

As the debate on encryption continues, we urge the committee to recognize that strong encryption is a commercial necessity that underpins millions of daily transactions and allows companies to safely store and move sensitive information. We have concerns over calls for weakened encryption and the privacy, security, economic, and competitive implications of these actions.

We are pleased that the committee has put together an expert discussion that can consider the legitimate rights and needs of consumers, businesses, governments, and the American economy. Our smartphones, and the other devices that we depend on, are essential parts of our lives. They hold our most personal information, including our health and financial data. This information needs to be protected from those who would seek to compromise our privacy and security.

At TechNet, we have great respect for the job that the FBI and other law enforcement agencies do. We fully understand that our nation faces grave threats and that we must be vigilant in protecting our homeland. Tech companies often work with law enforcement to provide expeditious access to data that companies possess through a valid legal process and emergency requests.

The challenge facing many technology companies, and now Congress, is that when a company does not have access to data, new legal requirements to create access points could force companies to eliminate security features from their products that would be counterproductive for both our nation's security and economic leadership. From a security perspective, once a vulnerability is established, it could be exploited by others who do not share the FBI's good intentions. The result: common transactions will become easy prey for bad actors, and customers around the world could lose faith in the trustworthiness of American products and choose alternatives that don't have the same vulnerabilities.



We appreciate the time that the Committee is taking to bring these issues to the public. We hope that the hearing will address the value of encryption and serve as a catalyst for a dialogue to chart a way forward on the complicated set of legal and technical issues surrounding encryption. TechNet is committed to finding balanced solutions that protect the safety and privacy of our citizens without damaging public trust, undermining security, and hindering economic growth and job creation. We are willing to work with Congress to achieve to these goals.



Linda Moore
President and CEO

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 2, 2016

Ms. Amy Hess
Executive Assistant Director
Science and Technology Branch
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Dear Ms. Hess:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 19, 2016, to testify at the hearing entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

Also attached are Member requests made during the hearing. The format of your responses to these requests should follow the same format as your responses to the additional questions for the record.

To facilitate the printing of the hearing record, please respond to these questions and requests with a transmittal letter by the close of business on Thursday, June 16, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachments

Attachment 1—Additional Questions for the RecordThe Honorable Tim Murphy

1. A number of other federal agencies - including Commerce, HHS and the State Department – support, fund, and even enforce the use of strong encryption. For example, the algorithm used by WhatsApp to provide end-to-end encryption was initially funded by the U.S. government. Obviously, there are multiple equities to consider in this debate – some which, I assume, generate differences of opinion within the executive branch about how to address this challenge.
 - a. Have other agencies pushed back or provided feedback on the FBI’s concerns about encryption?
 - b. Are there agencies or other federal entities that share your concerns?
2. This same dynamic applies to other technologies, as well. For example, the anonymization service, TOR, has received substantial support from the U.S. government for all the benefits it provides to dissidents and others living in oppressive regimes. Yet TOR has also become a tool for criminals, terrorists and others who wish to engage in illegal activities.
 - a. What challenges do TOR, or other anonymization services, present for the FBI and law enforcement? Do these challenges differ for state and local law enforcement?
3. How do we make sense of these apparently conflicting priorities within the government when it comes to encryption and other technologies that serve both noble and evil purpose?
4. Beyond encryption and anonymization services, please describe any additional areas of concern related to the issue of “going dark.”
5. One suggestion that has been offered to this problem is “legal hacking,” where the government either uses its own experts and resources to find exploitable vulnerabilities in products, or purchases the same from third-parties.

This seems like it would be a very expensive undertaking, and would involve a lot of manpower and resources.

- a. How much do you estimate a program like this would cost?
- b. How many experts would be required to staff such a program?
- c. Is this a viable alternative to weakening encryption?

- d. Or is it more of a tool in the tool belt, a potential option in certain circumstances but just one of what may need to be a suite of options moving forward?
6. How efficient would a program like this be?
- a. How long does it take to find exploitable vulnerabilities in products that can then be used to bypass strong encryption?
 - b. How long do those exploits usually work for?
7. Some devices contain a feature that users can enable to make it so that device deletes all of the data if a certain number of incorrect passcodes are tried. Absent this feature, it is my understanding that devices can be “brute-forced,” by simply trying different passcodes or passwords over and over again until the right one is found.
- a. How would the removal of this feature improve your ability to access encrypted devices?
 - b. What is your understanding of why this feature has been added to these devices?
 - i. Do you believe is reason is justified? Is there data to support your position?
 - c. Are there any downside or potential negative consequences by the removing this feature?
8. Many have suggested that law enforcement can rely on metadata as an alternative to exceptional access. Law enforcement has argued that while metadata can be useful in certain circumstance, its benefits are limited in real world investigations for a number of reasons. These include, but are not limited to: challenges locating and obtaining the necessary information; the volume and complexity of information, making it difficult to analyze; and it is less useful or compelling evidence in prosecutions.
- a. What are your capabilities for utilizing metadata?
 - b. Are there additional types of metadata or capabilities that companies do not currently provide that could improve law enforcement’s ability to utilize this information?
 - c. As more of our lives become connected to the Internet, it would seem logical to assume this only expands and enriches an individual’s digital footprint – does this present an opportunity for new and creative options for law enforcement to leverage this data?
 - i. If yes, please explain how and what options this presents law enforcement.

- ii. If no, please explain why not.
 - iii. Are there challenges or consequences to utilizing this information?
9. Do technology companies currently provide resources, training, or other expertise to you to help you make full use of the information potentially available?
- a. If yes, please describe the types of assistance you receive.
 - b. If no, please explain why not.
 - c. Does this present an opportunity for improvement both in terms of law enforcement's capabilities and also the relationship between the private sector and law enforcement?
 - i. If yes, please elaborate?
 - ii. If no, please explain why not?
10. Do you currently leverage the expertise of the academic community to help find or develop tools and solutions that would facilitate to better leverage metadata?
- a. If yes, please describe this collaboration or the types of assistance you receive.
 - b. If no, please explain why not.
 - c. Does this present an opportunity for improvement?
 - i. If yes, please elaborate?
 - ii. If no, please explain why not?
11. One specific concern related to metadata is the ability of smaller companies to respond to law enforcement requests.
- a. Are there ways to improve the capabilities and resources available to smaller companies that would assist them in responding to requests from law enforcement?
 - i. If yes, please explain how this could occur and what type of assistance could be provided.
 - ii. If no, please explain why it is not feasible.
 - b. Does the fact that some companies struggle to provide metadata lessen the value it provides to law enforcement, making it a less effective mitigation to the "going dark" problem?

12. Often this debate appears to be about picking sides – either you support law enforcement or you support the technology community. This feels like a lose/lose proposition.
 - a. Do you agree that this cannot be a black-and-white, us versus them, debate?
 - b. What is necessary to move past this perception to engage in an honest, constructive dialogue moving forward?
 - c. In your opinion, have we even scratched the surface of exploring new and creative solutions that acknowledge the concerns of both sides of this debate?

The Honorable H. Morgan Griffith

1. Is the FBI seeking legislation that would require tech companies to be able to assist federal investigators in breaking their own encryption?
 - a. If so, are you seeking the same thing from the U.S. Government sponsored Tor Network? Should the Government force Tor to put in a mechanism to subvert their encryption or withdraw funding?
2. Do you believe that terrorists, drug dealers, and other criminals are using Tor?
3. Have you raised any objections in the interagency process to the State Department's funding of Tor?
4. Why is the FBI focused on Apple, WhatsApp, and other commercial providers regarding the use of encrypted services, but not Tor?
5. Doesn't the government's support for Tor show the importance that even it places on encryption for protecting free speech around the world – despite the fact that it may be used by some bad actors?

Attachment 2—Member Requests for the Record

During the hearing, Members asked you to provide additional information for the record, and you indicated that you would provide that information. For your convenience, descriptions of the requested information are provided below.

The Honorable Michael C. Burgess, M.D.

1. The Commerce, Manufacturing, and Trade Subcommittee has been working very closely with the Federal Trade Commission on the issue of data breach notification and data security. A component of that effort has been the push for companies to strengthen data and 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 and protecting its customers. Has the FBI had any discussions with the FTC over whether back doors or access points might compromise secured data?

The Honorable Anna G. Eshoo

1. Did the FBI have discussions with Apple to let them know your agency had possession of the San Bernardino iPhone and ask for their help unlocking the phone? If so, when did these discussions take place?

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 2, 2016

Chief Thomas P. Galati
Intelligence Bureau
New York City Police Department
One Police Plaza Path
New York City, NY 10007

Dear Chief Galati:

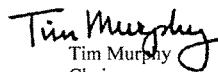
Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 19, 2016, to testify at the hearing entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Thursday, June 16, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

The Honorable Tim Murphy

1. The concept of law enforcement focusing their efforts on exploiting existing vulnerabilities or 'legal hacking' has started to take hold as a potential solution to the encryption challenge. At the same time, we have heard today that there is no one size fits all solution to this problem. I am interested in your perspective, based on real world experience:

a. Is this a viable alternative to weakening encryption?

Not in all cases. This technology is not widely available to local law enforcement, as it is often prohibitively expensive and can require unique expertise. Furthermore, depending on what exactly is being "hacked" (i.e., a phone's "contact" list or a third party app) there are complex legal issues which could be implicated. These issues have not been widely adjudicated in the courts and are unfamiliar concepts to many in the legal system, including the police.

b. Or is it more of a tool in the tool belt, a potential option in certain circumstances but just one of what may need to be a suite of options moving forward?

This would only qualify as a "tool in the tool belt" in rare circumstances, and again, only for those local agencies with the resources and expertise to deploy such a method.

2. Some devices contain a feature that users can enable to make it so that device deletes all of the data if a certain number of incorrect passcodes are tried. Absent this feature, it is my understanding that devices can be "brute-forced," by simply trying different passcodes or passwords over and over again until the right one is found.

a. How would the removal of this feature improve your ability to access encrypted devices?

A "brute force" attack could, in most instances, enable law enforcement to gain access to an encrypted phone. However, this would not allow law enforcement access to any activity that has occurred (or is stored in the record of) a "dark app." Many applications in use on phones today are so cloaked that even access to a phone does not reveal their activity/information. Furthermore, brute force attacks can be very time consuming, and will not be helpful in exigent circumstances.

b. What is your understanding of why this feature has been added to these devices?

To ensure that brute force attacks by law enforcement and criminals will be unsuccessful.

i. Do you believe this reason is justified? Is there data to support your position?

This reason is justified in that data that self-destructs as the result of brute force attacks protects against unauthorized third parties attempting to gain access to the phone. My support for this position comes from the fact that, in my police experience, stealing

smartphones is very common. A smartphone that can be hacked and re-used is valuable. A phone that cannot be unlocked is not.

c. Are there any downside or potential negative consequences by the removing this feature?

Yes. The ability to break into – and therefore re-program – a smartphone incentivizes thieves to steal them, re-program them, and then either use or sell them.

3. Many have suggested that law enforcement can rely on metadata as an alternative to exceptional access. Law enforcement has argued that while metadata can be useful in certain circumstance, its benefits are limited in real world investigations for a number of reasons. These include, but are not limited to: challenges locating and obtaining the necessary information; the volume and complexity of information, making it difficult to analyze; and it is less useful or compelling evidence in prosecutions.

a. What are your capabilities for utilizing metadata?

Through legal process as well as experienced and well-trained staff, NYPD investigatory units are uniquely positioned to utilize metadata. As the nation's largest police force, however, our ability to pursue this data is perhaps unique among most local law enforcement agencies.

b. Are there additional types of metadata or capabilities that companies do not currently provide that could improve law enforcement's ability to utilize this information?

Yes. Some social media companies, in particular, strip the metadata from documents they provide in compliance with a search warrant.

c. As more of our lives become connected to the Internet, it would seem logical to assume this only expands and enriches an individual's digital footprint — does this present an opportunity for new and creative options for law enforcement to leverage this data?

i. If yes, please explain how and what options this presents law enforcement.

The major innovation on the horizon in this area is the so-called “internet of things.” With most of the devices and appliances we use set at some point soon to go online, the ability for law enforcement to gain greater insight into the daily activities of subjects of investigation of course increases. It must be noted, however, that this will also entail a potentially significant increase in legal process. The courts may well see an enormous influx of subpoenas, search warrants, etc. Additionally, the standards and thresholds for this legal process have yet to be established.

ii. If no, please explain why not.

n/a

iii. Are there challenges or consequences to utilizing this information?

There are both. Law enforcement runs the risk of over-intrusiveness; there must therefore be careful legal protocols established for this type of investigation. Further, as noted above, this area of inquiry could lead to a heavy increase in the caseload of the courts and prosecutors. A challenge for law enforcement that this presents is that anything that is online can potentially be hacked, so criminals will also potentially have unprecedented access to a person's private life.

4. Do technology companies currently provide resources, training, or other expertise to you to help you make full use of the information potentially available?

Some do, but not all. Most do not offer a formal training process.

a. If yes, please describe the types of assistance you receive.

Most commonly, the companies holding this information provide guidance in how to frame and serve the legal process necessary to acquire this information. Among the major companies, most will advise on how best to frame requests so as to further an investigation. This, however, may be unique among local law enforcement to the NYPD, which interacts regularly with these firms.

b. If no, please explain why not.

Some of the companies law enforcement would potentially be interested in working with are outside of the country and do not comply with U.S.—or any—law enforcement. Other firms may not have a law enforcement compliance capability because of resource issues or an unwillingness to appear to transparent.

c. Does this present an opportunity for improvement both in terms of law enforcement's capabilities and also the relationship between the private sector and law enforcement?

Yes, especially among new firms whose business model is based on emerging technologies.

i. If yes, please elaborate?

A more formalized way to interact with law enforcement for such firms would be helpful.

ii. If no, please explain why not?

n/a

5. Do you currently leverage the expertise of the academic community to help find or develop tools and solutions that would facilitate to better leverage metadata?

Yes, in some instances.

a. If yes, please describe this collaboration or the types of assistance you receive.

As the nation's largest municipal police force, the NYPD fields numerous invitations to attend conferences, workshops, etc. At events like these, interactions with academia regarding best practices and new technologies is common. NYPD often presents at these events as well.

b. If no, please explain why not.

n/a

c. Does this present an opportunity for improvement?

We can always improve.

i. If yes, please elaborate?

The speed at which new technologies emerge today is blinding. Any interaction with academics who can provide insight on those technologies is helpful. Generally, however, we keep abreast of these issues through contacts with other law enforcement at the federal, state, and even international level. We also do it through contact with the companies themselves.

ii. If no, please explain why not?

n/a

6. One specific concern related to metadata is the ability of smaller companies to respond to law enforcement requests.

a. Are there ways to improve the capabilities and resources available to smaller companies that would assist them in responding to requests from law enforcement?

Of the emerging tech firms that we would be most interested in, most heavily tout their own security and their ability to safeguard information from government. Improving law enforcement's access would be helpful.

i. If yes, please explain how this could occur and what type of assistance could be provided.

Such firms should, as part of their basic growth plan, ensure that a legal compliance unit of some sort is in place and adequately staffed.

ii. If no, please explain why it is not feasible.

n/a

b. Does the fact that some companies struggle to provide metadata lessen the value it provides to law enforcement, making it a less effective mitigation to the "going dark" problem?

Yes, but while valuable, metadata is not a cure-all to the "going dark" problem.

7. Often this debate appears to be about picking sides — either you support law enforcement or you support the technology community. This feels like a lose/lose proposition.

a. Do you agree that this cannot be a black-and-white, us versus them, debate?

Yes.

b. What is necessary to move past this perception to engage in an honest, constructive dialogue moving forward?

An update to the CALEA law.

c. In your opinion, have we even scratched the surface of exploring new and creative solutions that acknowledge the concerns of both sides of this debate?

Yes, in the sense that the issues involved have been examined at length in the press, in many cases by those who are ill-informed or who take a "zero sum" approach to the problem. But no, in the sense that the technologies that are on the near horizon — as well as the "internet of things" — will both introduce new immediacy to the issue.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 2, 2016

Captain Charles Cohen
Commander
Office of Intelligence and Investigative Technologies
Indiana State Police
100 N. Senate Avenue
Third Floor
Indianapolis, IN 46204

Dear Captain Cohen:

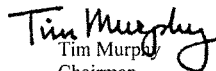
Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 19, 2016, to testify at the hearing entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Thursday, June 16, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy
Chairman

Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Responses to Questions

Captain Charles Cohen

Commander, Intelligence and Investigative Technologies

Indiana State Police

Testimony on April 19, 2016

Hearing Before the Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

United States House of Representatives

“Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives”

The Honorable Tim Murphy

1. The concept of law enforcement focusing their efforts on exploiting existing vulnerabilities or "legal hacking" has started to take hold as a potential solution to the encryption challenge. At the same time, we have heard today that there is no one size fits all solution to this problem. I am interested in your perspective, based on real world experience:

- a. Is this a viable alternative to weakening encryption?**
- b. Or is it more of a tool in the tool belt, a potential option in certain circumstances but just one of what may need to be a suite of options moving forward?**

In my experience, what some refer to as “legal hacking” is a method of last resort. It presents numerous challenges that often cannot be overcome. First, “legal hacking” requires that there is a vulnerability that has not previously been discovered by the hardware manufacturer, firmware developers, or third parties. Second, like all tools used by law enforcement in the recovery of forensic evidence, the methodology must pass tests of scientific rigor, including that it is valid and reliable, in order for the recovered evidence to be admissible in criminal court. Third, since this requires a one-off approach to every forensic examination the actual financial costs exceed practicality as a solution to the encryption issue. This is especially true when one considers that the Indiana State Police alone conducted forensic examinations of over 1,000 cellular phones in

2015—representing a myriad of combined manufacturers, models, operating systems, operating system versions, installed applications, and carriers.

Another concern with “legal hacking” as a primarily, or even routinely, considered solution is the potential amount of time required to access a device using this method. There is a relative time value of evidence in most criminal investigations. This means that investigators must not just be able to eventually access data and metadata stored on a device, but must be able to access this information relatively quickly. Law enforcement refers to this concept as “recognizing and respecting the investigative time line”. In the well-publicized case in San Bernardino County, California the suspects were dead and the information on an encrypted device needed to be accessed to determine its immediate relevant criminal intelligence value. By contrast, many investigations in which I am involved, and about which I am aware, involve ongoing victimization. In many traditional criminal investigations, there is a direct correlation between how quickly law enforcement can access information contained on encrypted devices and how quickly ongoing victimization can be stopped and future victimization prevented.

For example, the Criminal Division of the Washington State Attorney General's Office undertook a three and a half year research project, partially funded by the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, to study the investigation of child abduction murder cases. In this first of its kind research project, published in 1997, researchers reviewed more than 600 child abduction murder cases across the United States and interviewed the investigating detectives. This data provided law enforcement valuable insight into what investigative techniques tend to be most productive. In 76% of the missing children homicide cases studied, the child was dead within three hours of the abduction—and in 88.5% of the cases the child was dead within 24 hours. [<http://www.atg.wa.gov/child-abduction-murder-research>, accessed June 15, 2016]

It is a straw man argument that legal hacking and weak encryption are the only two available options. Several other options exist, including that previously used by Apple and currently used by Google, in which the operating system manufacturer retains the technical ability to comply with the proper service of legal process to decrypt the data residing on a device at rest or data in motion between devices. Another option is to place the technical capability with a Trusted Third Party (TTP). This method is routinely used in cryptography and electronic communication, and would allow the TTP to comply with the proper service of legal process to decrypt the data residing on a device at rest or data in motion between devices. Other options that provide for both customer security and the ability of government to solve crimes and protect people likely exist. It is decidedly preferable to engage in collaborative research and design that achieves results through open and earnest cooperation between industry and law enforcement. In this non-polarized environment, the best possible solutions can be discovered and deployed.

2. Some devices contain a feature that users can enable to make it so that device deletes all of the data if a certain number of incorrect passcodes are tried. Absent this feature, it is my understanding that devices can be "brute-forced," by simply trying different passcodes or passwords over and over again until the right one is found.

- a. How would the removal of this feature improve your ability to access encrypted devices?
- b. What is your understanding of why this feature has been added to these devices?
 - i. Do you believe is reason is justified? Is there data to support your position?
- c. Are there any downside or potential negative consequences by the removing this feature?

In my experience, simply removing the security feature that invokes complete data eradication after a certain number of failed pass code attempts does not explicitly expose the data to "brute-force" exceptional access solutions. That is because the developers that use this feature layer this with other features that also prevent "brute-force" from being a viable solution to accessing encrypted data.

An unknown Personal Identification Number (PIN) consisting of four numbers has 10,000 possible combinations. An unknown PIN consisting of six numbers has 1,000,000 possible combinations. This means that the longer the PIN, the less that "brute-force" is a viable solution to accessing encrypted data. Apple, as an example, changed the default PIN length from four to six numbers with the upgrade to iOS 9. It is possible for a customer to change the PIN length back to four numbers, as was the default on previous versions of the operating system.

Some operating system developers, such as Apple, also set a scheme that slows or delays the speed with which someone can try to enter PINs in attempt to guess or "brute-force" the correct PIN. Data to support this can be found in a document Apple published in May, 2016 entitled, "iOS Security iOS 9.3 or Later" which includes: "A large iteration count is used to make each attempt slower. The iteration count is calibrated so that one attempt takes approximately 80 milliseconds. This means it would take more than 5½ years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers." [https://www.apple.com/business/docs/iOS_Security_Guide.pdf, accessed June 14, 2016].

One must consider that the statute of limitations in most states, for most serious crimes is five years. So, in this publication, Apple estimates that it could take longer than the time allowed to charge someone with having committed a serious crime to access a device using iOS through "brute force" even when the feature to wipe data after a certain number of incorrect passcodes are tried is not enabled. This means that even without an option users can enable to make it so that the device deletes all of the data if a certain number of incorrect passcodes are tried, "brute-force" is not a viable option for law enforcement, or anyone else, to access the data residing on a device.

3. Many have suggested that law enforcement can rely on metadata as an alternative to exceptional access. Law enforcement has argued that while metadata can be useful in certain circumstance, its benefits are limited in real world investigations for a number of reasons. These include, but are not limited to: challenges locating and obtaining the necessary information; the volume and complexity of information, making it difficult to analyze; and it is less useful or compelling evidence in prosecutions.

- a. What are your capabilities for utilizing metadata?
- b. Are there additional types of metadata or capabilities that companies do not currently provide that could improve law enforcement's ability to utilize this information?
- c. As more of our lives become connected to the Internet, it would seem logical to assume this only expands and enriches an individual's digital footprint- does this present an opportunity for new and creative options for law enforcement to leverage this data?
 - i. If yes, please explain how and what options this presents law enforcement.
 - ii. If no, please explain why not.
 - iii. Are there challenges or consequences to utilizing this information?

The potential value of metadata during criminal investigations should not be underestimated. The more devices are connected to wireless routers, and connected and controlled via the internet, the more that metadata becomes of value in the course of criminal investigations. But, while metadata can potentially show activity, location, and time, it cannot show context. The context in which two people are communicating with each other, the reason why two people were at the same place at the same time, can best be learned through content evidence—data at rest or data in motion. An example of this comes from investigations involving child sexual solicitation. While metadata can potentially be used to determine that a device belonging to an adult was used to connect to a device used by a child, only content data—potentially stored either client-side on the devices or server-side by the Internet Service Provider—can be used to determine if the contact between the adult was criminal in nature.

There are several current challenges to our ability to use metadata in the course of criminal investigations. Among those challenges is that law enforcement often does not know what metadata is being collected by the involved companies during the normal course of business. In addition, there is currently no legal requirement for companies to collect certain types of metadata, or requiring that metadata which is collected in the normal course of business be retained for a specific period.

A real example of this challenge comes from a threat investigation in which I was personally involved. An unknown subject was using a Webmail provider based in the United States to send threatening communications to an identified victim. Law enforcement served legal process on the

company providing the Webmail service. That company responded to the legal process, providing the IP address associated with the threatening communication, after a period of 13 days. That IP address resolved to a cellular telecommunications provider, also based in the United States. Law enforcement then sent legal process to the provider requesting the telephone number or any other identifying information associated with the IP address at the specific date and time the threat was sent. The cellular telecommunications provider notified law enforcement that it made the business decision to only maintain metadata that associates an IP address to a particular device or telephone number for 72 hours. At the same time, another cellular telecommunications provider made the business decision to keep the exact same metadata for one year. This demonstrates that, in the absence of legislative oversight, different companies make different business decisions that can diminish the utility of metadata during criminal investigations.

It is certainly true that the amount of potentially relevant evidence in the digital world is growing, but that does not mean that it is necessarily available to law enforcement when we need it. More and more of that "rich digital footprint" lies behind barriers to access including encryption, heightened legal standards, and routine service provider delays in response to the service of legal process. There are no "new and creative" ways to use evidence held by a private company in the normal course of business, but to which law enforcement does not have access, even when it is legally warranted and judicial process is validly served on the private company.

Because technology has created an easier alternative, in many instances that which previously was available as physical evidence now only exists in the digital world. Why keep a stack of pictures in a shoebox in your closet when you can store them on an encrypted phone? While there is potential that metadata will assist in future criminal investigations, this is only true if law enforcement has access to the metadata in a forensically sound manner supported by a controlling legislative framework attuned to the demands of the investigative timeline.

4. **Do technology companies currently provide resources, training, or other expertise to you to help you make full use of the information potentially available?**
 - a. **If yes, please describe the types of assistance you receive.**
 - b. **If no, please explain why not.**
 - c. **Does this present an opportunity for improvement both in terms of law enforcement's capabilities and also the relationship between the private sector and law enforcement?**
 - i. **If yes, please elaborate?**
 - ii. **If no, please explain why not?**

It is not possible to answer the question in a binary way that technology companies either do, or do not, provide resources, training or other expertise. A few technology companies do provide training and resources to law enforcement. For example, one company that works with cryptocurrencies regularly provides technical training to law enforcement on the topic and makes itself available for investigative assistance. But, beyond some specific examples, such as this, my assessment is that the vast majority of technology companies do not provide resources, training, or other expertise to law enforcement in any sort of meaningful or organized way. At the other end of the spectrum, I have personally been in contact with technology companies that refused to tell me what types of information they retain in the normal course of business or by what names they keep that information, while at the same time telling me that if I do not use the company-specific name for the needed information the judicial warrant will be rejected.

Several technology companies that previously provided organized resources and training to law enforcement have drawn away from doing so in the last two to three years. I have observed this to be a concerning trend. One challenge that I have personally encountered, and which I have seen encountered by other criminal investigators and prosecutors, is the struggle to find expert or skilled fact witnesses who can provide testimony as to the meaning of information obtained from technology companies through the service of legal process. Most technology companies will not provide any interpretation or explanation of the information provided pursuant to legal process or provide a skilled fact or expert witness. At the same time, the format and structure of information provided pursuant to legal process is usually unique to the internal process of that individual company. Without such explanation and testimony, it is often not possible to get the information introduced as an item of evidence at a criminal trial.

The opportunity for better relations between law enforcement and the private sector is vast. There is a true need for better coordination and cooperation between law enforcement and the private sector. But, such a relationship would need to be incentivized. I see the ability to more effectively conduct criminal investigations and protect people as an existing incentive for law enforcement to improve this relationship. Unfortunately, I do not currently see a compelling incentive for the private sector beyond the desire to be good corporate citizens. At the same time, I see disincentives such as technology companies receiving criticism from certain third-party advocacy organizations when it becomes known that they were providing any form of material support to law enforcement or government.

5. **Do you currently leverage the expertise of the academic community to help find or develop tools and solutions that would facilitate to better leverage metadata?**
 - a. **If yes, please describe this collaboration or the types of assistance you receive.**
 - b. **If no, please explain why not.**
 - c. **Does this present an opportunity for improvement?**

- i. **If yes, please elaborate?**
- ii. **If no, please explain why not?**

Law enforcement most definitely does leverage the expertise of the academic community. The Indiana State Police has an ongoing and mutually beneficial relationship with Purdue University in this area that extends back for over a decade. Within the Internet Crimes Against Children (ICAC) task force community, law enforcement routinely works with and leverages the expertise of academics and experts from several universities.

In my experience, the collaboration has most benefitted law enforcement in development and validation of digital forensic tools. At the same time, I have seen these collaborations benefit both academic institutions and individual researchers by giving them direct access to practitioners and allowing them to engage in applied research. The biggest limiting factor for continued and increased collaboration between law enforcement and academia in these areas is the availability of funding.

- 6. **One specific concern related to metadata is the ability of smaller companies to respond to law enforcement requests.**
 - a. **Are there ways to improve the capabilities and resources available to smaller companies that would assist them in responding to requests from law enforcement.**
 - i. **If yes, please explain how this could occur and what type of assistance could be provided.**
 - ii. **If no, please explain why it is not feasible.**
 - b. **Does the fact that some companies struggle to provide metadata lessen the value it provides to law enforcement, making it a less effective mitigation to the "going dark" problem?**

The retention of metadata and response for requests for retained metadata by small technology companies is very similar to retention and provision of certain information by small financial institutions and small money transfer businesses pursuant to the Bank Secrecy Act of 1970 and subsequent associated legislation. In 1990, the United States Department of the Treasury created FinCEN in part to improve capabilities and resources both for financial institutions and law enforcement. In 1994, the mission of FinCEN was broadened to include regulatory responsibilities.

There are many parallels between metadata and data maintained by financial institutions that are regulated and supported under the Bank Secrecy Act and a series of subsequent laws, and the metadata and data maintained by technology companies, which currently lack similar regulation

and support. The establishment for technology companies of statutory regulations and an entity of similar structure and authority as FinCEN could provide assistance to, and improve the capabilities and resources available to, small technology companies.

7. **Often this debate appears to be about picking sides –either you support law enforcement or you support the technology community. This feels like a lose/lose proposition.**
 - a. **Do you agree that this cannot be a black-and-white, us versus them, debate?**
 - b. **What is necessary to move past this perception to engage in an honest, constructive dialogue moving forward?**
 - c. **In your opinion, have we even scratched the surface of exploring new and creative solutions that acknowledge the concerns of both sides of this debate?**

I could not agree more strongly that this cannot and should not be about picking sides or be a black-and-white, us versus them, issue. This is not a zero sum game. There are not winners and losers between law enforcement and the technology industry. If public sector law enforcement and private sector technology companies do not work together to find solutions such that there can be a balance between privacy and the ability to effectively conduct criminal investigations, current and future victims will be the losers.

As I testified, it is increasingly apparent to me that a component of this solution must be legislative. We must move beyond the fallacies that law enforcement wants a degradation of personal privacy and that industry is the only defense against such intrusions on liberties. It is my strong and sincere opinion that we have not yet scratched the surface both of potential solutions and potential concerns. It is clear that, like never before in the history of the United States, the law has not kept pace with technology. If we fail to find balanced and productive solutions now, that chasm will just continue to grow.

In my professional position, I routinely have the opportunity to interact with a wide array of law enforcement at the federal, state, and local level. From that interaction, I know that the law enforcement community values civil liberties and privacy to an extent that is difficult to adequately articulate. I also routinely have opportunity to interact with those that work in and represent technology companies. And, I know that technology companies want to act as good corporate citizens and protect the safety and security of their customers. What is needed is a third party to set the framework and incentive for industry and law enforcement to work together without recriminations or fear of negative business impact.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 2, 2016

Mr. Bruce Sewell
Senior Vice President and General Counsel
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014

Dear Mr. Sewell:

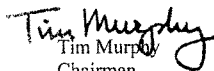
Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 19, 2016, to testify at the hearing entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Thursday, June 16, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

**Responses to Questions for the Record
“Deciphering the Debate Over Encryption: Industry and Law Enforcement
Perspectives”
Bruce Sewell, Senior Vice President and General Counsel
Apple, Inc.**

Questions for the record from The Honorable Tim Murphy

1. Often this debate appears to be about picking sides – either you support law enforcement or you support the technology community. This feels like a lose/lose proposition.

- a. Do you agree that this cannot be a black-and-white, us versus them, debate?

Answer: Yes, this issue is not about law enforcement versus the technology community. I believe all of us support the same goal—ensuring the safety of Americans and the security of information on which all of us depend. The debate needs to stay focused on how best to achieve that goal, and the role that encryption plays in safeguarding American interests. Strong encryption is an absolute necessity and is already prevalent throughout the economy. We believe the best path forward is for Congress to engage in a thorough and transparent discussion with all stakeholders.

- b. What is necessary to move past this perception to engage in an honest, constructive dialogue moving forward?

Answer: The American people deserve an open and honest conversation on the important questions raised by this debate. This means not only talking about how to help law enforcement do their job as well as possible, but also understanding the consequences that any proposed solutions would have to other threats and interests.

- c. In your opinion, have we even scratched the surface of exploring new and creative solutions that acknowledge the concerns of both sides of this debate?

Answer: It is important that any potential technical remedy be evaluated fairly in terms of benefit to law enforcement, as well as impact on digital security, the safety of the Nation’s infrastructure, and individuals’ privacy rights.

2. A lot of this debate has focused on Apple and, recently, WhatsApp. However, encryption is used by many companies and in a wide range of technologies.

- a. Can you give us a sense of the uses of encryption and breadth of technologies and service this includes?

Answer: Encryption undergirds much of the security technology that keeps our personal information safe, including financial information and health information. In addition, it is public record that encryption is used to protect the security of transportation systems, communications services, the power grid, emergency response services, and healthcare delivery, among other critical infrastructure that keep Americans living and working efficiently and safely.

- b. What is the role of encryption in securing critical infrastructure or the growing number of cyber-physical systems and internet connected devices, otherwise known as the Internet of Things?

Answer: Encryption is fundamental to the safety and security of much of the Nation's critical infrastructure. Increasingly, critical infrastructure is connected to the Internet and remotely controllable. Undermining encryption injects risk to key infrastructure systems including the power grid, banks and financial institutions, communications networks, the transportation system, 911 and emergency response systems, water purification and pumping stations, and hospitals. Significant disruptions to critical infrastructure could be deadly. Protecting the security of data and systems that operate critical infrastructure should be of paramount importance to the Nation.

Relatedly, products in our home and at work are more connected than ever, and this trend is growing. The "Internet of Things" (IoT) describes the network of "smart" devices that are embedded with Internet-connected sensors and that leverage cloud-based analytics that make the data actionable. This new data economy requires a foundation of trust and security. Users want to ensure that the data they share is kept private and secure. Encryption is an important tool for securing data in transit and at rest, and for maintaining authentication credentials to prevent bad actors from using IoT endpoints as gateways for broader network access. Government proposals that would restrict the use of encryption or limit the ability to design more secure systems would undermine new and evolving technologies.

3. When we talk about weakening encryption, how would decisions that weaken encryption in one sector—say communications or messaging—affect other forms of encryption or sectors, such as critical infrastructure or JOT devices and systems?

Answer: Encryption is central to many products and mechanisms that safeguard infrastructure across every sector of the economy. Weakening encryption injects risk to key infrastructure systems, including the power grid, banks and financial institutions, communications networks, the transportation system, 911 and emergency response systems, water purification and pumping stations, and hospitals. Significant disruptions to critical

infrastructure could be deadly. In addition, weakening encryption could lead to compromise of a person's personal information, such as health records or financial data.

- a. Is it possible to increase law enforcement access to certain encrypted devices or communications without affecting encryption in all systems?

Answer: We do not believe it is possible to create backdoors or other vulnerabilities in a certain class of devices or services without affecting the security of other systems. Encryption is an important tool for securing data in transit and at rest, and for maintaining authentication credentials to prevent bad actors from using internet-connected endpoints as gateways for broader network access. I mentioned in my testimony that smartphones are increasingly becoming gateways to other systems—transportation and electrical infrastructure, financial and communications systems, public health infrastructure, etc. A weakness in one system can be easily exploited to access another.

4. Law enforcement is concerned about the growing prevalence of default encryption, as well as the use of end-to-end and/or "warrant-proof" encryption.

- a. What factors are influencing the transition to default encryption?

Answer: Strong forms of encryption are becoming more and more the norm. In some cases, government agencies (e.g., the FTC) are directing the business community towards better encryption to protect consumers, and encryption is a legal requirement in some contexts. Our goal at Apple is to make our security as robust as we can while still maximizing the user experience. With developments in technology, we have been able to offer default encryption, which significantly strengthens protection of data from compromise.

- b. Which factors were most influential in Apple's decision to implement default encryption?

Answer: As I stated above, we will move to the strongest security we can that still allows for an excellent user experience. Technical developments have allowed for use of default encryption while still providing positive user experience.

5. What are the benefits of end-to-end encryption compared to alternatives such as a managed key system used by some companies to retain access to content for advertising, security scans or other purposes?

Answer: End-to-end encryption provides greater security to our customers and overall improves the security of data of all types. A managed key system, where

a key is retained by a third-party (other than the device owner), provides an opportunity to bad actors seeking to access private information or systems, weakening the security of the user's data and of the system overall.

- a. Is there evidence that demonstrates the improvement to security or other benefits that justify or otherwise influence the use of end-to-end encryption?

Answer: Several studies show that encryption provides demonstrable security benefits. For instance, according to SafeNet (now Gemalto), out of the over 700 million data records lost or stolen in 2015, only 4% of the breaches involved data that was encrypted in part or in full.¹

- b. Are there other factors influencing the shift to end-to-end encryption?

Answer: As stated above, Other branches of the government (e.g., the FTC) are directing the business community towards better encryption to protect consumers, and encryption is a legal requirement in some contexts.

- c. What influenced Apple's decision to implement end-to-end encryption?

Answer: Apple is always striving to provide the best security possible for customers while at the same time providing the highest level of usability. We take important steps to improve the security of our devices and services with every release. Since we know that customers lose devices or have them stolen, it is essential to protect the data on the device to the greatest extent possible.

6. Many have suggested that law enforcement can rely on metadata as an alternative to exceptional access. Law enforcement, however, has argued that while metadata can be useful in certain circumstance, its benefits are limited in real world investigations for a number of reasons. These include, but are not limited to: challenges locating and obtaining the necessary information; the volume and complexity of information, making it difficult to analyze; and it is less useful or compelling evidence in prosecutions.
 - a. What is your understanding of law enforcement's capabilities – at the federal, state and local levels, respectively - for utilizing metadata?

Answer: Our understanding from the public record is that capabilities vary widely from jurisdiction to jurisdiction. Apple works with law enforcement at all levels to respond to search warrants, and if we have responsive data, we provide it. Improving the capability of law enforcement agencies to solve

¹ 2015 Data Breach Statistics - Breach Level Index Findings, *available at*, <http://www.safenet-inc.com/resources/data-protection/2015-data-breaches-infographic/>

crimes more expeditiously, while preserving security features that protect personal and public safety, is a worthwhile goal.

- b. Are there additional types of metadata or capabilities that companies do not currently provide that could improve law enforcement's ability to utilize this information?

Answer: Apple currently provides to law enforcement all metadata that we collect that is responsive to a particular legal process.

- c. As more of our lives become connected to the Internet, it would seem logical to assume this only expands and enriches an individual's digital footprint – does this present an opportunity for new and creative options for law enforcement to leverage this data?

- i. If yes, please explain how and what options this presents law enforcement.
- ii. If no, please explain why not.
- iii. Are there challenges or consequences to utilizing this information?

Answer: The growth of the Internet of Things, among other technologies, opens up new and useful ways to enrich everyday life. At the same time, new sources of data collection undoubtedly expose more of our personal information. There is more information about all of us now than ever before; we leave digital footprints everywhere. Privacy and security concerns must be factored into any debate about the use of this information.

7. Does Apple currently provide resources, training, or other expertise to law enforcement, to help them make full use of the information potentially available to them?

- a. If yes, please describe these efforts.

Answer: Yes, we currently publish Law Enforcement Guidelines for use by law enforcement or other government entities in the U.S. when seeking information from Apple about users of Apple's products and services, or from Apple devices. Here is a link to our Legal Process Guidelines: <http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>

The Guidelines detail the data available and the type of process required to obtain that data. In addition, everyday our team works with individual law enforcement officers to help them understand our law enforcement compliance function.

b. If no, please explain why not.

Answer: See answer to a. above.

c. To your knowledge, do other technology companies currently provide resources, training, or other expertise to law enforcement, to help them make full use of the information potentially available to them?

Answer: We are not aware of what resources, training, or expertise other companies may provide to law enforcement.

d. Does this present an opportunity for improvement, both in terms of law enforcement's capabilities and also the relationship between the private sector and law enforcement?

Answer: Apple shares law enforcement's goal of creating a safer world and therefore continues to work with law enforcement. We have a team of dedicated professionals on call 24 hours a day, seven days a week, 365 days a year, to assist law enforcement. We believe that continued collaboration between law enforcement and the technology sector is important. We will continue to engage in a constructive dialogue with law enforcement around data that is available through lawful process.

8. One specific concern related to metadata is the ability of smaller companies to respond to law enforcement requests.

a. Is there a way for larger companies, who do have the knowledge and expertise, to help out their smaller peers?

i. If yes, please explain how this could occur and what type of assistance could be provided.

ii. If no, please explain why it is not feasible.

iii. Does the fact that some companies struggle to provide metadata lessen the value it could provide to law enforcement, making it a less effective mitigation to the "going dark" problem?

Answer: We have not examined what challenges other companies, regardless of size, may have related to the disclosure of metadata.

9. In the wake of the FBI's use of a third party to access the iPhone in the San Bernardino case, there has been considerable discussion about the concept of "legal hacking."

a. Since the newer designs of iPhones prevent the bypassing of the built-in

encryption, does Apple believe that legal hacking is an appropriate method for investigators to use to access evidence in investigations?

Answer: Apple spends countless hours and resources making our products safe and secure for our customers. If we find a vulnerability, we fix it immediately. Incentivizing law enforcement to search for and exploit vulnerabilities could have a deleterious impact on security and unintended consequences for American companies and their customers.

b. If law enforcement does use a vulnerability to access your product, presumably Apple would want to fix that vulnerability so it could not be used by others. But wouldn't law enforcement have an interest in maintaining that vulnerability, especially if they used time or resources to obtain it?

i. What challenges does that present for a company?

Answer: Our primary concern is the security of our customers; if we learn of a vulnerability, we will fix it expeditiously. If a third-party, whether a government entity or another entity acting on their behalf, were to discover a vulnerability and not disclose it, it could weaken the security of our users' confidential information.

ii. How do you manage that?

Answer: We do our best to fix to any vulnerability known to us as expeditiously as possible.

c. If legal hacking is not a viable option – and Apple cannot assist law enforcement with accessing a device - what other options does Apple believe are or should be available to investigators?

Answer: As we have said previously, this is the golden age of surveillance and the government can access significant amounts of Americans' personal data through lawful process. We agree that collaboration between law enforcement and the technology sector is important. We will continue to work with law enforcement around data that is available to them through lawful process.

10. Some devices contain a feature that users can enable to make it so that device deletes all of the data if a certain number of incorrect passcodes are tried. Absent this feature, it is my understanding that devices can be "brute-forced," by simply trying different passcodes or passwords over and over again until the right one is found.

- a. Apple has this feature – why did the company feel this was an important feature?

Answer: Apple is always striving to provide the best security possible for customers while at the same time providing the highest level of usability. We take important steps to improve the security of our devices and services with every release. Since we know that customers lose devices or have them stolen, it was essential to protect the data on the device to the greatest extent possible.

- b. In your opinion, what might be some of the consequences if it were removed?

Answer: If such feature were removed, it would considerably weaken the security of our customers' personal information, and it is likely that thieves who have been dissuaded from stealing smartphones because of the auto-erase feature would benefit from its removal. Strong security requires a layered and in-depth approach, including implementation of a strong password protection regime.

Questions for the record from The Honorable Susan Brooks

1. You testified that you and your team work very closely with local law enforcement and have regular conversations with law enforcement officials and policymakers. Specifically, you stated: "I work with senior people in local law enforcement on exactly these policy issues". What individuals and law enforcement agencies at the state and local level have you or your team discussed policy issues with? Did you discuss the shift to default device encryption, and other policy changes, with state and local law enforcement officials or agencies before iOS 8 was released? How often do you engage in policy related discussions with local law enforcement officials or agencies?

Answer: Apple does not discuss future products outside the company, but all of our operating systems are available to beta testers prior to the public release of those operating systems. Apple personnel regularly meet and speak via telephone on an operational level with many state and local law enforcement officials. This includes, for example, New York County District Attorney Cyrus Vance and East Baton Rouge District Attorney Hillar Moore.

Questions for the record from The Honorable Richard Hudson

1. The CEO of MSAB, a technology company, recently proposed in a Detroit News article that there is a way for the government to access data stored on our phones without building in a backdoor to the encryption. His solution is to build a

two part decryption system, where both the government and the manufacturer possess a unique decryption key. Both decryption keys would be necessary in addition to holding the physical device in order to decrypt and access the encrypted data.

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 technology industry, and the law enforcement community regarding a proposal like this or something similar to allow safe access to this data while still protecting consumer interest?

Answer: Creating keys introduces risk, regardless of who holds the key. A managed key system, in which the existence of a key retained by a third-party (other than the device owner) is known, introduces a concentrated opportunity to bad actors seeking to access information or systems. Those subject to law enforcement inquiries represent far less than one-tenth of one percent of our hundreds of millions of users. But creation of key makes all users and the entire system more. We do not have a technical means to allow law enforcement “safe” access to data while still protecting consumers’ interests and the overall security of the system.

Questions for the record from The Honorable Jerry McNerney

1. H.R. 4651, of which I am an original co-sponsor, would create a 16-person commission of experts from fields including technology, privacy, law enforcement, and national intelligence, to provide Congress with recommendations on how to ensure that law enforcement has the information it needs while also ensuring that our security is not compromised in the process. Do you support this approach?

Answer: We are encouraged by bipartisan multi-jurisdictional efforts in the House and Senate to examine the importance of strong encryption to Americans’ personal security and to the Nation’s security. The American people deserve an open and honest conversation around the important questions raised by this debate. We look forward to working with you and the Committee to further examine this issue.

2. What are the implications for U.S. competitiveness and jobs in the technology sector if American companies are forced to weaken the security of their products

Answer: The market for strong encryption is robust and global. Although the U.S. remains at the cutting-edge of this technology, strong encryption products are increasingly available around the world. If consumers no longer can count on the security of our products and the strength of the encryption technology we employ, they will obtain encryption products elsewhere, which will certainly disadvantage U.S. industry and the American public. The technology sector has been a leading exemplar of innovation and competitiveness, and we should strive to maintain both.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 2, 2016

Mr. Amit Yoran
President
RSA Security
174 Middlesex Turnpike
Bedford, MA 07130

Dear Mr. Yoran:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 19, 2016, to testify at the hearing entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Thursday, June 16, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

The Honorable Tim Murphy

1. **Often this debate appears to be about picking sides – either you support law enforcement or you support the technology community. This feels like a lose/lose proposition.**
 - a. **Do you agree that this cannot be black-and-white, us versus them, debate?** Yes
 - b. **What is necessary to move past this perception to engage in an honest, constructive dialogue moving forward?** Today's debate needs to balance the equities of, on the one hand, the needs of law enforcement to solve and prosecute crimes, sometimes heinous crimes, and, on the other hand, our security, privacy, and economic competitiveness. We do not face an either/or choice between security and privacy. All parties should agree there is a continuum of options that have to be carefully weighed as we consider the thin line that connects these issues.
 - c. **In your opinion, have we even scratched the surface of exploring new and creative solutions that acknowledge the concerns of both sides of this debate?** No, the discussion to this point has, in large part, been overly simplified or misunderstood by many. I appreciate this Committee beginning the process of examining this issue and we must all understand that 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.
2. **A lot of this debate has focused on Apple and, recently, WhatsApp. However, encryption is used by many companies and in a wide range of technologies.**
 - a. **Can you give us a sense of the uses of encryption and breadth of technologies and service this includes?** Good encryption is the basis of all security technology. RSA solutions use strong encryption algorithms to protect almost every industry and many nations. Our products are found in government agencies, banks, utilities, retailers, as well as hospitals and schools. Our business enables those we work with to effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately reduce IP theft, fraud, and cybercrime. With a world-class incident response team with expertise, battle-tested processes and sophisticated tools, we have helped hundreds of customers investigate and respond to security incidents and, more importantly, recover from advanced attacks. On a broader scale, we also regularly and rapidly disseminate threat intelligence to our customers in order to empower them to take appropriate measures to protect their company assets from the ever-changing landscape of advanced threats.

b. What is the role of encryption in securing critical infrastructure or the growing number of cyber-physical systems and Internet connected devices, otherwise known as the Internet of Things?

Good cryptosystems are the fundamental building blocks for good cyber security; without the availability of good encryption, those defending vital U.S. networks and systems would be at a massive disadvantage. This year more than 10 billion devices will connect to networks around the world. And in the next few years, that number will increase by over an order of magnitude. With the veritable explosion of smart devices, many of which connect not just to the network, but to each other, significant security concerns arise. Despite the rapidly evolving technology landscape that envelops us, the fundamentals of information security remain static. Concepts like visibility, identity, and risk continue to be mainstays. However, scaling these concepts out to the Internet of Things (IoT) requires thought. To address expected concerns as IoT devices proliferate, we must continue to innovate with security protocols and methods like security analytics.

3. When we talk about weakening encryption, how would decisions that weaken encryption in one sector – say communications or messaging – effect other forms of encryption or sectors, such as critical infrastructure or IOT devices and systems? By its very nature weakening security in one format of data or device exposes risks in every other system connected to that data or device.

a. Is it possible to increase law enforcement access to certain encrypted devices or communications without affecting encryption in all systems? How would access work? Compromises of even the most sensitive and well-protected systems occur on a regular basis. These are the breaches we see on the news and the world of breaches that we do not even know about. The technical controls and procedures required to govern and audit legitimate access introduce an even greater complexity. Whoever possesses the capability of gaining exceptional access now carries the largest target on their back. They have a need of the greatest magnitude to safeguard their own infrastructure and protect the exceptional access. We have not seen the government demonstrate this exceptional capability to date. A compromise of the “Exceptional Access” method would compromise the effectiveness of the entire system. The result might be massively destructive to society. In addition, we must think about how a US policy of exceptional access would be viewed globally. The consequences would not only be devastating to the US innovation economy but other countries are anxiously awaiting to see what we do and in some cases countries around the world will follow suit and require US companies to provide the same access to their governments.

4. Law enforcement is concerned about the growing prevalence of default encryption, as well as the use of end-to-end and/or “warrant-proof” encryption.

a. What factors are influencing the transition to default encryption?

Customer demand is driving much of the shift - be it private or government customers. It is a key best practice, in fact, required for federal government certification. There has been an enormous focus on the number of breaches occurring in the private sector and default encryption is an effective way to increase security and privacy. Regulatory agencies view encryption as part of the best practices for cybersecurity and hold their regulated companies for compliance. Our industry is being asked to defend against these breaches while providing additional access to the government. Many companies have made a decision to give customers more control over their digital security and default encryption is an effective way to do this.

5. What are the benefits of end-to-end encryption compared to alternatives such as a managed key system used by some companies to retain access to content for advertising, security scans or other purposes?

The idea behind authenticated encryption is not only to preserve the confidentiality of the underlying data, but also to ensure its authenticity and integrity; i.e., it was encrypted only by the person who had knowledge of the encryption key and no one else could have modified the data. Authenticated encryption is considered a best practice when applying encryption techniques. In other words, if the key is compromised, then all of the data ever encrypted with this key becomes compromised. A more common practice is to negotiate a new key per transaction and use your longer-term key to help ensure the authenticity and integrity of the negotiation process. Each transaction is then encrypted with a fresh key that is discarded shortly after the transaction is completed. An adversary who compromises a given key only learns the contents of a given transaction and not the transactions that preceded it (or any subsequent transactions for that matter).

a. Is there evidence that demonstrates the improvement to security or other benefits that justify or otherwise influence the use of end-to-end encryption? The proof of success is the failure to access the data.

b. Are there other factors influencing the shift to end-to-end encryption?

6. Many have suggested that law enforcement can rely on metadata as an alternative to exceptional access. Law enforcement, however, has argued that while metadata can be useful in certain circumstances, its benefits are limited in real world investigations for a number of reasons. These include, but are not limited to: challenges locating and

obtaining the necessary information; the volume and complexity of information, making it difficult to analyze; and it is less useful or compelling evidence in criminal prosecutions.

- a. **What is your understanding of law enforcement's capabilities – at the federal, state, and local levels, respectively – for utilizing metadata?** Law enforcement has access to a lot of information they need to do their jobs. Data is readily accessible to law enforcement operating through proper legal channels. There is a need for a better strategy to manage the quantity and efficiency of the information and analysis. 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 as our society's use of technology evolves.

- b. **Are there additional types of metadata or capabilities that companies do not currently provide that could improve law enforcement's ability to utilize this information?** In addition to meta-data, law enforcement can now gain access to raw content at an unprecedented level. Business is transforming faster than ever before. Technology has become the key differentiator in just about every industry, and information is the fuel. By gaining access to a customer's information, or perhaps more importantly the information of a prospective customer, companies can simply comb through such data, a process known as data-mining, and produce the most targeted information of the greatest value. This is a practice that each and every one of our industry leading corporations is utilizing. The new economy uses information to delight us. The magic of the applications we use and the utility and enjoyment we get from them are not on our computer or mobile devices. The power of modern apps and business transcends our computing platforms and occurs in the cloud. Application providers process it, and sort the unencrypted information in order to deliver the insight we want. For information efficiency and resiliency purposes, unless you very conscientiously make the deliberate effort to evade it, the majority of content you produce or interact with is accessible in a clear text form by the organization you work for and the companies you engage with in your personal capacity. This makes such information readily accessible to law enforcement operating through proper legal channels.

- c. **As more of our lives become connected to the Internet, it would seem logical to assume this only expands and enriches an individual's digital footprint – does this present an opportunity for new and creative options for law enforcement to leverage this data?**

- i. **If yes, please explain how and what options this presents law enforcement.** Yes, meta-data, which is practically impossible to protect, includes information about who you are, where you are, who you are communicating or interacting with, the length, frequency, volume and duration of your communications, what applications you are using, and other troves of information.
 - ii. **If no, please explain why not.**
 - iii. **Are there challenges or consequences to utilizing this information?** While much of this information is constitutionally protected from law enforcement collection, they can, and do, legally gain access to this information, including purchasing it from data aggregators. Law enforcement has an overwhelming volume of information readily available to it, creating challenges to efficiently manage and fully leverage it.
- 7. **Does RSA currently provide resources, training, or other expertise to law enforcement, to help them make full use of the information potentially available to them?**
 - a. **If yes, please describe these efforts.** We provide training and services tied to our products. During this training, we highlight the ability to use big data and information in a cybersecurity mission, but we don't train law enforcement on specific techniques for their law enforcement mission.
 - b. **If no, please explain why not.**
 - c. **To your knowledge, do other technology companies currently provide resources, training, or other expertise to law enforcement, to help them make full use of the information potentially available to them?** Yes, other companies provide specific training or personnel that support law enforcement's mission.
 - d. **Does this present an opportunity for improvement, both in terms of law enforcement's capabilities and also the relationship between the private sector and law enforcement?** Yes, law enforcement has the opportunity to take advantage of the many technologies and services available in the private sector if they engage in direct dialogue. However, past conversation has been focused narrowly and in the wrong direction.
- 8. **One specific concern related to metadata is the ability of smaller companies to respond to law enforcement's requests.**
 - a. **Is there a way for larger companies, who do have the knowledge and expertise, to help out there smaller peers?** It would be difficult without the smaller company incurring significant costs to retain and share this information.

- i. **If yes, please explain how this could occur and what type of assistance could be provided.**
- ii. **If no, please explain why it is not feasible.** It would not only be cost prohibitive but it would be very difficult to navigate the sharing of confidential information between companies and the government. I would refer you to a letter sent to Congressional leadership by "Engine", a policy, advocacy, and research organization supporting startups as an engine for economic growth, addressing the current debate and its impact to small technology startups.
- iii. **Does the fact that some companies struggle to provide metadata lessen the value it could provide to law enforcement, making it a less effective mitigation to the "going dark" problem?** No. An overwhelming number of requests made by law enforcement are complied with by the private sector. As technologies permeate every aspect of our daily lives, this trail has exploded in a robust and detailed journaling of our activities and communications. Our very interaction with the world around us produces a rich set of data that is continually being transmitted and produces an overwhelming amount of information and meta-data about that information. This meta-data, which is practically impossible to protect, includes information about who you are, where you are, who you are communicating or interacting with, the length, frequency, volume and duration of your communications, what applications you are using, and other troves of information.

The Honorable Richard Hudson

1. **The CEO of MSAB, a technology company, recently proposed in a Detroit News article that there is a way for the government to access data stored on our phones without building in a backdoor to the encryption. His solution is to build a two-part decryption system, where both the government and the manufacturer possess a unique decryption key. Both decryption keys would be necessary, in addition to holding the physical device in order to decrypt and access the encrypted data.**

I'm 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 technology industry, and the law enforcement community regarding a proposal like this or something similar to allow safe access to this data while still protecting consumer interests? How would access work? Compromises of even the most sensitive and well-protected systems occur on a regular basis. These are the breaches we see on the news and the world of breaches that we do not even know about. The technical controls

and procedures required to govern and audit legitimate access introduce an even greater complexity. Whoever possesses the capability of gaining exceptional access now carries the largest target on their back. They have a need of the greatest magnitude to safeguard their own infrastructure and protect the exceptional access. We have not seen the government demonstrate this exceptional capability to date. A compromise of the "Exceptional Access" method would compromise the effectiveness of the entire system. The result might be massively destructive to society.

The Honorable Jerry McNerney

- 1. H.R. 4651, of which I am an original co-sponsor, would create a 16-person commission of experts from fields including technology, privacy, law enforcement, and national intelligence, to provide Congress with recommendations on how to ensure that law enforcement has the information it needs while also ensuring that our security is not compromised in the process. Do you support this approach?** Yes, RSA is encouraged by both the Digital Security Commission Act of 2016 (H.R. 4641) and the establishment of the House Bipartisan Encryption Working Group. Both could provide industry, law enforcement, and other stakeholders with a forum to discuss the potential impact of any proposed path forward, legislative or otherwise, and balance, sometimes, competing interests.
- 2. In your testimony, you note that exceptional access would substantially increase system complexity and that this in turn would pose threats to our security. Can you explain why increasing system complexity would result in greater security risks?** As system complexity increases, so too do the risks of a compromise. In their purest form, security and complexity are typically antithetical to each other. The more complex the system the less safe it is. Each time we add a level or layer of complexity, we add potential for vulnerability. Bear in mind that it can take a significant amount of time and vetting before systems are considered to be secure enough in practice. An exceptional access system will therefore require a more significant incubation period.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 2, 2016

Dr. Matthew Blaze
Associate Professor, Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania
220 South 33rd Street
Philadelphia, PA 19104

Dear Dr. Blaze:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 19, 2016, to testify at the hearing entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Thursday, June 16, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy
Chairman

Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Attachment—Additional Questions for the Record

The Honorable Tim Murphy

1. Often this debate appears to be about picking sides – either you support law enforcement or you support the technology community. This feels like a lose/lose proposition.
 - a. Do you agree that this cannot be a black-and-white, us versus them, debate?
 - b. What is necessary to move past this perception to engage in an honest, constructive dialogue moving forward?
 - c. In your opinion, have we even scratched the surface of exploring new and creative solutions that acknowledge the concerns of both sides of this debate?
2. Are there options for assisting law enforcement – including those outside the federal government – that do not create unjustifiable vulnerabilities or otherwise irresponsibly undermine our overall security?
3. A lot of this debate has focused on Apple and, recently, WhatsApp. However, encryption is used by many companies and in a wide range of technologies.
 - a. Can you give us a sense of the uses of encryption and breadth of technologies and service this includes?
 - b. What is the role of encryption in securing critical infrastructure or the growing number of cyber-physical systems and internet connected devices, otherwise known as the Internet of Things?
3. When we talk about weakening encryption, how would decisions that weaken encryption in one sector - say communications or messaging - effect other forms of encryption or sectors, such as critical infrastructure or IOT devices and systems?
 - a. Is it possible to increase law enforcement access to certain encrypted devices or communications without affecting encryption in all systems?
4. Law enforcement is concerned about the growing prevalence of default encryption, as well as the use of end-to-end and/or “warrant-proof” encryption.
 - a. What factors are influencing the transition to default encryption?
 - b. Of those factors, in your opinion, which are the most important or influential for decision-makers in the private sector?

5. Why is default encryption valuable to the security of our digital infrastructure?
6. What are the benefits of end-to-end encryption compared to alternatives such as a managed key system used by some companies to retain access to content for advertising, security scans or other purposes?
 - a. Is there evidence that demonstrates the improvement to security or other benefits that justify or otherwise influence the use of end-to-end encryption?
 - b. Are there other factors influencing the shift to end-to-end encryption?
7. Many have suggested that law enforcement can rely on metadata as an alternative to exceptional access. Law enforcement, however, has argued that while metadata can be useful in certain circumstance, its benefits are limited in real world investigations for a number of reasons. These include, but are not limited to: challenges locating and obtaining the necessary information; the volume and complexity of information, making it difficult to analyze; and it is less useful or compelling evidence in prosecutions.
 - a. What is your understanding of law enforcement's capabilities – at the federal, state and local levels, respectively - for utilizing metadata?
 - b. Are there additional types of metadata or capabilities that companies do not currently provide that could improve law enforcement's ability to utilize this information?
 - c. As more of our lives become connected to the Internet, it would seem logical to assume this only expands and enriches an individual's digital footprint – does this present an opportunity for new and creative options for law enforcement to leverage this data?
 - i. If yes, please explain how and what options this presents law enforcement.
 - ii. If no, please explain why not.
 - iii. Are there challenges or consequences to utilizing this information?
8. To your knowledge, do technology companies currently provide resources, training, or other expertise to law enforcement, to help them make full use of the information potentially available to them?
 - a. Does this present an opportunity for improvement?
 - b. Does law enforcement currently, or could they in the future, leverage the expertise of the academic community to help find or develop tools and solutions that would allow them to better leverage metadata?
 - c. Are there other opportunities for the academic community to assist law

enforcement in keeping pace with rapidly evolving technologies?

9. One specific concern related to metadata is the ability of smaller companies to respond to law enforcement requests.
 - a. Is there a way for larger companies, who do have the knowledge and expertise, to help out their smaller peers?
 - i. If yes, please explain how this could occur and what type of assistance could be provided.
 - ii. If no, please explain why it is not feasible.
 - iii. Does the fact that some companies struggle to provide metadata lessen the value it could provide to law enforcement, making it a less effective mitigation to the “going dark” problem?
10. In the wake of the FBI’s use of a third party to access the iPhone in the San Bernardino case, there has been considerable discussion about the concept of “legal hacking.”
 - a. In terms of discovering and developing exploitable vulnerabilities, can you give us a sense of how technically difficult it is to do?
 - b. Do you believe the government either currently has, or is capable of hiring and retaining experts skilled enough to make “legal hacking” a viable solution to some of the problems discussed today?
 - c. How would this type of capability scale to individuals at the state and local level?
11. In the “Going Bright” report, you and your co-authors state that, on average, exploitable vulnerabilities remain unknown for an average of 312 days.
 - a. Are you aware of whether or not that number has increased or decreased?
 - b. Do you expect that number to change in the future? For example, are we as a society getting better at catching and patching vulnerabilities, and therefore they will be less useful in the context of “legal hacking?”
12. There are two primary types of data implicated in the “going dark” discussion, data-at-rest and data-in-transit.
 - a. From a technical and policy perspective, what are the critical differences in these two types of data?
 - b. How will those differences affect any possible solutions or mitigations to this problem?

- i. Will they require different solutions for each type of data?
13. Some devices contain a feature that users can enable to make it so that device deletes all of the data if a certain number of incorrect passcodes are tried. Absent this feature, it is my understanding that devices can be “brute-forced,” by simply trying different passcodes or passwords over and over again until the right one is found.
 - a. Do you believe this is an important feature?
 - i. If so, please explain why.
 - ii. If not, please explain why.
 - b. What are the potential consequences of removing this feature and how do you weigh those consequences against the question of law enforcement access to encrypted devices? In other words, how do you weigh the risks of removing this feature against the consequences of other potential options that have been discussed for improving law enforcement access to encrypted devices?
14. A fellow witness, Daniel Weitzner, recently wrote a post for Lawfare called “the Encryption Debate Enters Phase Two,” in which he posed two questions that society needs to answer. First, he asked what kinds of assistance technology companies can provide law enforcement agencies that come bearing lawful orders, and second, he asked what kinds of surveillance powers we should grant to our governments that preserve our values.
 - a. In your opinion, what are the answers to these two questions?
15. In your testimony, you explained that one of the ways to reduce threats to our digital infrastructure is to design that infrastructure to be as simple as possible, thereby “minimizing” the potential attack surface. You also stated that mandating a lawful access capability would run directly counter to that best practice.
 - a. How would a lawful access capability inherently complicate a product’s design?
 - i. Is this conclusion specific to the concept of a one-size-fits-all solution, such as key escrow?
 - ii. Are there ways to improve lawful access without increasing complexity or unacceptably undermining security?

The Honorable Richard Hudson

1. The CEO of MSAB, a technology company, recently proposed in a Detroit News article that there is a way for the government to access data stored on our phones without building in a backdoor to the encryption. His solution is to build a two part decryption system, where both the government and the manufacturer possess a unique decryption key. Both decryption keys would be necessary in addition to holding the physical device in order to decrypt and access the encrypted data.

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 technology industry, and the law enforcement community regarding a proposal like this or something similar to allow safe access to this data while still protecting consumer interest?

The Honorable Jerry McNerney

1. H.R. 4651, of which I am an original co-sponsor, would create a 16-person commission of experts from fields including technology, privacy, law enforcement, and national intelligence, to provide Congress with recommendations on how to ensure that law enforcement has the information it needs while also ensuring that our security is not compromised in the process. Do you support this approach?
2. In your testimony, you note that your prior work includes discovering technical flaws with the Clipper Chip in the 1990s. What lessons can we draw from the Clipper Chip experience for the encryption issues before us today?

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 2, 2016

Mr. Daniel J. Weitzner
Director, MIT Internet Policy Research Initiative
Principal Research Scientist, MIT Computer Science and Artificial Intelligence Lab
Massachusetts Institute of Technology
32 Vassar Street
Cambridge, MA 02139

Dear Mr. Weitzner:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 19, 2016, to testify at the hearing entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Thursday, June 16, 2016. Your responses should be mailed to Greg Watson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Greg.Watson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy
Chairman
Subcommittee on Oversight and Investigations

cc: Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment



Internet Policy Research Initiative
Massachusetts Institute of Technology

*Questions for the Record following hearing on "Deciphering the Debate Over Encryption:
Industry and Law Enforcement Perspectives."*

30 June 2016

Hon. Tim Murphy
Chairman, Subcommittee on Oversight and Investigations
Energy and Commerce Committee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Murphy,

Thank you for inviting me to appear before your subcommittee on the matter of "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives." Please accept these response to the questions for the record from you and your colleagues.

The Honorable Tim Murphy

1. *Often this debate appears to be about picking sides - either you support law enforcement or you support the technology community. This feels like a lose/lose proposition.*
 - a. *Do you agree that this cannot be a black-and-white, us versus them, debate?*
 - b. *What is necessary to move past this perception to engage in an honest, constructive dialogue moving forward?*
 - c. *In your opinion, have we even scratched the surface of exploring new and creative solutions that acknowledge the concerns of both sides of this debate?*

This is not a black and white debate. There are a number of worthwhile and creative investigative techniques that can be found that will meet many law enforcement needs without impairing security, privacy or global competitiveness. However, in order for the debate to move beyond the rhetoric, we must begin to formalize the debate through a more precise and technically-specific assessment of the challenges that law enforcement faces, rather than trying to impose a one-size-fits all regulatory solution on a exceedingly diverse and rapidly changing technology environment.

2. *Are there options for assisting law enforcement - including those outside the federal government - that do not create unjustifiable vulnerabilities or otherwise irresponsibly undermine our overall security?*

There are a number of ways to enhance law enforcement's investigative capabilities that do not poke further holes in our overall security. For instance, law enforcement can develop technical expertise in computer security such that they have the ability, where lawful, necessary and proper, to exploit systems that they discover locally. We have seen in the San Bernardino case that lawful hacking techniques can prove to be a useful tool to enable law enforcement to gather investigative information even when that information is protected by strong encryption. No security system is perfect. Therefore, in many cases there will be ways to recover data or infer its contents without requiring that service providers keep keys to decrypt all information.

3. *A lot of this debate has focused on Apple and, recently, WhatsApp. However, encryption is used by many companies and in a wide range of technologies.*
- a. *Can you give us a sense of the uses of encryption and breadth of technologies and service this includes?*
 - b. *What is the role of encryption in securing critical infrastructure or the growing number of cyber-physical systems and internet connected devices, otherwise known as the Internet of Things?*

It is almost easier to list the set of technologies that do not need to use encryption than to enumerate all that depend on cryptography. For instance, every application on nearly every computer used by individuals and enterprises requires software updates, but to ensure that this update does not contain malware, it must be cryptographically verified. Similarly, any time you use a browser to interact with a website, that website must be end-to-end encrypted or you will run the risk of running malicious code from an adversary, or having your credentials stolen by a malicious middleman.

These are far from hypothetical risks. As discussed in my testimony, failing to cryptographically verify updates through this code-signing process can lead to developer's software being subverted to spread malware. Flame, a sophisticated nation-state malware campaign discovered in 2012, exploited outdated cryptography in Microsoft Update to infect Windows PCs. Apple failure to cryptographically verify updates to iTunes turned the program into an infection point for the FinFisher virus, which was then found to be in use by oppressive governments spying on local dissidents. Most recently, an update framework used 78 by hundreds of OS X apps was found to be vulnerable to these exact same sorts of attacks, leaving thousands of users at risk of losing complete control of their computers, including anything they access on that device - bank accounts, private chat, email accounts, health records, and social media.

There have also been many examples of interception of account information from websites or apps that do not encrypt their data in transit. For instance, as recently as 2010, major websites

including Facebook, Google, LinkedIn, and Reddit failed to encrypt connections to their sites using HTTP over an encrypted protocol, known as HTTPS. This failure made those sites vulnerable to "session hijacking attacks" that allowed attackers watching the network to gain access to user accounts. Such attacks were not difficult to execute, for instance, an easily installable Firefox plugin called Firesheep allowed anyone in the vicinity of an unencrypted wifi connection to gain access to unsuspecting users' email, social media, and bank accounts with a literal click of a button. To see how far reaching this vulnerability could be, think of all the times users connect to an untrusted airport wifi hotspot to download an app, to check email, access health records, or converse with friends. Strong encryption makes it possible for that user to do so without needing to fully trust the myriad of devices and organizations between his or her device and the service being accessed. Conversely, without encryption, a malicious middleman such as the wifi router owner, the Internet service provider, or a disgruntled network administrator could easily gain control of an unsuspecting user's computer or bank account.

So-called Internet of Things systems will have even greater dependency on strong encryption. At the technical level, IoT devices are very similar to normal computing devices, and therefore require the same update processes and secure communication that your everyday laptop does. However, it is more likely that such systems will remain unmonitored by a user, while maintaining always-on sensors such as a microphone or camera. Updates and telemetry data passed between devices and the manufacturer must therefore be encrypted and verified to avoid incredibly damaging consequences --- when someone hacks into a laptop they might be access to your tax returns or your love-letters, but a hacker with access to an IoT device such as a home thermostat or kitchen oven can potentially burn down the house.

4. *When we talk about weakening encryption, how would decisions that weaken encryption in one sector - say communications or messaging - effect other forms of encryption or sectors, such as critical infrastructure or IoT devices and systems?*
 - a. *Is it possible to increase law enforcement access to certain encrypted devices or communications without affecting encryption in all systems?*

Today's computer software -- whether consumer-oriented apps or enterprise-style database systems -- is built from a set of widely used interchangeable parts known as software libraries. Today, there are only a few cryptography libraries used in production. Writing good crypto code is difficult. Correct implementation of cryptographic algorithms requires deep computer science and systems-level knowledge, so applications almost always rely on third party libraries or services to encrypt both data at rest and in transit. In fact, the difficulty in implementing cryptography has led to very few implementations of these frameworks. Almost every Android device uses one of two libraries. Bugs introduced in such cryptographic frameworks (like Android's libraries) would therefore proliferate to vulnerabilities in seemingly unrelated apps (like your banking or email app). Given the realities of today's software development environment it is not possible to quarantine law enforcement accessible systems to only consumer-grade technologies. These weakened software components would almost certainly find their way into IoT and SCADA systems as well.

5. *Law enforcement is concerned about the growing prevalence of default encryption, as well as the use of end-to-end and/or "warrant-proof" encryption.*
- a. *What factors are influencing the transition to default encryption?*
 - b. *Of those factors, in your opinion, which are the most important or influential for decision-makers in the private sector?*

Internet users and enterprise software customers are demanding strong encryption because of a widespread and well-founded recognition of increased cybersecurity risk. Consider smart phone users who put more and more personal information on mobile devices, including emails, bank account information, personal location, family photos, etc. The economic value of stealing a person's phone today goes far beyond the value of the physical phone.

Meanwhile, the usability costs of default encryption have gone down. Device battery life has increased, as well as computing efficiency, meaning that the intensive math required to employ strong encryption has become easy to do on almost all devices.

Second, the push to ubiquitous encryption is also well motivated by the litany of systemic vulnerabilities resulting from a history of hardware and software vendors failing to encrypt and/or cryptographically verify data. The damage from failures to properly encrypt data has been exacerbated by the slow and arduous pace of eliminating bad code once it has been added to the overall software ecosystem.

The combination of these two factors has led the security community to advocate applying encryption and authentication as much as is possible, since failing to do so has been repeatedly shown to cause serious damage to user security and privacy.

However, the transition to on-by-default end-to-end encryption has only partially happened, and may well not happen fully. Where data is held in an environment deemed to be trusted, the costs of key management necessary to encrypt enterprise data at rest may not be seen as justified by users. It is difficult, for instance, to create usable encrypted backup storage solutions. Indeed, Apple's iCloud backs up user data to an unencrypted store. Further, other companies often provide services that use the metadata and data the user provides for analytics and ad revenue. It is not clear why these incentives would change drastically in the near term. That every single data storage and communication component will not be fully encrypted creates opportunities for law enforcement to get lawful access to sensitive data.

6. *Why is default encryption valuable to the security of our digital infrastructure?*

See answer to number 3.

7. *What are the benefits of end-to-end encryption compared to alternatives such as a managed key system used by some companies to retain access to content for advertising, security scans or other purposes?*
- a. *Is there evidence that demonstrates the improvement to security or other benefits that justify or otherwise influence the use of end-to-end encryption?*
 - b. *Are there other factors influencing the shift to end-to-end encryption?*

True user-to-user encrypted connections protect individuals and enterprises against insiders who might misuse data, or attackers who have managed to get into a service provider's network. An adversary that's wormed his way into a cloud services platform such as Google or Amazon Web Services will be able to access all user data. Enterprise customers using cloud services will want to be sure that at their data is encrypted with keys not available to the cloud services provider as a way to minimize the risk of insider threat arising from either malicious employees or security breaches on the part of the cloud provider. However, the enterprise customer itself may retain the ability to decrypt data without the knowledge or control of individual users in the enterprise.

Some of the difficulty with this debate is the lack of formalism in the definition of what actually constitutes an "end." The term "end-to-end" originally comes from computer networking,¹ in which a client (eg your computer) communicates with a server (e.g. Google's email server). End to end encryption in this context would be an encrypted connection between your computer and Google. If we define "end-to-end" to mean user-to-user (as in, an encrypted email from you to your friend) it takes on a different set of security properties than those encrypted from client to server.

8. *Many have suggested that law enforcement can rely on metadata as an alternative to exceptional access. Law enforcement, however, has argued that while metadata can be useful in certain circumstance, its benefits are limited in real world investigations for a number of reasons. These include, but are not limited to: challenges locating and obtaining the necessary information, the volume and complexity of information, making it difficult to analyze, and it is less useful or compelling evidence in prosecutions.*
- a. *What is your understanding of law enforcement's capabilities - at the federal, state and local levels, respectively - for utilizing metadata?*

We do not have access to information about the internal capabilities of the federal, state, or local law enforcement. However, it is likely that law enforcement could use additional resources to further integrate computer security researchers and developers into law enforcement at all levels. A few questions that are worth asking law enforcement on the subject:

¹ J. H. Saltzer, D. P. Reed, and D. D. Clark. 1984. [End-to-end arguments in system design](#). *ACM Trans. Comput. Syst.* 2, 4 (November 1984), 277-288. This is the original paper that introduced the concept of "end to end" arguments in computer science.

- Are there examples from investigations where metadata analysis either failed or succeeded in supplementing access to content that was impeded by encryption?
 - What is the capacity of federal law enforcement to provide data analysis assistance to local and state?
 - Does law enforcement at all or any level have the capability to build and retain skilled technical teams devoted to media exploitation and analysis? What metrics do law enforcement agencies have on their ability to recruit and retain talent?
 - What opportunities currently exist in law enforcement organizations for recruitment and competitive compensation of talented technical staff?
- b. Are there additional types of metadata or capabilities that companies do not currently provide that could improve law enforcement's ability to utilize this information? As more of our lives become connected to the Internet, it would seem logical to assume this only expands and enriches an individual's digital footprint - does this present an opportunity for new and creative options for law enforcement to leverage this data?*
- i. If yes, please explain how and what options this presents law enforcement.*
 - ii. If no, please explain why not.*
 - iii. Are there challenges or consequences to utilizing this information?*

In general, nearly any data that a company collects now is already subject to law enforcement access under either a subpoena, 'reasonable articulable suspicion', or probable cause standard, depending on the nature of the information. It is unclear whether or not law enforcement actually requires more data or more advanced investigative techniques to take advantage of existing data. In order to make good use of this data, law enforcement may need additional analytic tools and technologies. In order to protect privacy and civil liberties, we must assure that there are both legal and technical protections in place to assure that law enforcement has access to the right information under the proper legal standard, and that the data is only used for legally authorized purposes.

9. *To your knowledge, do technology companies currently provide resources, training, or other expertise to law enforcement, to help them make full use of the information potentially available to them?*
- a. Does this present an opportunity for improvement?*
 - b. Does law enforcement currently, or could they in the future, leverage the expertise of the academic community to help find or develop tools and solutions that would allow them to better leverage metadata?*
 - c. Are there other opportunities for the academic community to assist law enforcement in keeping pace with rapidly evolving technologies?*

We have not studied this question.

10. One specific concern related to metadata is the ability of smaller companies to respond to law enforcement requests.

- a. Is there a way for larger companies, who do have the knowledge and expertise, to help out their smaller peers?
 - i. If yes, please explain how this could occur and what type of assistance could be provided.
 - ii. If no, please explain why it is not feasible.
 - iii. Does the fact-that some companies struggle to provide metadata lessen the value it could provide to law enforcement, making it a less effective mitigation to the "going dark" problem?

Companies asked to provide metadata may face at two different challenges. The first is technical --- even when a software firm has unencrypted access to a data set, it does not mean that it has been actively collecting it in a way that might be easily searchable and retrievable for timely response. If significant system re-design is required, then it is not clear that third parties will have the ability or incentive to help in this regard.

The second is set of challenges are in the legal and administrative domain. As Internet services and app-based communications take their place alongside traditional telecommunications services, the effective operation of electronic surveillance law will depend on the ability to scale from a small number of large, vertically-integrated network operators to a large number of small service providers that may have difficulty in responding to law enforcement requests. Responsible compliance with surveillance law does have costs and requires application of legal expertise. Many small providers will not have the resources to hire legal and technical staff to comply with surveillance requests. If compliance costs and uncertainties are high, both law enforcement and privacy interests stand to lose. Compliance will be haphazard and unaccountable, with some firms erring on the side of privacy, and others on the side of law enforcement. However, if the legal rules and administrative mechanisms are sufficiently clear, then it will be possible for third-party services to develop to enable smaller firms to outsource their surveillance compliance to either law firms or specialized trusted third parties such as those that came onto the market after CALEA was enacted. But no third party market will develop if compliance requires extensive subjective legal judgment.

11. In your opinion, what are the top three policy considerations related to legal hacking?
 - a. What are the potential downsides to the use of legal hacking?
 - i. In your opinion, do they outweigh the potential benefits?
 - b. Is legal hacking a "solution"? Or is it one of a suite of potential options for law enforcement?
 - c. How would this type of capability scale to individuals at the state and local level?

These are three policy questions raised by the prospect of "lawful hacking."

First, who will be responsible to be sure that exploits used by law enforcement do no harm innocent users? There is an inherent conflict of interest between law enforcement investigators who want to succeed in a specific investigation and the broader needs of the public to be free from known but possibly hidden security vulnerabilities. Will courts have the technical expertise to make such judgments with the public interest in mind?

Second, once an exploit is used in an authorized hacking event, what rules should govern when and whether to disclose the vulnerability so that other users are not subject to the same risks? When should vulnerabilities be disclosed? The vulnerabilities equities process is currently encumbered by security classification rules. If the process is to be used widely there will be no way to have adequate oversight if all of the information is classified.

Third, it is unlikely that the FBI's Remote Operations Unit (ROU) is currently capable of providing adequate lawful hacking tools and support to all state and local law enforcement agencies. How would the FBI prioritize assistance to state and local police?

12. *There are two primary types of data implicated in the "going dark" discussion, data-at-rest and data-in-transit.*
- a. *From a technical and policy perspective, what are the critical differences in these two types of data?*
 - b. *How will those differences affect any possible solutions or mitigations to this problem?*
 - i. *Will they require different solutions for each type of data?*

There is considerable risk in trying to make policy based on technical distinctions which appear, at this moment in time, to be fixed, but will certainly change over time. Whether data is in motion or at rest will be a function of change engineering requirements over time, not necessarily reflective of any inherent privacy or security requirement. For example, when surveillance of electronic mail was first addressed by Congress, it was a 'store-and-forward' medium, meaning that it was principally data in motion. However now most email is actually stored in place for most of its life cycle. Policymakers should define functional requirements that define the security, privacy and surveillance requirements of service providers, law enforcement and users, rather than relying on technical implementation details, which are certain to change.

13. *Some devices contain a feature that users can enable to make it so that device deletes all of the data if a certain number of incorrect passcodes are tried. Absent this feature, it is my understanding that devices can be brute-forced, by simply trying different passcodes or passwords over and over again until the right one is found.*
- a. *Do you believe this is an important feature?*
 - i. *If so, please explain Why.*
 - ii. *If not, please explain Why.*

This is a very important security feature for a variety of both hardware and software applications. If this weren't a feature, physical access to the device would always mean having access to the device's contents because it is possible to try every possible password until chancing on the correct one. This is known as a 'brute force' attack. Any time a user loses or has their device stolen, that user could lose access to his or her bank accounts, email, and social network. This would be unacceptable.

14. What are the potential consequences of removing this feature and how do you weigh those consequences against the question of law enforcement access to encrypted devices? In other words, how do you weigh the risks of removing dns feature against the consequences of other potential options that have been discussed for improving law enforcement access to encrypted devices?

As stated above, without these limits against brute force, physical access to the device would always mean having access to the device's contents. Any time a user loses or has their device stolen, that user could lose access to his or her bank accounts, email, and social network. This would be unacceptable.

Further, any restriction on this would be made ineffective on devices with longer passwords. A four character password is trivially brute-forceable, but there are 94^{16} possible 16 character passwords. In other words, if we assume that a password check could be done every millisecond, a 16 character password would likely take approximately 10^{25} minutes or 2×10^{19} years to find it. That exceeds the average lifespan of mobile device users, and indeed, human history.

15. You recently wrote a post for Lawfare called the "Encryption Debate Enters Phase Two," in which you posed two questions that society needs to answer. First, you asked what kinds of assistance technology companies can provide law enforcement agencies that come bearing lawful orders, and second, you asked what kinds of surveillance powers we should grant to our governments that preserve our values.
a. In your opinion, what are the answers to these two questions?

The answer to the first question regarding the kinds of assistance that companies should be required to give to law enforcement is discussed in answer to question 10. The answer to the second question must begin with a commitment to transparency and public accountability, along with full commitment to Constitutional values. Of particular importance in the global Internet is for the United States and other democratic nations to implement surveillance law in a manner that gives Internet users around the world confidence that their privacy is being protected. United States surveillance law, thanks to our longstanding Fourth Amendment tradition with independent judicial review is a legal framework to be proud of. We must, however, assure that

there are visible accountability mechanisms in place to set a high standard for the rest of the world and assure continued trust in United States based Internet services.

The Honorable Richard Hudson

1. *The CEO of MSAB, a technology company, recently proposed in a Detroit News article that there is a way for the government to access data stored on our phones without building in a backdoor to the encryption. His solution is to build a two part decryption system, where both the government and the manufacturer possess a unique decryption key. Both decryption keys would be necessary in addition to holding the physical device in order to decrypt and access the encrypted data.*
2. *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 technology industry, and the law enforcement community regarding a proposal like this or something similar to allow safe access to this data while still protecting consumer interest?*

My colleagues and I wrote a larger blog post on this issue entitled "[Warning Signs: A Checklist for Recognizing Flaws of Proposed 'Exceptional Access' Systems](#)" that addresses exactly this kind of suggested system. To put it bluntly, implementing this sort of escrow system is much more complex than MSAB's CEO has implied. It is of course possible to implement such a system, but it is likely not possible to do so without incredibly significant security risks. What, for instance, happens when a private key is lost to an intelligence adversary? What happens when a device crosses international borders; how do we ensure that a Russian escrow key system isn't used in the US?

During the question and answer session at the hearing, there was extensive discussion about the analogy between bank safe deposit boxes and encryption systems. Members of the committee asked the important question: if the United States legal system has managed to provide law enforcement exceptional access to bank safe deposit boxes, then why can't we do the same thing for encryption systems? How is it that we can assure government access to safe deposit boxes (upon presentation of an appropriate court order) but not to encrypted communications. From a security perspective, main difference between the bank safe deposit box and encryption systems is that in the case of encrypted digital systems, we are all, effectively, using the same digital vault. So a technical flaw or administrative weakness in the means by which government gets access to the data in the digital vault puts every single use of that system around the world at risk. If the technique by which the government gets access to digital data falls into the wrong hands, all users of that system are vulnerable. By contrast, a bank robber may be equipped with the same drill used to give the government access to the private contents of a safe deposit box, that robber will still have to go from bank to bank to bank to steal from a large number of people. But in the digital world, if that secret key comes into the hands of a criminal, it can be used against numerous users very quickly.

The Honorable Jerry McNerney

H.R. 4651, of which I am an original co-sponsor, would create a 16-person commission of experts from fields including technology, privacy, law enforcement, and national intelligence, to provide Congress with recommendations on how to ensure that law enforcement has the information it needs while also ensuring that our security is not compromised in the process. Do you support this approach?

A public, technically-informed bi-partisan consideration of these issues is indeed called for. While we are not here to take position on specific legislation, myself and my staff would be more than happy to help this commission in any way.

* * * * *

