THE ENCRYPTION TIGHTROPE: BALANCING AMERICANS' SECURITY AND PRIVACY

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MARCH 1, 2016

Serial No. 114–78

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

98–899 PDF WASHINGTON : 2016

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 THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
MIMI WALTERS, California
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
DAVE TROTT, Michigan
MIKE BISHOP, Michigan

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
SCOTT PETERS, California

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

CONTENTS

MARCH 1, 2016

OFFICIAL HEARING RECORD

UNPRINTED MATERIAL SUBMITTED FOR THE HEARING RECORD

Material submitted by the Honorable Zoe Lofgren, a Representative in Congress from the State of California, and Member, Committee on the Judiciary. This submission is available at the Committee and can also be accessed at:

http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104573

Material submitted by Bruce Sewell, Senior Vice President and General Counsel, Apple, Inc. This submission is available at the Committee and can also be accessed at:

http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104573

THE ENCRYPTION TIGHTROPE: BALANCING AMERICANS' SECURITY AND PRIVACY

TUESDAY, MARCH 1, 2016

HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
Washington, DC.

The Committee met, pursuant to call, at 1:05 p.m., in room 2141, Rayburn House Office Building, the Honorable Bob Goodlatte (Chairman of the Committee) presiding.

Present: Representatives Goodlatte, Sensenbrenner, Chabot, Issa, King, Jordan, Poe, Chaffetz, Marino, Gowdy, Labrador, Collins, DeSantis, Walters, Buck, Conyers, Nadler, Lofgren, Cohen, Johnson, Chu, Deutch, Gutierrez, Bass, Richmond, DelBene, Jeffries, Cicilline, and Peters.

Staff Present: (Majority) Shelley Husband, Chief of Staff & General Counsel; Branden Ritchie, Deputy Chief of Staff & Chief Counsel; Zachary Somers, Parliamentarian & General Counsel; Kelsey Williams, Clerk; Caroline Lynch, Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Ryan Breitenbach, Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; (Minority) Perry Apelbaum, Staff Director & Chief Counsel; Danielle Brown, Parliamentarian & Chief Legislative Counsel; Aaron Hiller, Chief Oversight Counsel; Joe Graupensperger, Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; James Park, Chief Counsel, Subcommittee on the Constitution; David Greengrass, Counsel; Eric Williams, Crime Detailee; and Veronica Eligan, Professional Staff Member.

Mr. GOODLATTE. We'd ask all the members of the media that are taking thousands of pictures here, I'm sure they got some excellent ones of the Director, but we ask you to please clear aside so we can begin the hearing.

The Judiciary Committee will come to order. And without objection, the Chair is authorized to declare recesses of the Committee at any time. We welcome everyone to this afternoon's hearing on The Encryption Tightrope: Balancing Americans' Security and Privacy. And I will begin by recognizing myself for an opening statement.

We welcome everyone today to this timely and important hearing on encryption. Encryption is a good thing. It prevents crime, it prevents terrorist attacks, it keeps our most valuable information safe, yet it is not used as effectively today as is necessary to protect

against the ever-increasing sophistication of foreign governments, criminal enterprises, and just plain hackers.

We see this manifest almost every week in the reports of losses of massive amounts of our most valuable information from government agencies, retailers, financial institutions, and average Americans. From identity theft, to the compromising of our infrastructure, to our economic and military security, encryption must play an ever-increasing role, and the companies that develop it must be encouraged to increase its effectiveness.

Encryption is a topic that may sound arcane, or only the province of techies, but, in fact, it is a subject whose solutions will have far-reaching and lasting consequences. The Judiciary Committee is a particularly appropriate forum for this congressional debate to occur. As the Committee of exclusive jurisdiction over the United States Constitution, the Bill of Rights, and the Federal Criminal Laws and Procedures, we are well-versed in the perennial struggle between protecting Americans' privacy and enabling robust public safety.

This Committee is accustomed to addressing many of the significant legal questions arising from laws that govern surveillance and government access to communications, particularly the Wiretap Act, the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, and the Communications Assistance to Law Enforcement Act, otherwise known as CALEA.

Today's hearing is a continuation of the Committee's work on encryption, work that Congress is best suited to resolve. As the hearing title indicates, society has been walking a tightrope for generations in attempting to balance the security and privacy of Americans' communications with the needs of our law enforcement and intelligence agencies. In fact, the entire world now faces a similar predicament, particularly as our commerce and communications bleed over international boundaries on a daily basis.

Encryption in securing data in motion, and in storage, is a valuable technological tool that enhances Americans' privacy, protects our personal safety and national security, and ensures the free flow of our Nation's commerce. Nevertheless, as encryption has increasingly become a ubiquitous technique to secure communications among consumers, industry, and governments, a national debate has arisen concerning the positive and negative implications for public safety and national security.

This growing use of encryption presents new challenges for law enforcement seeking to obtain information during the course of its investigations, and, even more foundationally, test the basic framework that our Nation has historically used to ensure a fair and impartial evaluation of legal process used to obtain evidence of a crime.

We must answer this question: How do we deploy ever stronger, more effective encryption without unduly preventing lawful access to communications of criminals and terrorists intent on doing us harm? This now seems like a perennial question that has challenged us for years. In fact, over 15 years ago, I led congressional efforts to ensure strong encryption technologies, and to ensure that the government could not automatically demand a backdoor key to encryption technologies. This enabled the U.S. encryption market

to thrive and produce effective encryption technologies for legitimate actors rather than see the market head completely overseas to companies that do not have to comply with basic protections. However, it is also true that this technology has been a devious tool of malefactors.

Here is where our concern lies: Adoption of new communications technologies by those intending harm to the American people is outpacing law enforcement's technological capability to access those communications in legitimate criminal and national security investigations.

Following the December 15 terrorist attack in San Bernardino, California, investigators recovered a cell phone owned by the County government, but used by one of the terrorists responsible for the attack. After the FBI was unable to unlock the phone and recover its contents, a Federal judge ordered Apple to provide reasonable technical assistance to assist law enforcement agents in obtaining access to the data on the device, citing the All Writs Act as its authority to compel.

Apple has challenged the court order, arguing that its encryption technology is necessary to protect its customers' communications, security, and privacy, and raising both constitutional and statutory objections to the Magistrate's order.

This particular case has some very unique factors involved, and, as such, may not be an ideal case upon which to set precedent. And it is not the only case in which this issue is being litigated. Just yesterday, a magistrate judge in the Eastern District of New York ruled that the government cannot compel Apple to unlock an iPhone pursuant to the All Writs Act.

It is clear that these cases illustrate the competing interests at play in this dynamic policy question, a question that is too complex to be left to the courts and must be answered by Congress. Americans surely expect that their private communications are protected. Similarly, law enforcement's sworn duty is to ensure that public safety and national security are not jeopardized if possible solutions exist within their control.

This body, as well, holds its own constitutional prerogatives and duties. Congress has a central role to ensure that technology advances so as to protect our privacy, help keep us safe, and prevent crime and terrorist attacks. Congress must also continue to find new ways to bring to justice criminals and terrorists. We must find a way for physical security not to be at odds with information security. Law enforcement must be able to fight crime and keep us safe, and this country's innovative companies must, at the same time, have the opportunity to offer secure services to keep their customers safe.

The question for Americans and lawmakers is not whether or not encryption is essential, it is; but instead, whether law enforcement should be granted access to encrypted communications when enforcing the law and pursuing their objectives to keep our citizens safe.

I look forward to hearing from our distinguished witnesses today as the Committee continues its oversight of this real-life dilemma facing real people all over the globe.

It's now my pleasure to recognize the Ranking Member of the Committee, the gentleman from Michigan, Mr. Conyers, for his opening statement.

Mr. CONYERS. Thank you, Chairman Goodlatte. Members of the Committee and our first and distinguished guest, I want to associate myself with your comments about our jurisdiction. It is not an accident that the House Judiciary Committee is the Committee of primary jurisdiction with respect to the legal architecture of government surveillance.

In times of heightened tension, some of our colleagues will rush to do something, anything, to get out in front of an issue. We welcome their voices in the debate, but it is here, in this Committee room, that the House begins to make decisions about the tools and methods available to law enforcement.

I believe that it is important to say up front, before we get into the details of the Apple case, that strong encryption keeps us safe, even as it protects our privacy. Former National Security Agency Director, Michael Hayden, said only last week that America is more secure with unbreakable end-to-end encryption. In this room, just last Thursday, former Secretary of Homeland Security, Michael Chertoff, testified that in his experience, strong encryption laws help law enforcement more than it hinders any agency in any given case.

The National Security Council has concluded that the benefits to privacy, civil liberties, and cybersecurity gained from encryption outweigh the broader risks created by weakening encryption. And Director Comey himself has put it very plainly: universal, strong encryption will protect all of us, our innovation, our private thoughts, and so many other things of value, from thieves of all kinds. We will all have lock boxes in our lives that only we can open, and in which we can store all that is valuable to us. There are lots of good things about this.

Now for years, despite what we know about the benefits of encryption, the Department of Justice and the Federal Bureau of Investigation have urged this Committee to give them the authority to mandate that companies create backdoors into their secure products.

I have been reluctant to support this idea for a number of reasons. The technical experts have warned us that it is impossible to intentionally introduce flaws into secure products, often called backdoors, that only law enforcement can exploit to the exclusion of terrorists and cyber criminals. The tech companies have warned us that it would cost millions of dollars to implement and replace them at a competitive disadvantage around the world. The national security experts have warned us that terrorists and other criminals will simply resort to other tools entirely outside the reach of our law enforcement and intelligence agencies.

And I accept that reasonable people can disagree with me on each of these points, but what concerns me, Mr. Chairman, is that in the middle of an ongoing congressional debate on this subject, the Federal Bureau of Investigation would ask a Federal magistrate to give them the special access to secure products that this Committee, this Congress, and the Administration have so far refused to provide.

Why has the government taken this step and forced this issue? I suspect that part of the answer lies in an email obtained by The Washington Post and reported to the public last September. In it, a senior lawyer in the intelligence community writes that although the legislative environment toward encryption is very hostile today, it could turn in the event of a terrorist attack or a criminal event where strong encryption can be shown to have hindered law enforcement. He concluded that there is value in keeping our options open for such a situation.

I'm deeply concerned by this cynical mind-set, and I would be deeply disappointed if it turns out that the government is found to be exploiting a national tragedy to pursue a change in the law.

I also have doubts about the wisdom of applying the All Writs Act, enacted in 1789, codified in 1911, and last applied to a communications provider by the Supreme Court in 1977, to a profound question about privacy and modern computing in 2016. I fear that pursuing this serious and complex issue through the awkward use of an inept statute was not, and is not, the best course of action, and I'm not alone in this view.

Yesterday, in the Eastern District of New York, a Federal judge denied a motion to order Apple to unlock an iPhone under circumstances similar to those in San Bernardino. The court found that the All Writs Act, as construed by the government, would confer on the courts an overbroad authority to override individual autonomy. However, nothing in the government's argument suggests any principal limit on how far a court may go in requiring a person, or company, to violate the most deeply rooted values.

We could say the same about the FBI's request in California. The government's assertion of power is without limiting principle, and likely to have sweeping consequences, whether or not we pretend that the request is limited to just this device or just this one case.

This Committee, and not the courts, is the appropriate place to consider those consequences, even if the dialogue does not yield the results desired by some in the law enforcement community. I'm grateful that we are having this conversation today back in the forum in which it belongs, the House Judiciary Committee. And so I thank the Chairman very much. And I yield back.

Mr. GOODLATTE. Thank you, Mr. Conyers.

And without objection, all other Members' opening statements will be made a part of the record.

We welcome our distinguished witness of today's first panel. And if you would please rise, I'll begin by swearing you in.

Do you swear that the testimony that you are about to give shall be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. COMEY. I do.

Mr. GOODLATTE. Thank you very much. Please be seated.

I'll now begin by introducing our first distinguished witness today, Director James Comey of the Federal Bureau of Investigation. Director Comey began his career as an Assistant United States Attorney for both the Southern District of New York and the Eastern District of Virginia. After the 9/11 terrorist attacks, Director Comey returned to New York to become the United States Attorney for the Southern District of New York. In 2003, he was ap-

pointed deputy attorney general under the United States Attorney General, John Ashcroft.

Director Comey is a graduate of the College of William & Mary and the University of Chicago Law School.

Director, welcome. Your entire written statement will be made a part of the record. And I ask that you summarize your testimony in 5 minutes. And we have the timing light that you're well familiar with on the table. Again, welcome. We're pleased that you are here, and you may begin your testimony.

TESTIMONY OF HONORABLE JAMES B. COMEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. COMEY. Thank you so much, Mr. Chairman, Mr. Conyers. Thank you for hosting this conversation, and for helping us all talk about an issue that I believe is the hardest issue I've confronted in government, which is how to balance the privacy we so treasure, that comes to us through the technology that we love, and also achieve public safety, which we also all very much treasure.

I worry a little bit that we've been talking past each other, both folks in the government and folks in the private sector, when it comes to this question of encryption, which we in the government call "going dark." What I'd like to do is just take 3 or 4 minutes and try to frame how I think about it, in a way I hope is fair, fair-minded, and if it's not, I hope you'll poke at me and tell me where you think it's not, but these are the things I believe to be true:

First, that the logic of encryption will bring us, in the not-too-distant future, to a place where all of our conversations and all of our papers and effects are entirely private; that is, where no one can listen to our conversations, read our texts, read our emails unless we say so, and no one can look at our stuff, read our documents, read things we file away without our agreement. That's the first thing I believe, that the logic of encryption is taking us there.

The second thing I believe is, as both you and Mr. Conyers said, there's a lot of good about this, a lot of benefits to this. All of us will be able to keep private and keep protected from thieves of all kinds, the things that matter most to us, our ideas, our innovation, our secret thoughts, our hopes, our dreams. There is a lot to love about this. We will all be able to have storage spaces in our life that nobody else can get into.

The third thing I believe is that there are many costs to this. For the last two centuries, public safety in this country has depended, in large measure, on the ability of law enforcement agents going to courts and obtaining warrants to look in storage areas or apartments, or to listen with appropriate predication oversight to conversations. That is the way in which law enforcement brings us public safety. It is very, very important, and it's been part of the balance in ordered liberty, that sometimes the people's stuff can be looked at, but only with predication and only with oversight and approval by an independent judiciary.

The fourth thing I believe is that these two things are in tension in many contexts, increasingly in our national security work, and in law enforcement work, generally across the country. We see it obviously in ISIL's efforts to reach into this country, and using mobile messaging apps that are end-to-end encrypted, task people to

kill innocent people in the United States. That is a huge feature of our national security work and a major impediment to our counterterrorism work, because even with a court order, what we get is unreadable; to use a technical term, it's gobbledygook. Right? We cannot decrypt that that which is covered by strong encryption.

We also see it in criminal work across the country. We see very tragically last year in Baton Rouge where a pregnant woman 8 months pregnant was killed by somebody she opened the door to. And her mom says she kept a diary, but it's on her phone, which is locked, and so the case remains unsolved.

And most recently and most prominently, as both Mr. Conyers and the Chairman mentioned, we see it in San Bernardino, a case where two terrorists, in the name of ISIL, killed 14 people and wounded 22 others at an office gathering and left behind three phones, two of which, the cheaper models, they smashed beyond use, and the third was left locked.

In any investigation that is done competently, the FBI would try to get access to that phone. It's important that it's a live, ongoing terrorism investigation, but in any criminal investigation, a competent investigator would try and use all lawful tools to get access to that device, and that's what you see happening in San Bernardino.

The San Bernardino case is about that case. It obviously highlights the broader issue and, of course, it will we looked upon by other judges and other litigants, but it is about the case and trying to do a competent job of understanding, is there somebody else? And are there clues to what else might have gone on here? That is our job.

The fifth thing I believe is that democracies resolve these kind of really hard questions through robust debate. I think the FBI's job is very, very limited. We have two jobs. The first is to investigate cases like San Bernardino, and to use tools that are lawful and appropriate. The second thing, it's our job to tell the American people, the tools you are counting on us to use to keep you safe are becoming less and less effective.

It is not our job to tell the American people how to resolve that problem. The FBI is not some alien force imposed upon America from Mars. We are owned by the American people, we only use the tools that are given to us under the law. And so our job is simply to tell people there is a problem. Everybody should care about it, everybody should want to understand if there are warrant-proof spaces in American life. What does that mean? And what are the costs of that and how do we think about that?

I don't know what the answer is. It may be the American people, through Congress and the courts, decide it's too hard to solve, or law enforcement can do its job well enough with strong encryption covering our communications and our papers and effects, or that it's something that we have to find a way to fix to achieve a better balance. I don't know. My job is to try to offer thoughtful explanations about the tools the FBI has, and to bring them to the attention of the American people, and then answer questions about that.

So I'm very, very grateful for this forum, very, very grateful for this conversation. There are no demons in this debate. The compa-

nies are not evil, the government's not evil. You have a whole lot of good people who see the world through different lenses, who care about things, all care about the same things, in my view. The companies care about public safety, the FBI cares about innovation and privacy. We devote our lives to try to stop people from stealing our innovation, our secrets, and hacking into our devices. We care about the same things, which should make this in a way an easier conversation, which I very much look forward to. Thank you.

[The prepared statement of Mr. Comey follows:]

Department of Justice

STATEMENT OF

JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"ENCRYPTION TIGHTROPE:
BALANCING AMERICANS' SECURITY AND PRIVACY"

PRESENTED

MARCH 1, 2016

James B. Comey
Director
Federal Bureau of Investigation

Before the
Committee on the Judiciary
U.S. House of Representatives

At a Hearing Entitled
"Encryption Tightrope: Balancing Americans' Security and Privacy"

Presented
March 1, 2016

Good morning, Chairman Goodlatte, Ranking Member Conyers, and members of the Committee. Thank you for the opportunity to appear before you today to discuss the challenges to public safety and national security that have eroded our 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 visibly 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 are on the frontlines of the fight against cyber crime, and we know first-hand the damage that can be caused by those who exploit vulnerable and insecure systems. We support and encourage the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data so as to promote our overall safety.

American citizens care deeply about privacy, and rightly so. Many companies have been responding to a market demand for products and services that protect the privacy and security of their customers. This has generated positive innovation that has been crucial to the digital economy. We, too, care about these important principles. Indeed, it is our obligation to uphold civil liberties, including the right to privacy.

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.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take 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. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

We must 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 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 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, and child exploitation — where critical evidence came from smart phones, computers, and online communications.

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.

We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and

also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the FBI, and the United States Government as a whole.

Of course, encryption is not the only technology terrorists and criminals use to further their ends. Terrorist groups, such as ISIL, 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 in 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 are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop — evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

We would like to emphasize that the Going Dark problem is, at base, one of technological choices and capability. 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 has provided to us to keep America safe.

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?

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 specific cases of possible national security threat. Mr. Chairman, we believe that the challenges posed by the Going Dark problem are grave, growing, and extremely complex. At the outset, it is important to emphasize that we believe that there is no one-size-fits-all strategy that will ensure progress. All involved must continue to ensure that citizens' legitimate privacy

interests can be effectively secured, including through robust technology and legal protections. 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. GOODLATTE. Thank you, Director Comey. We'll now proceed under the 5-minute rule with questions for the witness, and I'll begin by recognizing myself.

Director, there has been quite a bit of debate on the government's reliance on the All Writs Act, which most people had never heard of until the last week or so. That is being used in this case to try to compel Apple to bypass the auto erase functions on the phone. It has been characterized as an antiquated statute dating back to 1789, that was never intended to empower the courts to require a third party to develop new technology.

How do you respond to that characterization? Has the FBI relied on the Act in the past to gain access to iPhones or other similar devices, and is the Act limited to the circumstances in which Congress has already imposed a statutory duty on a third party to provide assistance?

Mr. COMEY. Thank you, Mr. Chairman. I smile a little bit when I hear that, because old doesn't mean bad, at least I hope it doesn't, because I'm rapidly approaching that point. The Constitution is as old or older than the All Writs Act, and I think that's still a pretty useful document.

It's a tool that I use. I think there's some Members of the Committee who are former Federal prosecutors. Every assistant U.S. Attorney knows it. I used it when I started as an AUSA in 1987. It is an Act that Congress passed when the Constitution was a baby, so there was a vehicle for judges to get their orders complied with. And it's been used many, many, many times, and interpreted by the courts many times, including by the Supreme Court.

The cases at hand are simply about, as I understand it, what is the reach of the All Writs Act. It's still good law, but how far does it extend, especially given how technology has changed. And I think the courts are going to sort that out. There was a decision yesterday in New York, there will be decisions in California. There will probably be lots of others, because this is a problem law enforcement is seeing all over the country.

Mr. GOODLATTE. Let me ask you about that decision in New York, because in its brief in the California case, Apple argues that a provision of CALEA, another Federal statute, actually prohibits the magistrate from ordering it to design a means to override the auto erase functions on the phone. Just yesterday, a magistrate in New York upheld that argument. Can you comment on that?

Mr. COMEY. Not in an intelligent way, because I haven't read the decision out of New York. I understand the basic contours of the argument. I don't fully get it, honestly, because CALEA is about data in motion, and this is about data at rest, but I also think this is the kind of thing judges do. They take acts of Congress and try to understand, so what does it mean, especially given changing circumstances. So I expect it'll be bumpy, there will be lots of lawyers paid for lots of hours of work, but we will get to a place where we have the courts with an understanding of its reach.

Mr. GOODLATTE. Now, if the FBI is successful in requiring Apple to unlock this phone, that won't really be a one-time request, correct?

Mr. COMEY. Well, the issue of locked phones certainly not, because it's become a——

Mr. GOODLATTE. It will set a precedent for other requests from the Federal Bureau of Investigation and any other law enforcement agency to seek the same assistance in many, many, many other cases?

Mr. COMEY. Sure, potentially, because any decision of a court about a matter is potentially useful to other courts, which is what a precedent is. I happen to think, having talked to experts, there are technical limitations to how useful this particular San Bernardino technique will be, given how the phones have changed, but sure, other courts, other prosecutors, other lawyers for companies will look to that for guidance or to try and distinguish it.

Mr. GOODLATTE. So that technology once developed, which I presume they could destroy again, but then will have to recreate hundreds of times, how confident are you—whichever procedure Apple decided to pursue, how confident are you that what you are requesting, which is the creation effectively of a key, a code, how confident are you that will remain secure and allow all the other customers of Apple, and when this is applied to other companies' technology as well, how confident are you that it will not fall into the wrong hands and make everyone's communication devices less secure, not more secure?

Mr. COMEY. First, I've got to quibble a little bit with the premise of your question. I hear people talk about keys or backdoors. I actually don't see that this way. I mean, there are issues about backdoors. This is about—there's already a door on that iPhone. Essentially we're asking Apple, take the vicious guard dog away; let us try and pick the lock. The later phones, as I understand the 6 and after, there aren't doors, so there isn't going to be, can you take the guard dog away and let us pick the lock.

But, look, I have a lot of faith, and maybe I don't know them well enough, in the company's ability to secure their information. The iCloud, for example, is not encrypted, right, but I don't lie awake at night worrying about whether they're able to protect the contents of the iCloud. They are very, very good at protecting their information and their innovation. So no thing is for certain, but I think these folks are pros.

Mr. GOODLATTE. Thank you very much. The Chair recognizes the Ranking Member, Mr. Conyers, for his questions.

Mr. CONYERS. Thank you, Chairman Goodlatte. And welcome, again, to our forum here, a very regular visitor to the Judiciary Committee.

Director Comey, it's been suggested that Apple has no interest in helping law enforcement in any criminal case and that the company cares more about marketing than about investigating a terrorist attack. In your view, are companies like Apple generally cooperative when the FBI asks for assistance accompanied by appropriate legal process? Did Apple assist with this particular investigation?

Mr. COMEY. I think, in general, all American companies, and I can't think of an exception sitting here, want to be helpful, especially when it comes to public safety, because they have families and children just as we do, so that's the attitude we're met with.

And in this particular case, as in many others, Apple was helpful to us. We had lots of good conversations about what we might be

able to do to get this device open, and we got to place where they said, for reasons that I don't question their motive, we're not willing to go further, and the government made a decision, we still have an avenue to pursue with the judge. We'll go to the judge. But I don't question their motives.

Mr. CONYERS. All right. Thank you. I sense that you're still reluctant to speak about how your success in this case might set a precedent for future actions. You indicated last week that this litigation may guide how other courts handle similar requests. Could you elaborate on that, please?

Mr. COMEY. Sure. There's no—first of all, let me say this. I've been trying to explain to people, this case in San Bernardino is about this case. And the reason I've tried to say that so much publicly is, I worry very much about the pain, frankly, to the victims in this case when they see this matter that's so important to them becoming a vehicle for a broader conversation. So I want to make sure that everybody, especially the FBI, remains grounded in the fact this is about that case. My wife has a great expression she uses to help me be a better person, which is, "It's not about you, Dear."

This case in San Bernardino is not about the FBI, it's not about Apple, it not about Congress, it's not about anything other than trying to do a competent investigation in an ongoing, active case. That said, of course, any decision by a judge in any forum is going to be potentially precedential in some other forum; not binding, but guidance, either positive or against. The government lost the case yesterday in Brooklyn. We could lose the case in San Bernardino, and it will be used as precedent against the government. That's just the way the law works, which I happen to think is a good thing.

Mr. CONYERS. Thank you. If you succeed in this case, will the FBI return to the courts in future cases to demand that Apple and other private companies assist you in unlocking secure devices?

Mr. COMEY. Potentially, yes. If the All Writs Act is available to us and the relief under the All Writs Act as explained by the courts fits the powers of the statute, of course.

Mr. CONYERS. And, finally, I think we can acknowledge, then, that this case will set some precedent, and if you succeed, you will have won the authority to access encrypted devices, at least for now. Given that you've asked us to provide you with that authority since taking your position at the Bureau, and given that Congress has explicitly denied you that authority so far, can you appreciate our frustration that this case appears to be little more than an end run around this Committee?

Mr. COMEY. I really can't, Mr. Conyers. First of all, I don't recall a time when I've asked for a particular legislative fix. In fact, the Administration's position has been they're not seeking legislation at this time. But I also—we're investigating a horrific terrorist attack at San Bernardino. There's a phone that's unlocked that belonged to one of the killers. The All Writs Act that we've used since I was a boy, we think is a reasonable argument to have the court use the All Writs Act to direct the company to open that phone. That's what this is about. If I didn't do that, I ought to be fired, honestly.

I can also understand your frustration at the broader conversation, because it goes way beyond this case. This case will be resolved by the courts. It does not solve the problem we're all here wrestling with.

Mr. CONYERS. I thank the Director, and I yield back any unused time. Thank you, Mr. Chairman.

Mr. GOODLATTE. Thank you. And the Chair recognizes the gentleman from Ohio, Mr. Chabot, for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman. I have a statement from the Application Developers Alliance here that I'd like to have included in the record.

Mr. GOODLATTE. Without objection, it will be made a part of the record.

[The information referred to follows:]

Application Developers Alliance

Government Mandates to Weaken Encryption: A Threat to Democracy, Capitalism, and Security

U.S. House of Representatives
Committee on the Judiciary
"The Encryption Tightrope: Balancing Americans' Security and Privacy"
March 1, 2016

The Application Developers Alliance (the "Alliance") welcomes and appreciates the opportunity to submit a statement for the Committee on the Judiciary's (the "Committee") hearing titled "The Encryption Tightrope: Balancing Americans' Security and Privacy." Consumers want their personal data protected, and businesses want their confidential data protected however, cyberhackers and data thieves are a constant threat to security. For several years, law enforcement and consumer protection officials have helped grow the data protection marketplace by using enforcement tools to require consumer data be protected. Responding appropriately to these marketplace and government forces, digital industry developers regularly create encryption tools to ensure that consumers' personal information and private communications remain private.

This statement serves to share with the Committee the challenges that software developers and our digital industry partners will face if we try to both protect privacy *and* provide privacy-breaching special access like backdoors, decryption, and other methods to the government. Technology experts have and will continue to address the technological impossibility of creating software vulnerabilities that only the most well-intentioned can access. This statement will address the resulting investment uncertainty, consumer mistrust, and business turbulence developers in small- and medium-sized enterprises will face if forced to comply with demands similar to the court order handed down by Judge Sheri Pym.

When this hearing concludes, the privacy vs. security debate will continue. The Alliance urges Congress to be reflective, not reactive, in its approach, carefully considering the consequences to poking holes in encryption. In today's digital marketplace, Americans near and far rely on the security of their software to make purchases, establish connections, and store sensitive data. Any hasty, short-sighted decision will destroy the Internet-driven economy as we know it.

1015 7th Street NW, Second Floor | Washington, DC | 20001
appdevelopersalliance.org

The Application Developers Alliance (the "Alliance") was founded in January 2012 to support developers as entrepreneurs, innovators, and creators. Alliance membership includes more than 150 companies and an additional 65,000 individuals.

On behalf of the app industry and our innovative, entrepreneurial members, the Committee should consider the following:

1. A government mandate, like the order handed down by Judge Pym on February 16, 2016, which would force Apple to deliberately compromise software security, runs counter to American ideals, sets a dangerous precedent for judges in other cases to point to, and is a threat to consumers' and the nation's best interests.

2. The Federal Trade Commission (FTC), State Attorneys General, the FBI, privacy advocates and consumers are correct: protecting data while using it to build exciting new products and services is unquestionably good for businesses and consumers. The entire software ecosystem is committed to both data innovation and data protection.

3. Software developers compete in a global marketplace and the products they create are used around the world. If developers are required to provide special access to the U.S. government, then many other governments will require similar access, and still other governments will cite this access as evidence of non-compliance with their national privacy laws. Instead of enjoying global digital opportunities, developers will be buffeted by conflicting laws and false choices that pose significant financial and legal risk. Developers and their customers will have to choose between compliance and market access.

4. Privacy-breaching special access makes software inherently less secure and less trustworthy. By providing access to one or more governments, the developer is creating a vulnerability that can be exploited by hackers, thieves, terrorists, and other criminals. Data protection prevents cybercrime and identity theft; encryption is the best data protection tool we have. Encryption proponents are not weighing privacy and civil liberties above

security. Instead, we recognize that enhanced security and crime prevention techniques *require* strong data protection.

Today's Privacy vs. Law Enforcement Debate is Not New: Curbing Government Overreach since the Eighteenth Century

Like many policy debates spawned by technological advances, today's encryption debate is like a new cover version of an old song. America's privacy vs. law enforcement debate began with the country's inception more than 200 years ago. Knowing that privacy is a vital piece of any well-functioning democratic society, our nation's Founding Fathers enshrined this ideal in our Constitution with the Fourth Amendment – protection from unreasonable searches and seizures.

After two centuries, some in the law enforcement community are still searching for cracks to exploit in our privacy foundation. In today's global, digital marketplace, businesses and consumers are technologically savvy and smart about data protection. Almost daily, Americans see companies of all stripes and sizes hacked by cybercriminals and experience their own identity theft horrors. In fact, identity theft has been the top consumer complaint to the FTC for fifteen consecutive years.

Moreover, revelations that some in the U.S. national security and law enforcement communities employed widespread, untargeted bulk surveillance are still fresh in the minds of consumers and businesses. Mass surveillance, and its seemingly willful disdain for proper legal process, has made citizens justifiably skeptical of law enforcement promises that unfettered access to digital networks will be utilized judiciously. In contrast, international governments require U.S. companies ensure that international consumer and business data is adequately protected, including the U.S. government. In 2016, Americans rightly demand that their data remain secure and private.

Encryption is no longer a niche market. Just 20 years ago, there were few digital products and services, and the market for encryption was small and specialized. Today, our hardware contains a slew of innovative software and other features like messaging apps, social media, cameras, video and voice recorders, not to mention telephones. Each of these innovative features may incorporate encryption to ensure that private data remains private. This privacy is also critical for business and

enterprise software to secure for example, intellectual property, financial information, and health care data.

As a result of this global focus on trust and security, many businesses are bundling encryption with products and services and are working to improve those offerings. Venture capitalists and institutional investors are betting heavily on secure trust-based business models, while computer scientists are building better systems that provide more privacy and security value – developments that businesses and consumers concerned about cyberthieves and identity theft eagerly await.

Yet, against this trend in favor of privacy and security, the FBI and other law enforcement entities are attacking and seeking vulnerabilities in encryption technologies that are protected by the Fourth Amendment. Law enforcement has an obvious and substantial interest in prosecuting crime and protecting people, but creating software vulnerabilities that will enable more identity theft and cause more consumer harm is not the right solution.

Today's Privacy vs. Law Enforcement Debate Could Have Severe and Lasting Implications for the Digital Marketplace

In light of the ubiquity of digital products and services, and the magnitude of cybercrime and identity theft, it is perplexing that the FBI and others in law enforcement are disparaging the very large, substantial, and determined encryption market that it has encouraged. Their efforts cut against prevailing wisdom and send confusing, unhelpful mixed messages to developers and the publishers and enterprises they work with.

First, government mandates to developers to build software vulnerabilities against their will and self-interest is alarming and sets a dangerous precedent. These mandates, such as the one ordered by Judge Pym, are reflexive and exhibit a misunderstanding of what is and is not in consumers' -- and the nation's -- best interest. Apple CEO Tim Cook was correct to say his company would not comply with the order to create software to deliberately undermine the security of an iPhone. The software, which does not currently exist, could be stolen or replicated by bad actors to gain access to the private and sensitive information of innocent civilians. Even more troubling is the thought

that others in the law enforcement community, say a district attorney in New York, could force a small enterprise to create similar software to gain access to a phone for a routine drug investigation. In Apple's case, the company may have the time, finances, and human capital to comply with the order should it choose to do so. A small business however, absolutely does not have the resources to comply with such mandates. Judge Pym's mandate would be nothing short of a final blow for many small enterprises.

Additionally, the government's mixed messages on the issue of encryption could paralyze developers in their business cycle. As developers, investors and customers ask which government agency is in charge and whether data protection is really a government-approved value, the marketplace can freeze up. If this uncertainty continues for too long then lawyers will have to help developers make a difficult and perhaps pyrrhic decision: which federal mandate should I follow and which one should I ignore?

Over the course of several years virtually every government law enforcement and consumer protection agency has sung from the encryption and data protection hymnal.

- The FTC advises consumers that "[e]ncryption is the key to keeping your personal information secure online," and consistently requires app developers to use "reasonable" data security practices, including encryption, to protect consumers' information from hackers and data thieves.
- California Attorney General Kamala Harris recommends that developers "transmit user data securely, using encryption" and endorses legislation "requiring encryption to protect personal information in transit."
- In Nevada, lawmakers have mandated the use of encryption to protect personal information.
- In Massachusetts, companies are strongly encouraged to encrypt and protect the data of individuals within the state. If the data is compromised, companies would be subject to significant penalties.
- In Rhode Island, breach notification laws now codify an encryption requirement. A "breach of the security system" occurs when there is "unauthorized access or acquisition of unencrypted computerized data," and an entity must use at least 128-bit encryption.

- In Washington, a safe harbor provision exists for companies that protect data with encryption. Encryption would exempt covered entities that are subject to the HIPAA/HITECH breach notification requirements or to the Interagency Guidance issued pursuant to the Gramm-Leach-Bliley Act.
- President Obama's Review Group on Intelligence and Communications Technologies recommended that the U.S. Government promote national security by "fully supporting and not undermining" encryption standards and generally available commercial encryption, and "supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage."
- And President Obama has personally called on industry to protect Americans' privacy and civil liberties, and proclaimed himself "a strong believer in strong encryption.... there's no scenario in which we don't want really strong encryption."
- Less than five years ago, the FBI recommended organizations to "encrypt data so the hacker can't read it."

Industry has already come up with the correct response. Hardware manufacturers are selling encrypted Blackphones. Companies such as Apple, Google, and Yahoo are embedding encryption into their software and operating systems. Messaging software, like Yik Yak and SpiderOak, are offering encrypted consumer solutions. And industries like banking, healthcare, transportation and manufacturing are extremely focused on secure, encrypted solutions. Cloud storage companies like SurDoc are already taking these legislative cues and industry norms to heart by encrypting data in transit and at rest. Many other companies, especially small- and medium-sized enterprises continue to wait for further guidance and clarity from lawmakers before investing significant resources in this important technology.

Third, nearly every software developer is pursuing international customers. Thus, it is important that Congress consider other countries' reactions to U.S. digital policy and how other countries' policies could create challenges to American digital services or America's global interests.

By demanding unfettered access to digital products and services, the FBI is putting American companies' international opportunities at risk. European and South American policymakers have virulently criticized U.S. Government collection of European citizens' and leaders' communications

data, and many have demanded that U.S. companies provide assurances that their products and services are not susceptible to U.S. Government hacking. Leading European policymakers have repeatedly urged more robust European consumer privacy laws, stating forthrightly that this is intended to harm U.S. digital services and advantage European services. Mandating privacy-breaching special access increases the risk that international governments will cite U.S. companies' non-compliance with privacy laws to justify banning American digital products and services from doing business in their country. Compounding this problem are governments – for example Russia, China and some in South America – that are choosing to only do business with companies based in their own country.

The Application Developers Alliance is a global organization and our European and American members are equally optimistic about our industry, consumer adoption and economic opportunity. None of our members – anywhere in the world – desire a trade war that divides the global Internet and global opportunity into smaller subsets of national markets. But if Congress requires U.S. companies to provide special access for FBI or others, it should anticipate European policymakers to respond emphatically. Mandatory privacy-breaching special access will instigate trade wars and exacerbate international business challenges.

Special access like what the FBI is seeking diminishes consumer trust and creates challenges for developers and all digital businesses. In addition to government risk, developers will face marketplace challenges if forced to provide privacy-breaching special access to law enforcement. Our customers – in the United States and abroad – expect their communications to be private and secure when purchasing or using software. Since our sector's inception, developers have prioritized the security and handling of their customers' data because they know that good data stewardship is critical to business success. Enabling governments to access data and ignoring future technological risks undermining the customer trust that developers worked hard to obtain.

Congress should also anticipate that governments worldwide will demand their own special access for their own security and law enforcement interests. This will increase further the risk that consumer and business data could be compromised. Larger companies might have the resources to build-in the required special access and might have enough consumer trust to withstand the associated scrutiny, but startups and resource-strapped small innovators will be challenged to find

resources to build multiple backdoors, and will also have greater trust problems than established competitors. Of course, all software not complying with other governments' demands could easily be locked out of those markets.

What is more, repressive regimes around the world might point to our own government's request for special access as leverage to curb privacy and free speech in their countries. Software like social media is ushering in a radical new paradigm where anyone, regardless of economic status, creed, or race can speak out and shed light on wrongdoings. It would be unjust and immoral for the U.S. Government to give any leverage to repressive governments who do not share our democratic ideals.

Fourth, from a technical standpoint, any opening in security creates a vulnerable access point for hackers, thieves, and foreign governments to exploit. While the FBI would have us believe that law enforcement alone will be privy to our sensitive data, history demonstrates that bad actors will always be ahead of the curve and find an avenue to manipulate those openings. As one well-regarded cryptographer said – "you can't build a backdoor that only the good guys can walk through."

Currently, consumers read about data breaches on an almost daily basis. Though the market is demanding tighter security measures, there are only two types of companies in the world: those that have been breached and those that do not know they have been breached. Consumers expect businesses to respond to these breaches and many have bolstered their security features, oftentimes through encryption. Requiring companies to create special access undermines consumers' and businesses' desires to secure data in storage, in transit, and across the supply chain. End-to-end encryption is the only way to secure user data from all outside forces while simultaneously giving consumers greater control of their data.

Forcing holes in software security harms startups and small innovators the most. Many – perhaps most – of the small companies that are Alliance members lack the resources to create specific access point for the right people, let alone the right people in select countries. While the U.S. government is pleading to tech companies "let us in," they simultaneously warn companies to keep hackers and other countries out. Because providing special access it technically challenging and

very expensive, it is extremely difficult for large companies, let alone startups, to meet these conflicting demands. Developers and startups already must overcome significant cost hurdles before products get to market, and any regulatory inconsistency or redundancy is one burden too many.

* * * * *

In closing, the Alliance urges Congress to remember that encryption technologies are a market response to consumer demands, business needs, and U.S. and international government recommendations to protect consumer data. When a developer builds a thriving business model around privacy, security, and consumer trust, only to be told the FBI wants your products to be secure, but not too secure, this disrupts the marketplace. It is bad for innovation, bad for business and bad for consumers. It is only good for hackers and cyberthieves who prey on private consumer data and commercially sensitive data.

Americans correctly demand that their personal data is secure. Just as importantly, businesses deserve support from lawmakers to ensure that these protection technologies grow to become the industry norm in a stable marketplace. The Alliance is happy to address any questions and looks forward to working with Congress on this very important issue.

Mr. CHABOT. Thank you, Mr. Chairman.

And, Director Comey, like yourself, I happen to be a graduate of the College of William & Mary, so I'm going to start off with a tough question. Anything nice you'd like to say about the College of William & Mary?

Mr. COMEY. I could tell there with glow coming from your seat. That's explained by your being a member of the Tribe. Best thing ever happened to me besides—I actually met my wife there. That's the best thing that ever happened to me. Second best is that I was there.

Mr. CHABOT. Excellent. Yes, it's a great place to go. There are two members currently. Ms. Titus of Nevada is also a graduate.

Now, this hearing is about electronic data security, or as you describe it——

Mr. GOODLATTE. The Chair is happy to extend additional time to the gentleman for recognizing an important Virginia educational institution.

Mr. CHABOT. I appreciate the Chairman.

And as is already indicated, this is about electronic data security or, as you described it, keeping our stuff online private. So I'd like to ask you this, and it may seem a little off topic, but I don't think it is.

A few weeks back, the FBI's general counsel, James Baker, acknowledged that the FBI is "working on matters related to former Secretary of State Hillary Clinton's use of a private email server." And then the White House press secretary, Josh Earnest, stated that "some officials over there," referring to the FBI, "had said that Hillary Clinton is not a target of this investigation, and that it's not trending in that direction." And the President then weighed in, even though he apparently had never been briefed on the matter, commenting that he didn't see any national security implications in Hillary's emails, and obviously, this is a matter of considerable import.

Is there anything that you can tell us as to when this matter might be wrapped up one way or the other?

Mr. COMEY. I can't, Congressman. As you know, we don't talk about our investigations. What I can assure you is that I am very close personally to that investigation to ensure that we have the resources we need, including people and technology, and that it's done the way the FBI tries to do all of its work: independently, competently, and promptly. That's our goal, and I'm confident it's being done that way, but I can't give you any more details beyond that.

Mr. CHABOT. I certainly understand, and I appreciate that. I thought you might say that, but you can't blame me for trying. Let me move on.

If Apple chose to comply with the government's demand, maybe it does have the technical expertise and time and finances to create such a vulnerability so we can get in and get that information. But let me ask you, what about a small business? I happen to be the Chairman of the House Small Business Committee. Wouldn't such a mandate to, say, a small company, a startup, say, with, you know, four or five, six employees, wouldn't that be a huge burden on a small business to have to comply with this sort of thing?

Mr. COMEY. I think it might be, and that's one of the factors that I understand the courts consider in passing on an All Writs Act request, the burden to the private actor, how much it would cost them, how much time and effort? And I think Apple's argument in this case is, it would take us a ton of effort, time, and money to do it, and so that's one of the reasons we shouldn't be compelled to do it. So it's a consideration built into the judicial interpretations of the Act.

Mr. CHABOT. Thank you. As the Chair of the Committee, we'd ask you certainly to consider how this could affect—you know, seven out of 10 new jobs created in the economy are small business folks; half of the people employed in this country in the private sector are small businesses, and I think we should always consider them. Let me move on to something else.

In his testimony from our December 2015 hearing about H.R. 699, the Email Privacy Act, Richard Littlehale, the Assistant Special Agent in charge of Criminal Investigation Division of the Tennessee Bureau of Investigations, voiced a frustration with the increasing technological capabilities of both criminals and noncriminals.

Rather than trying to arguably infringe on the Fourth Amendment rights of all Americans, would it be possible to better train our law enforcement officers and equip them to keep up with this changing world that we're discussing today?

Mr. COMEY. Well, there's no doubt that we have to continue to invest in training so that all of our folks are digitally literate and able to investigate in that way. The problem we face here is all of our lives are on these devices, which is why it's so important that they be private, but that also means all of criminals' and pedophiles' and terrorists' lives are on these devices, and if they can't—if they're warrant-proof, even a judge can't order access to a device, that is a big problem. I don't care how good the cop is, I don't care how good the agent is, that is a big problem. So that, we can't quite train our way around.

Mr. CHABOT. Thank you very much. I'm always almost out of time so let me concludes with, go Tribe. Thank you.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from New York, Mr. Nadler, for——

Mr. NADLER. Thank you. Since we've gone a little far afield here, let me do so again very briefly to point out that, among others, Thomas Jefferson, who, among his minor accomplishments, was the Founder of the Democratic Party, was also a graduate of William & Mary.

Mr. CHABOT. True.

Mr. NADLER. Mr. Comey, Director Comey, the attack—well, we're all certainly very condemning of the terrorist attack in San Bernardino, and we all—our hearts go out to the families and victims of that. I commend the FBI for everything you've done to investigate this matter. Now, the two terrorists are dead and another coconspirator, the neighbor, is in jail. You have used the USA Freedom Act to track their phone calls and invest—which this Committee wrote last year—to track their phone calls and investigate everyone they ever spoke to on that phone. The FBI has done a great job already. Now, let me ask a few questions.

It's my understanding that the—that we have found that the attack in San Bernardino was not, in any way, planned or coordinated by ISIS. Is that correct? It may have been inspired by, but not directed or planned by.

Mr. COMEY. Right. So far as we know, correct.

Mr. NADLER. And have you eliminated any connection between the two suspects and any overseas terrorist organization?

Mr. COMEY. Eliminated any? We have not——

Mr. NADLER. Have you seen any evidence of any, is a better way of putting it?

Mr. COMEY. We have not seen any evidence of that.

Mr. NADLER. Okay. Now, given those facts—so there's no evidence of any coordination with anybody else, that's the two homegrown, self-motivated, perhaps inspired-by-ISIS terrorists. Now, the investigators seized the iPhone in question on December 3; the FBI reached out to Apple for assistance on December 5. Apple started providing the FBI with information, with account information, I gather, the same day, but then the next day, on December 6, at the instruction of the FBI, San Bernardino County changed the password to the iCloud account associated with that device. They did so without consulting Apple, at the instruction or suggestion of the FBI. And changing that password foreclosed the possibility of an automatic backup that would allowed Apple to provide you with this information without bypassing its own security, and thus necessitating, in the first place, the application to the court that you made and that we're discussing today. In other words, if the FBI hadn't instructed San Bernardino County to change the password to the iCloud account, all of this would have been unnecessary, and you would have had that information. So my question is, why did the FBI do that?

Mr. COMEY. I have to—first of all, I want to choose my words very, very carefully. I said there is no evidence of direction from overseas terrorist organizations. This is a live investigation. I can't say much more beyond that. This investigation is not over, and I worry that embedded in your question was—and that you understood me to be saying that.

Second, I do think, as I understand it from the experts, there was a mistake made in that 24 hours after the attack where the County, at the FBI's request, took steps that made it hard—impossible later to cause the phone to back up again to the iCloud. The experts have told me I'd still be sitting here, I was going to say unfortunately, not unfortunately, fortunately, I'm glad I'm here, but we would still be in litigation, because, the experts tell me, there's no way we would have gotten everything off the phone from a backup. I have to take them at their word. But that part of your premise of your question is accurate.

Mr. NADLER. Okay. So the second part of my question is, it wasn't until almost 50 days later on January 22 when you served the warrant. Given the allegedly critical nature of this information, why did it take the FBI 50 days to go to court?

Mr. COMEY. I think there were a whole lot of conversations going on in that interim with companies, with other parts of the government, with other resources to figure out if there was a way to do it short of having to go to court.

Mr. NADLER. Okay. Thank you. Now, can you offer a specific case, because I do think we all understand that it's not just a specific case, it will have widespread implications in law, and however the courts resolve this, which is essentially a statutory interpretation case, the buck is going to stop here at some point, we're going to be asked to change the law.

So encryption software is free, open source, and widely available. If Congress were to pass a law forcing U.S. companies to provide law enforcement with access to encrypted systems, would that law stop bad actors from using their own encryption?

Mr. COMEY. It would not.

Mr. NADLER. It would not. So the bad actors would just get around it?

Mr. COMEY. Sure. Encryption's always been available to bad actors, nation states——

Mr. NADLER. So if we were to pass a law saying that Apple and whoever else had to put backdoors, or whatever you want to call them, into their systems, the bad actors that were—and with all the appropriate—with all the—not appropriate, all the concomitant surrenders of privacy, et cetera, et cetera, the bad actors could easily get around that by making their own encryption systems?

Mr. COMEY. The reason I'm hesitating is I think we're mixing together two things: data in motion and data at rest. The bad guys couldn't make their own phones, but the bad guys could always try and find a device that was strongly encrypted.

The big change here happened in the fall of 2014 when the company split from available encryption to default, and that's——

Mr. NADLER. Yeah. But couldn't——

Mr. COMEY [continuing]. That's the shadow of going dark and——

Mr. NADLER. But couldn't foreign companies and bad actors generally do that, whatever we said?

Mr. COMEY. Sure. Potentially people could say, I love this American device, but because I worry about a judge ordering access to it, I'm going to buy this phone from a Nordic country that's different in some way. That could happen. I have a hard time seeing it happen a lot, but it could happen.

Mr. NADLER. My time has expired. Thank you.

Mr. ISSA. Mr. Chairman, I'd like to ask unanimous consent some documents be placed in the record at this time. I'd like to ask unanimous consent that Patent Number 0240732, patent——

Mr. GOODLATTE. Without objection.

Mr. ISSA. Thank you. Additionally, 27353, another patent; additionally, a copy of the USA Today entitled, "Ex-NSA Chief Backs Apple On iPhone;" additionally, from Science and Technology, an article that says, "Department of Homeland Security awards $2.2 million to Malibu, California, company for mobile security research and, in other words, an encryption-proof, unbreakable phone;" additionally and lastly, the article in Politico today on the New York judge's ruling in favor of Apple.

Mr. GOODLATTE. Without objection, they will all be made a part of the record.

[The information referred to follows:]

(No Model.)

H. O. KINLOCH.

Supplementary Dash Board for Vehicles.

No. 240,732. **Patented April 26, 1881.**

Fig. 1.

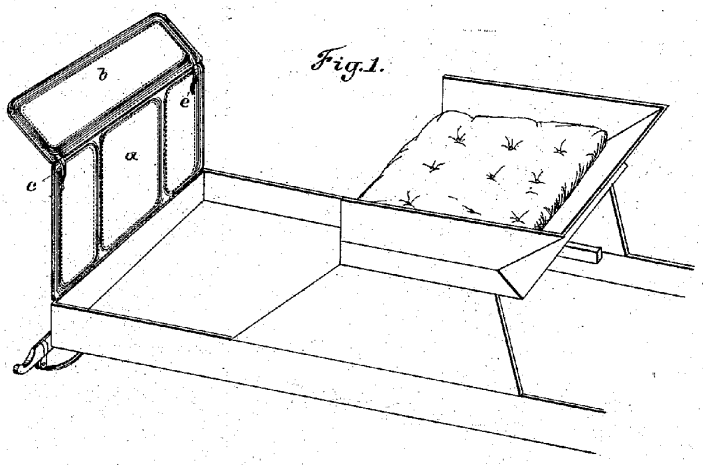
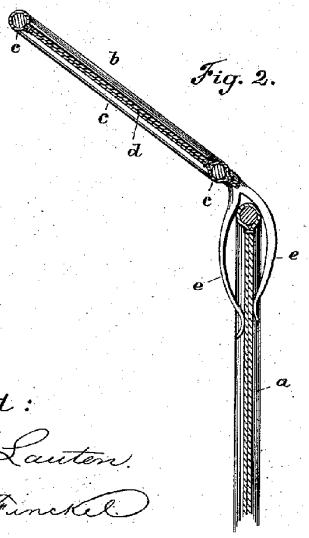


Fig. 2.



Attest:

Herm. Lauten.

Geo. M. Finckel

Inventor:

Henry O. Kinloch,

by his attorney,

Wm. H. Finckel

US 20150027353A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2015/0027353 A1**

(43) **Pub. Date: Jan. 29, 2015**

Sagebiel

(54) **ACTIVE SAFE**

(71) Applicant: **TenCate Advanced Armor USA, Inc.**, Newark, OH (US)

(72) Inventor: **Erick James Sagebiel**, Castroville, TX (US)

(21) Appl. No.: **14/444,449**

(22) Filed: **Jul. 28, 2014**

Related U.S. Application Data

(60) Provisional application No. 61/858,724, filed on Jul. 26, 2013.

Publication Classification

(51) **Int. Cl.**

E05G 1/10 (2006.01)

E05G 1/14 (2006.01)

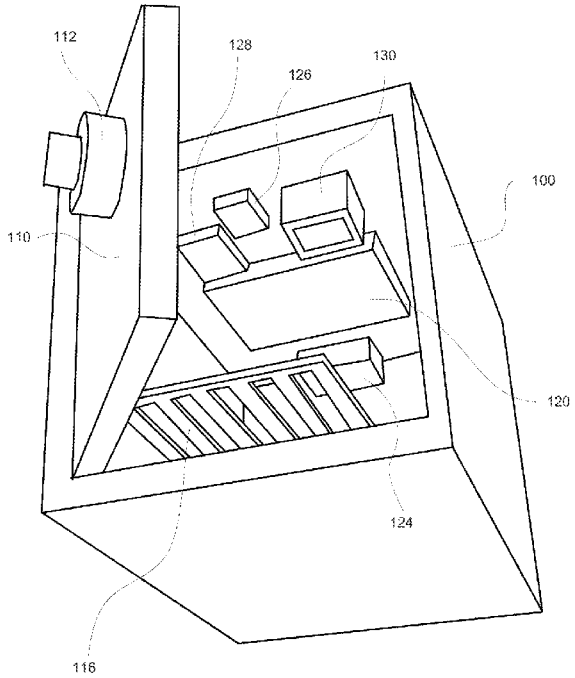
(52) **U.S. Cl.**

CPC ... ***E05G 1/10*** (2013.01); ***E05G 1/14*** (2013.01)

USPC **109/24**; 109/23; 109/36; 109/38

(57) **ABSTRACT**

Active containers and related systems configured for destroying container contents may include safes with a hardened storage space, a content destruction element configured to destroy material contained in the storage space, and an arming device. The content destruction element may include, for example, an incendiary, an explosive, a liquid, a gas, a magnet and/or an electrical source. The arming device may be configured to arm and initiate the content destruction element using various modes, which may be based on different arming criteria and firing criteria. The arming criteria and/or the firing criteria may include movement of the container, acceleration, penetration of the container, elapsed time, an arming signal, as well as an explicit firing signal. The container may include various sensors to assist in making relevant determinations, such as a positioning system, an accelerometer, a heat sensor, a pressure sensor, etc.



Ex-NSA chief backs Apple on iPhone 'back doors'

Susan Page, USA TODAY 11:29 p.m. EST February 24, 2016

(Photo: Jasper Colt, USAT)

McLEAN, VA — Retired four-star general Michael Hayden, who as director of the NSA installed and still defends the controversial surveillance program to collect telephone metadata on millions of Americans, says he opposes proposals to force Apple and other tech companies to install "back doors" in digital devices to help law enforcement.

In an emerging court battle over access to information on the iPhone owned by one of the San Bernardino attackers, Hayden says "the burden of proof is on Apple" to show that limited cooperation with investigators would open the door to broader privacy invasions. Apple is being asked not to decrypt information on the smartphone but rather to override the operating system so investigators could try an endless series of passwords to unlock it.

"In this specific case, I'm trending toward the government, but I've got to tell you in general I oppose the government's effort, personified by FBI Director Jim Comey," Hayden told Capital Download in an interview about his memoir, *Playing to the Edge: American Intelligence in the Age of Terror*. "Jim would like a back door available to American law enforcement in all devices globally. And, frankly, I think on balance that actually harms American safety and security, even though it might make Jim's job a bit easier in some specific circumstances."

In a statement released late Sunday, Comey said the San Bernardino litigation "isn't about trying to set a precedent or send any kind of message. It is about the victims and justice. Fourteen people were slaughtered and many more had their lives and bodies ruined. We owe them a thorough and professional investigation under law. That's what this is. The American people should expect nothing less from the FBI."

USA TODAY

Capital Download - Conversations with Washington's biggest newsmakers

(http://www.usatoday.com/topic/1d4316 61-9ab3-4a83-8e9c-920f3033e02a/capital-download/)

USA TODAY

Latest: U.S. vs. Apple over San Bernardino iPhone

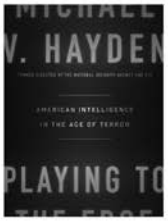
(http://www.usatoday.com/story/tech/news/2016/02/23/latest-us-vs-apple-over-san-bernardino-iphone/80786384/)

Hayden, 70, brings unparalleled credentials to the roiling debate. The retired Air Force general is the only person ever to head both the super-secret National Security Agency and the Central Intelligence Agency. In his 448-page memoir, published Tuesday by Penguin Press, he recalls being at the NSA on Sept. 11, 2001, when Al Qaeda attacked the World Trade Center and the Pentagon. He led the CIA during firestorms over its detention and interrogation of terror suspects, and while targeted killings by drones grew.

The title of the book — on the jacket, even the words bleed to the edge — refers to his conclusion that intelligence officials should play so close to the line that they get chalk dust on their cleats. "It's unapologetic," he says of his account of the decision-making behind drone attacks, the use of waterboarding and other interrogation techniques, the intelligence failures in the lead-up to the invasion of Iraq, and the culture of America's espionage agencies.

All that makes his conclusion that privacy concerns should trump security demands on this issue — putting him on the side of libertarian Sen. Rand Paul and fugitive NSA contractor Edward Snowden — especially powerful.

A federal District Court judge in California last week ordered Apple to bypass security barriers on the iPhone5c that had been used by Syed Rizwan Farook, who with his wife killed 14 people at an office holiday party in December. In a defiant public letter, Apple CEO Tim Cook announced the company wouldn't comply. Apple argues the tool inevitably would be used not just in one isolated case but repeatedly.



Gen. Michael Hayden's book, "Playing to the Edge: American Intelligence in the Age of Terror." *(Photo: Penguin Press)*

The showdown has reinvigorated proposals for Congress to pass a law that would require tech companies including Apple, Facebook and Google to provide a "back door" in digital devices so law-enforcement officials could access encrypted information during investigations. The debate has become an issue in the presidential campaign. Republican frontrunner Donald Trump has called for a boycott of Apple products unless the company cooperates with the San Bernardino investigators.

"Look, I used to run the NSA, OK?" Hayden told USA TODAY's weekly video newsmaker series. "Back doors are good. Please, please, Lord, put back doors in, because I and a whole bunch of other talented security services around the world — even though that back door was not intended for me — that back door will make it easier for me to do what I want to do, which is to penetrate. ...

"But when you step back and look at the whole question of American security and safety writ large, we are a safer, more secure nation without back doors," he says. With them, "a lot of other people would take advantage of it."

USA TODAY

Congress looks to boost email privacy; increase social media surveillance

(http://www.usatoday.com/story/news/2016/02/21/congress-looks-boost-email-privacy-increase-social-media-surveillance/80557184/)

Hayden was interviewed in the living room of his home in the northern Virginia suburbs, not far from the CIA, decorated with furniture, artwork and mementos from his foreign postings and long career: Carved chests from Korea, religious icons from Bulgaria, a small oil painting of an outdoor scene presented as a gift by the Romanian intelligence service.

A trim man with a crisp military bearing, Hayden is watching with some concern the debate over national security in the 2016 campaign. Democratic president Bill Clinton appointed him to head the NSA; Republican president George W. Bush appointed him to head the CIA. (Hayden was an adviser to and supporter of former Florida governor Jeb Bush, who suspended his candidacy Saturday.)

"It takes a complex process and tries to capture it in something about the length of a bumper sticker," he says. "Some candidates say we should use waterboarding and a lot more because they deserve it," a reference to Trump. "Well, we never used any technique against anyone because they deserved it. ... The things we did were forward-looking, to learn things to protect America.

"The same thing with regard to carpet-bombing," a tactic endorsed by Texas Sen. Ted Cruz against the self-proclaimed Islamic State. "Carpet-bombing is inherently immoral and unworthy of a nation like ourselves."

And he calls Trump's proposal to ban temporarily all Muslims from entering the United States "absolutely not helpful, incredibly harmful" in a battle against terrorism in which the biggest threat comes from self-radicalized individuals living in the United States.

"It goes to the character of us as a nation," he says. "We are a welcoming society. We assimilate immigrants far better than our European friends. And it shows up, it shows up in the fact that most of these horrific events don't happen here. They happen there. Why would you put at risk a war-winning advantage — i.e. you are a welcoming society? Why would you put that at risk by that kind of pronouncement? That actually is incredibly harmful to American safety — just saying that that would be your policy."

Hayden also is caustic when asked about potential security breaches from the decision by Democratic candidate Hillary Clinton to exclusively use of a private email server when she was secretary of State.

"Once you've set it up this way, nobody has to be stupid, lazy, unintelligent — it's gone bad," he says. "You've going to end up with information on this private server that just shouldn't be there, let alone all the questions about preserving government records." Those concerns aren't allayed even if no classified material was sent or received at her private address, he says.

"How much energy would I expend if I were still director of the National Security Agency and someone told me I could get access to the unclassified email server of [Russian Foreign Minister] Sergei Lavrov? I'd move heaven and Earth to do that. And here you've got these private, intimate conversations by a senior official of the U.S. government sitting out there in what I would call an unprotected environment."

The disclosure that Clinton had used the private server was a surprise last year to reporters and others. Does he assume that foreign intelligence agencies long had known about it and targeted it?

"I would lose all respect for a whole bunch of foreign intelligence agencies if they weren't sitting back, paging through the emails," he replied.

SNOWDEN, SPIES AND SECURITY

Hayden has had a reputation as a plain-spoken man, and he's no longer constrained by the senior offices he held in the Air Force, the NSA and the CIA. Among his comments in his interview with Capital Download:

- **On whether Americans are safer than they were on 9/11:** "That danger level has gone down steadily ... (but) here's the sad story. I think since 2012, that line has been going back up. ... It's the growth of ISIS. It's Jihad 2.0 coming at us — a very tough, violent enemy living in a safe haven the size of a good-sized American state, not in the middle of nowhere like Afghanistan, but in the middle of the Middle East."
- **On the biggest threat ahead for the United States:** "For the things that can go bump in the night tonight and really affect us, I put terrorism and cyber attack. ... Go out three, four, five years in the future, here I begin to worry about states I call ambitious, brittle and nuclear: Iran, Pakistan, North Korea, even the Russians." Ten years in the future, the challenge is China, he said. "If we don't get our relationship with the emerging People's Republic of China right, that is something that could lead to global catastrophe."
- **On the possibility of a plea bargain for fugitive NSA contractor Edward Snowden:** "I pity the American president who thinks he can be lenient on Mr. Snowden and believe that would be cost-free amongst the people on which he will continue to rely on for the safety of the nation."
- **On a lesson learned from leaks that exposed the NSA's metadata collection of Americans' phone records:** "When it comes out that way, the natural American instinct is to take that story and run to the darkest corner of the room. If we had been more open about what we had been doing, it would have counteracted that a bit. For want of a better word, it would have immunized our society against what I viewed as an overreaction to the revelation."
- **On today's challenge for intelligence agencies:** "To be good, American espionage has to be powerful and it has to be secretive inside a political culture that more and more distrusts two things: power and secrecy."
- **On balancing security and liberty:** "What we're trying to do here is what free people and this free people have done since the inception of the republic, which is to balance two things, both of which are virtues: our security and our privacy. There are no permanent answers to that. We debate them continuously based on the totality of circumstances in which we find ourselves. The point I make to our countrymen: This is not a struggle between the forces of light and the forces of darkness. This is a good people, trying to find the right balance."
- **On why the presidential campaign of Jeb Bush, whom he had endorsed, struggled:** "Because a significant portion of the American electorate in both parties are right now more interested in what I would call a primal scream. We're actually getting a very robust primal scream out of a candidate in each party right now. ... I understand the primal scream. People are frustrated. But you can't govern with a primal scream."

Read or Share this story: http://usat.ly/1TytqTj

Official website of the Department of Homeland Security

Homeland Security

Science and Technology

Our Work | Strategic Directions | Business Opportunities | S&T News | About S&T

Science and Technology > S&T Awards $2.2M to Malibu Calif Company

Share / Email

DHS S&T Awards $2.2 Million to Malibu, California Company for Mobile Security Research

Release Date: August 12, 2015

For Immediate Release
DHS Science & Technology Press Office
Contact: John Verrico, (202) 254-2385

Washington, D.C. – The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) today announced a $2.2 million cybersecurity Mobile Technology Security (MTS) research and development (R&D) award that will help secure mobile devices for the federal government. The contract award, as a result of Broad Agency Announcement HSHQDC-14-R-B0015 by the Cyber Security Division, was made to HRL Laboratories, LLC from Malibu, California to work on mobile security research in mobile device instrumentation.

"Mobile devices have become critical tools for government personnel to accomplish our mission," said DHS Under Secretary for Science and Technology Dr. Reginald Brothers. "Protecting government information and users by securing these devices is an S&T priority."

The MTS award is a part of the Mobile Device Security (MDS) R&D project which aims to accelerate the adoption of secure mobility for government and private sector organizations. The MDS project is developing R&D technologies in mobile device instrumentation, transactional security methods, mobile security management tools and mobile device layer protection.

Mobile security research in mobile device instrumentation will look at applying a breakthrough low power anomaly detection system that provides unobtrusive, and continuous, behavior-based authentication for mobile devices. HRL Laboratories' approach is based on a "brain-inspired" algorithm of learning user behaviors.. In operation, the system will provide security alerts to activate novel early warning system (EWS) algorithms. An important result of this development will be the combination of managing the power efficiency of hardware with intermittent EWS classification to remove false alarms; inferring behavioral anomalies from native mobile device sensors; and working to attain less than one false alert per week. Ultimately, this work will be implemented by HRL, and subcontractor The Boeing Company, on a Boeing Black™ smartphone.

"Given the recent cyber intrusions, it is even more important to enable secure mobile authentication for our mobile devices" said Cyber Security Division MDS Program Manager Vincent Sritapan. "With performers like HRL Labs, we can build innovative secure technologies that leverage sensors on the device, use breakthrough low power technologies, and provide new forms of mobile access control that defends against adversaries."

The successful launch of this R&D project will enable S&T to provide cutting-edge, secure technologies to the Department, government, and enterprising organizations to help create a secure and seamless mobile experience.

For more information, visit scitech.dhs.gov/cyber-research or email SandT-Cyber-Liaison@HQ.DHS.GOV.

###

Review Date: August 12, 2015

Science and Technology Issues & Programs

POLITICO

A protester holds up an iPhone that reads, "No Entry" outside of the the Apple store on 5th Avenue on Feb. 23, 2016, in New York City. | Getty

Federal judge: Apple doesn't have to unlock iPhone in N.Y. case

The ruling is likely to bolster Apple's resistance.

By **JOSH GERSTEIN** | 02/29/16 05:55 PM EST

A federal magistrate in Brooklyn, New York, has denied the government's application to force Apple to help law enforcement gain access to an iPhone belonging to a man who pled guilty in a meth conspiracy.

The ruling is likely to bolster Apple's resistance in California to a separate FBI request that the company help investigators circumvent security features on an iPhone used by one of the terrorists in the San Bernardino shootings.

In the New York case, U.S. Magistrate Judge James Orenstein rejected federal prosecutors' claim that a 1789 law authorizes the government to obtain a court order seeking to bypass a passcode-lock on an Apple phone.

"Nothing in the government's arguments suggests any principled limit on how far a court may go in requiring a person or company to violate the most deeply-rooted values to provide assistance to the government the court deems necessary," Orenstein wrote.

Apple originally cooperated with prosecutors in the Brooklyn case, but reversed course after Orenstein asked the company's lawyers to weigh in with a formal legal position.

Mr. ISSA. Thank you, Mr. Chairman. Am I recognized?

Mr. GOODLATTE. The gentleman is recognized for 5 minutes.

Mr. ISSA. Thank you, Mr. Chairman.

Justice Scalia said, it's best—said best what I'm going to quote almost 30 years ago in *Arizona v. Hicks* in which he said, "There is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of all of us."

I think that stands as a viewpoint that I have to balance when asking you questions. As I understand the case, and there's a lot of very brilliant lawyers and experienced people that know about All Writs Act, but what I understand is that you, in the case of Apple in California, are demanding, through a court order, that Apple invent something, fair to say, that they have to create something.

And if that's true, then my first question to you is the FBI is the premier law enforcement organization with laboratories that are second to none in the world. Are you testifying today that you and/or contractors that you employ could not achieve this without demanding an unwilling partner do it?

Mr. COMEY. Correct.

Mr. ISSA. And you do so because you have researched this extensively?

Mr. COMEY. Yes. We've worked very, very hard on this. We're never going to give up, but we've worked——

Mr. ISSA. Did you receive the source code from Apple? Did you demand the source code?

Mr. COMEY. Did we ask Apple for their source code? I don't—not that I'm aware of.

Mr. ISSA. Okay. So you couldn't actually hand a software person the source code and say, can you modify this to do what we want, if you didn't have the source code. So who did you go to, if you can tell us, that you consider an expert on writing source code changes that you want Apple to do for you? You want them to invent it, but who did you go to?

Mr. COMEY. I'm not sure I'm following the question.

Mr. ISSA. Well, you know, I'm going to assume that the burden of Apple is X, but before you get to the burden of Apple doing something it doesn't want to do, because it's not in its economic best interests, and they've said that they have real ethical beliefs that you're asking them to do something wrong, sort of their moral fiber, but you are asking them to do something, and there's a burden, no question at all, there's a burden, they have to invent it. And I'm asking you, have you fully viewed the burden to the government? We have—we spend $4.2 trillion every year. You have a multi-billion dollar budget. Is the burden so high on you that you could not defeat this product, either through getting the source code and changing it or some other means? Are you testifying to that?

Mr. COMEY. I see. We wouldn't be litigating if we could. We have engaged all parts of the U.S. Government to see does anybody that has a way, short of asking Apple to do it, with a 5C running IOS 9 to do this, and we do not.

Mr. ISSA. Okay. Well, let's go through the 5C running IOS 9. Does the 5C have a nonvolatile memory in which all of the encrypted data and the selection switches for the phone settings are all located in that encrypted data?

Mr. COMEY. I don't know.

Mr. ISSA. Well, it does.

Mr. COMEY. Okay.

Mr. ISSA. And take my word for it for now. So that means that you can, in fact, remove from the phone all of its memory, all of its nonvolatile memory, its disk drive, if you will, and set it over here and have a true copy of it that you could conduct infinite number of attacks on. Let's assume that you can make an infinite number of copies once you make one copy, right?

Mr. COMEY. I have no idea.

Mr. ISSA. Well, let's go through what you asked. And I'm doing this, because I came out of the security business, and this befuddles me that you haven't looked at the source code, and you don't really understand the disk drive, at least to answer my rather, you know, dumb questions, if you will.

If there's only a memory, and that memory, that nonvolatile memory sits here and there's a chip, and the chip does have an encryption code that was burned into it, and you can make 10,000 copies of this chip, this nonvolatile memory hard drive, then you can perform as many attacks as you want on it.

Now, you've asked specifically Apple to defeat the finger code so you can attack it automatically, so you don't have to punch in codes. You've asked them to eliminate the ten and destroy, but you haven't, as far as I know, asked them, okay, if we make 1,000 copies, or 2,000 copies of this, and we put it with the chip, and we run five tries, 00 through 04, and then throw that image away and put another one in and do that 2,000 times, won't we have tried, with a nonchanging chip and an encryption code that is duplicated 2,000 times, won't we have tried all 10,000 possible combinations in a matter of hours?

If you haven't asked that question, the question is, how can you come before this Committee and before a Federal judge, and demand that somebody else invent something, if you can't answer the questions that your people have tried this?

Mr. COMEY. First thing, I'm the Director of the FBI. If I could answer that question, there would be something dysfunctional in my leadership.

Mr. ISSA. No. I only asked if your people had done these things. I didn't ask you if that would work. I don't know if that work. I asked you, who did you go to, did you get the source code? Have you asked these questions, because you're expecting somebody to obey an order to do something they don't want to do, and you haven't even figured out whether you could do it yourself. You just told us, well, we can't do it, but you didn't ask for the source code, and you didn't ask the questions I asked here today, and I'm just a—I'm just a guy that——

Mr. GOODLATTE. The time of the gentleman has expired, and the Director is permitted to answer the question.

Mr. ISSA. Thank you, Mr. Chairman.

Mr. COMEY. I did not ask the questions you're asking me here today, and I'm not sure I fully even understand the questions. I have reasonable confidence, in fact, I have high confidence that all elements of the U.S. Government have focused on this problem and have had great conversations with Apple. Apple has never suggested to us that there's another way to do it other than what they've been asked to do in the All Writs Act. It could be when the Apple representative testifies, you'll ask him and we'll have some great breakthrough, but I don't think so. But I'm totally open to suggestions. Lots of people have emailed ideas. I've heard about mirroring, and maybe this is what you're talking about. We haven't figured it out, but I'm hoping my folks are watching this, and if you've said something that makes good sense to them, we'll jump on it and we'll let you know.

Mr. ISSA. Thank you.

Mr. GOODLATTE. The Chair recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman. And thank you, Director Comey, for your service to our country and your efforts to keep us safe. It is appreciated by every member of this Committee. And along with your entire agency, we do value your service and appreciate it.

I remember in law school the phrase "bad cases make bad law." I'm sure we all heard that, and I think this might be a prime example of that rule. We can't think of anything worse than what happened in San Bernardino, two terrorists murdering innocent people. It's outrageous. It sickens us, and it sickens the country. But the question really has to be, what is the rule of law here? Where are we going with this?

And as I was hearing your opening statement talking about a world where everything is private, it may be that the alternative is a world where nothing is private, because once you have holes in encryption, the rule is, it's not a question of if, but when those holes will be exploited and everything that you thought was protected will be revealed.

Now, the United States law often tends to set international norms, especially when it comes to technology policy. And, in fact, China removed provisions that required backdoors in its counterterrorism law passed in December because of the strong international norm against creating cyber weaknesses, but last night, I heard a report that the ambassadors from America, the United States, Canada, Germany, and Japan, sent a joint letter to China, because they're now thinking about putting a hole in encryption in their new policy.

Did you think about the implication for foreign policy, what China might do, when you filed the motion in San Bernardino, or was that not part of the equation?

Mr. COMEY. Yeah. I don't think—I don't remember thinking about it in the context of this particular investigation, but I think about it a whole lot broadly, which is one of the things that makes it so hard. There are undoubtedly international implications, actually, I think less to the device encryption question and more to the data in motion question, but, yeah, I have no doubt that there's international implications. I don't have good visibility into what the

Chinese require from people who sell devices in their country. I know it's an important topic.

Ms. LOFGREN. Before I forget, Mr. Chairman, I'd like to ask unanimous consent to put in the record an op-ed that was printed in The Los Angeles Times today authored by myself and my colleague, Mr. Issa, on this subject.

Mr. GOODLATTE. How could anyone object to that being a part of the record?

[The information referred to follows:]

Opinion / Op-Ed

Op-Ed Government 'backdoor' access to a single iPhone would undo years of progress in online security

People rally in front of an Apple Store in San Francisco on Feb. 23 to show their support for the company in its legal battle with the FBI. (John G. Mabanglo / EPA)

By **Zoe Lofgren and Darrell Issa**

MARCH 1, 2016, 5:00 AM

While the media has reported on nearly every minutia of the ongoing litigation between Apple and the FBI, we seem to have lost sight of the bigger picture.

This is not just about government investigators gaining access to the iPhone 5C used by Syed Rizwan Farook, one of the attackers who killed 14 people in San Bernardino late last year.

It's not just about one technology company's right to conduct business as it sees fit, or even the rights of all technology companies.

It's about Americans' broader rights to privacy.

The FBI says its wants a backdoor for just one phone, but it's clearly trying to set a precedent.

Allowing the government "backdoor" access to just this one phone would undo years of technological advances in online security.

The Department of Justice is reportedly seeking court orders to make Apple unlock and extract data from as many as 12 other phones around the country, which sources familiar with the cases say weren't even used in acts of terrorism. Manhattan Dist. Atty. Cyrus Vance Jr. says he has as many as 175 iPhones that he would "absolutely" try to force Apple to break into if the government wins its San Bernardino case. The Los Angeles Times also reports that the Los Angeles Police and Sheriff's departments alone have hundreds of phones they'd like opened too.

The FBI says its wants a backdoor for just one phone, but it's clearly trying to set a precedent. Both the FBI and the DOJ want law enforcement agents to have the legal authority and the technical capability to access any phone they suspect to contain information of value.

Moreover, although the focus for the moment is on smartphones, the government's desire for backdoor technology could easily extend to every product that connects to the Internet and every computerized system, including the systems that protect our money, cars, identities, televisions and, increasingly, the systems that run our thermostats, refrigerators and even our lightbulbs.

The proper place for this argument is not a courtroom in California, but in Congress where there can be public debate and full consideration. Indeed, the issue of mandating technological backdoors for government investigators is already a topic of vigorous discussion among the people's elected representatives in Washington. The emerging consensus is that a backdoor intended for use by law enforcement will inevitably, eventually be exploited by criminals. Creating this vulnerability would thus endanger Americans, giving not only government agents but also hackers access to our most intimate and carefully guarded personal information.

Instead of weakening privacy protections, lawmakers should support legislation — like that which passed the House with overwhelming support on three separate occasions — prohibiting government-mandated backdoors that intentionally undermine and undercut the development and deployment of strong data security technologies.

Zoe Lofgren is the senior Democrat on the House Judiciary Subcommittee on Immigration and Border Security. Darrell Issa is the Republican chairman of the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet.

Follow the Opinion section on Twitter @latimesopinion and Facebook

This article is related to: Opinion, Commentary, FBI, Zoe Lofgren, Apple iPhone, Darrell E Issa, Personal Data Collection

Ms. LOFGREN. I just note that in terms of the—you mentioned that the code at Apple, that they've done a pretty good job of protecting their code and you didn't remember anything getting out loose, but I do think, you know, if you take a look, for example, at the situation with Juniper Networks, where they had—their job is cybersecurity, really, and they felt that they had strong encryption, and yet, there was a vulnerability, and they were hacked and it put everybody's data, including the data of the U.S., I mean, of the FBI and the State Department and the Department of Justice at risk, and we still don't know what was taken by our enemies.

Did you think about the Juniper Networks issue when you filed the All Writs Act report, you know, remedy in San Bernardino?

Mr. COMEY. No. But I think about that and a lot of similar intrusions and hacks all day long, because it's the FBI's job to investigate those and stop those.

Ms. LOFGREN. I was struck by your comment that Apple hadn't been hacked, but, in fact, iCloud accounts have been hacked in the past. I think we all remember in 2014, the female celebrity accounts that were hacked from the cloud, from iCloud, and CNBC had a report that China likely attacked iCloud accounts. And then in 2015, last year, Apple had to release a patch in response to concerns that there had been brute force attacks at iCloud accounts.

So I am anticipating, we'll see, that Apple will take further steps to encrypt and protect not only its operating system that it has today, but also the protection as well as the iCloud accounts.

And I'll just close with this. I have on my iPhone all kinds of messaging apps that are fully encrypted, some better than others. Some were designed in the United States, a bunch of them were designed in other countries. And I'm not—I wouldn't do anything wrong on my iPhone, but if I were a terrorist, I could use any one of those apps and communicate securely, and there wouldn't be anything that the U.S. Government, not the FBI, not the Congress, or the President could do to prevent that from occurring. So I see this as, you know, the question of whether my security is going to be protected, but the terrorists' will continue abate.

And I thank you, Mr. Comey, for being here. I yield back, Mr. Chairman.

Mr. GOODLATTE. The Chair thanks the gentlewoman.

And the Chair recognizes the gentleman from Texas, Mr. Poe, for 5 minutes.

Mr. POE. Thank you, Director. I appreciate you being here.

Start with a little—some basics. The Fourth Amendment protects citizens from government. Citizens have rights; government has power. There is nowhere I see in the Fourth Amendment that there is an except-for-terrorists-cases exception or fear cases, that the Fourth Amendment should be waived. I signed lots of warrants in 22 years from everybody, including the FBI. Four corners of the warrant, what is to be searched, and law enforcement typically would fulfill the duty or ability in that warrant as far as they could, which is a good thing, and return the warrant.

Now we have a situation where the issue is not lawful possession. FBI is in lawful possession of the San Bernardino phone; lawful possession of the phone in New York. Do you agree with me on that?

Mr. COMEY. Yes.

Mr. POE. So we're not talking about whether the phones are in lawful possession. The issue is whether—the specific issue is whether government can force Apple, in this case, to give them the golden key to unlock the safe because they can't develop the key. I know that's kind of simplistic, but is that a fair statement or not?

Mr. COMEY. No.

Mr. POE. Not? Let me ask you this—okay, you say it is not. Apple develops the software and gives it to—and unlocks the phone, but this is not the only phone in question. Is that correct? There are other phones that FBI has in lawful possession that you can't get into.

Mr. COMEY. Sure. Law enforcement increasingly encounters phones, investigations all over the place that can't be unlocked. I would mention the Baton Rouge case too.

Mr. POE. All right. There's several. How many cases do you have in lawful possession that you want to get into the phone but you can't get into it because you don't have the software to break into it or to get into it?

Mr. COMEY. I don't know the number. A lot.

Mr. POE. A lot.

Mr. COMEY. And they are all different, which is what makes it hard to talk about any one case without being specific about what kind of phone it is.

Mr. POE. But you are in lawful possession of all these phones. This is not the issue of whether FBI lawfully possesses them. You have these phones. You can't get into them. Here is a specific phone. You want iPhone—Apple to develop software to get into this phone.

My question is, what would prevent the FBI from then taking that software and going into all those other phones you have and future phones you seize?

Mr. COMEY. I see. This seems like a small difference, but I think it's actually kind of a big difference. The ask, the direction from the judge is not to have Apple get us into the phones; it's to have Apple turn off by developing software that will tell the phone to turn off the auto erase and the delay features so that we can try and guess the password.

And so, in theory, if you had another 5C running iOS 9, which is what makes this relief possible—I mean it when I say it's obsolete, because I understand the 6s—there is no door for us to even try and pick the lock on, so it wouldn't work. But if there were phones in the same circumstances, sure, you could ask for the same relief from a court to try and make effective the search warrant.

Mr. POE. So, rather than giving you the key, it's really you want Apple to turn the security system off so they can get into the phone or you can get into the phone?

Mr. COMEY. Yeah. My homely metaphor was: take away the drooling watchdog that is going to attack us if we try and open it. Give us time to pick the lock.

Mr. POE. Or like the Viper system that Mr. Issa developed. Turn off the Viper system so you can get into the phone.

And it boils down to the fact of whether or not government has the ability to demand that occur. We have two court rulings. They

are different. I have read the opinions. They are different, a little different cases. Would you agree or not, Congress has to resolve this problem? We shouldn't leave it up to the judiciary to make this decision. Congress should resolve the problem and determine exactly what the expectation of privacy is in these particular situations of encryption or no encryption; key, no key? Do you agree or not?

Mr. COMEY. I think that the courts are competent—and this is what we've done for 230 years—to resolve the narrow question about the scope of the All Writs Act. But the broader question we're talking about here goes far beyond phones or far beyond any case. This collision between public safety and privacy, the courts cannot resolve that.

Mr. POE. And only—the Congress should then resolve, what is the expectation of privacy in this high-tech atmosphere of all this information stored in many different places on the cloud, on the phone, wherever it's stored, and—would you agree or not? I am just asking, should Congress resolve this issue of expectation of privacy of the American citizens?

Mr. COMEY. I think Congress certainly has a critical role to play. Like I said, since the founding of this country, the courts have interpreted the Fourth Amendment and the Fifth Amendment, so they are competent. That's an independent branch of government. But I think it is a huge role for Congress to play, and we're playing it today, I hope.

Mr. POE. I agree with you. I think it's Congress' responsibility to determine the expectation of privacy in this high-tech world.

And I yield back, Mr. Chairman.

Mr. GOODLATTE. The time of the gentleman has expired.

The gentleman from Tennessee is recognized for 5 minutes. There's 9 minutes and 45 seconds remaining in this vote. I will take a chance if the gentleman from Tennessee will.

Mr. COHEN. If you want to go, I will go, or I will come back.

Mr. GOODLATTE. I am trying to move it along and not keep the Director any longer than we have to, so go ahead.

Mr. COHEN. Thank you.

Director Comey, are there limitations that you could see in permitting the FBI or government in a court to look into certain records, certain type of cases, certain type of circumstances that you could foresee, or do you want it open for any case where there could be evidentiary value?

Mr. COMEY. I am not sure I am following you. I like the way we have to do our work, which is go to a judge in each specific case and show lawful authority and a factual basis for access to anybody's stuff.

Mr. COHEN. But if we decided to pass a statute and we thought it should be limited in some way, maybe to terrorism or maybe to something where it's a reasonable expectation that a person's life is in jeopardy or that you could apprehend somebody who has taken somebody's life, have you thought about any limits?

Because, you know, under what you are saying, you go to a court, I mean, you could go to a court for cases that are not capital cases, and that's—I don't think anybody here—what the public is fascinated or riveted on is the fact that what happened in San

Bernardino was so awful, and if we can find some communication or some list that was in the cloud that these people contacted, you know, Osama bin Laden's cousin and that they get—and find out that he has something to do with it, then that's important. But if you are talking about getting into somebody's information to find out who they sold, you know, 2 kilos or two bags or whatever is a whole different issue.

Where would you limit it if you were coming up with a statute that could satisfy both your interest in the most extreme, important cases and yet satisfy privacy concerns?

Mr. COMEY. Yeah, I see. I am sorry. I misunderstood the question.

I don't know and haven't thought about it well enough. And, frankly, I don't think that ought to be the FBI making that—offering those parameters to you. There is precedent for that kind of thing. We can only seek wire taps, for example, on certain enumerated offenses in the United States, so it has to be really serious stuff before a judge can even be asked to allow us to listen to someone's communications in the United States. It can't just be any offense. So there's precedent for that kind of thing, but I haven't thought about it well enough.

Mr. COHEN. Thank you. Because I am slow in getting up there to vote and the Republicans hit the—real quickly, I am going to yield back the balance of my time and start to walk fast.

Mr. GOODLATTE. The Chair thanks the gentleman.

The Committee will stand in recess. We have two votes on the floor, with 7 minutes remaining in the first vote.

Mr. Director, we appreciate your appearance. We will come back soon.

[Recess.]

Mr. GOODLATTE. The Committee will reconvene and continue with questions for Director Comey.

And the Chair recognizes the gentleman from Utah, Mr. Chaffetz, for 5 minutes.

Mr. CHAFFETZ. Thank you, Mr. Chairman.

And to the Director, thank you so much for being here.

As I have mentioned before, my grandfather was a career FBI agent, so I have great affinity for the agency and what you do and how you do it. They almost always make us proud.

But the big question for our country is, you know, how much privacy are we going to give up in the name of security? And as you said, there is no easy answer to that.

But when, historically, with all the resources and assets of the Federal Government, all the expertise, all the billions of dollars, when has it been the function of government to compel or force a private citizen or a company to act as an agent of the government to do what the government couldn't do?

Mr. COMEY. That's a legal question. In lots of different circumstances, private entities have been compelled by court order to assist, again through the All Writs Act. New York Telephone is the Supreme Court case, the seminal case on the topic.

Mr. CHAFFETZ. So let's talk for a moment about what you can see and what you can do. With all due respect to the FBI, they did—they didn't do what Apple had suggested they do in order to re-

trieve the data, correct? I mean, when they went to change the password, that kind of screwed things up. Did it not?

Mr. COMEY. Yeah, I don't know that that's accurate actually. I wasn't there. I don't have complete visibility. But I agreed with the questioner earlier: there was an issue created by the effort by the county at the FBI's request to try and reset it to get into it quickly.

Mr. CHAFFETZ. And if they didn't reset it, then they could have gone to a WiFi, local WiFi, a known WiFi access, and performed that backup so they could go to the cloud and look at that data, correct?

Mr. COMEY. Right. You could get in the cloud through that mechanism anything that was backup-able—to make up a word—to the cloud, but that does not solve your full problem. I think I would still be sitting here talking about it otherwise.

Mr. CHAFFETZ. But let's talk about what the government can see on using a phone, and it's not just an iPhone. But you can look at metadata, correct?

Mr. COMEY. Yes.

Mr. CHAFFETZ. The metadata is not encrypted, correct? If I called someone else or that phone had called other people, all of that information is available to the FBI, correct?

Mr. COMEY. In most circumstances, right. Metadata——

Mr. CHAFFETZ. In this case—let's talk about this case. You want to talk about this case. You can see the metadata, correct?

Mr. COMEY. My understanding is we can see most of the metadata.

Mr. CHAFFETZ. How would you define metadata?

Mr. COMEY. I was just going to say that. Metadata, as I understand it, is records of time of contact, numbers assigned to the particular caller or texter. It's everything except content. You can't see what somebody said, but you can see that I texted to you in theory.

My understanding is with text in particular, that's tricky. Particularly texting using iMessage, there's limitations on our ability to see the metadata around that. Again, I am not an expert, but that's my understanding.

Mr. CHAFFETZ. And do you believe that geolocation, if you are tracking somebody's actual—where they are, is that content or is that metadata?

Mr. COMEY. My understanding is it depends upon whether you are talking historical or real time when it comes to geolocation data, but it can very much implicate the warrant requirement and does in the FBI's work a lot.

Mr. CHAFFETZ. So that's what we're trying to—what's frustrating to me, being on Judiciary, being the Chairman of the Oversight Committee, there is nobody on the this panel as in a republic and representative of the people that have been able to see what the guidance is post-Jones in understanding how you interpret and what you are actually doing or not doing with somebody's geolocation.

Mr. COMEY. You have asked that of the FBI and not been able to get it?

Mr. CHAFFETZ. Department of Justice, they have been asking for this for years. What's frustrating is the Department of Justice is asking for more tools, more compulsion, and we can't even see what

you are already doing. We can't even see to the degree you are using stingrays and how they work. I mean, I think I understand how they work, but what sort of requirements are there? Is it articulable suspicion? Is there a probable cause warrant that's being used or needed?

And it's not just the FBI. I mean, you have got the IRS and Social Security and others using stingrays, again, other tools that I would argue are actually content into somebody's life and not just the metadata that you are able to see.

So how do we get exposure? How do we help you if we can't—if you routinely refuse—and I say "you," meaning the Department of Justice—access in explaining to us what tools you already do have and what you can access? How do we solve that?

Mr. COMEY. Yeah, I don't have a great answer sitting here. I will find out what's been asked for and what's been given. I like the idea of giving as much transparency as possible. I think people find it reassuring, at least with respect to the FBI. To take cell phone tower simulators, we always use search warrants. And so that shouldn't be that hard to get you that information.

Mr. CHAFFETZ. What I worry about, you may be responsible, but I don't know what the IRS is doing with them, and I have a hard time figuring out when that is responsible.

Last comment, Mr. Chairman. To what degree are you able to access and get into, either in this case or broadly, are you able to search social media in general, and are you using that as an effective tool to investigate and combat what you need to do?

Mr. GOODLATTE. The time of the gentleman has expired. The witness can answer the question.

Mr. COMEY. Social media is a feature of all of our lives, and so it's a feature of a lot of our investigations. Sometimes it gives us useful information; sometimes not. It's hard to answer in the abstract, but it's a big part of our work.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Georgia, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, Director Comey.

The Framers of our Constitution recognized a right to privacy that Americans would enjoy. The Fourth Amendment pretty much implies that right to privacy. Does it not?

Mr. COMEY. I am not a constitutional scholar. I think a scholar, if he were sitting here, might say it's not the Fourth Amendment that's the source of the right to privacy; it's other amendments of the Constitution. But that's a technical answer. The Fourth Amendment is critically important because it's a restriction on government power. You may not look at the people's stuff, their houses, their effects without a warrant and without an independent judiciary.

Mr. JOHNSON. But it also grants impliedly to the government, the Fourth Amendment, the authority to search and seize when the search or seizure is reasonable. Is that correct?

Mr. COMEY. Again, to be technical, I think the answer is Congress has given the government that authority through statute. The Fourth Amendment is a restriction on that authority.

Mr. JOHNSON. The Fourth Amendment says that the right of the people to be secure in their place, in their persons, housings, pa-

pers, and effects against unreasonable searches and seizures shall not be violated and no warrant shall issue but upon probable cause, supported by oath or affirmation.

And what I am reading into the Fourth Amendment is that the people do have a right to privacy, have a right to be secure in their persons, housings, papers, and effects, but I am also reading into it an implied responsibility of the government to, on occasion, search and seize. Would that be your reading of it also?

Mr. COMEY. Yes.

Mr. JOHNSON. And, of course, upon probable cause. But there are some circumstances where, in a hot pursuit or at the time of an arrest, there's some exceptions that have been carved out to where a warrant is not always required to search and seize. Is that correct?

Mr. COMEY. Yes. You mentioned one, the so-called exigent circumstances doctrine, where if you are in the middle of an emergency and you are looking for a gun that a bad guy might have hid, you know, in a car or something, you don't necessarily have to go get the warrant. If you have the factual basis, you can do the search and then have the judge look at it and validate it.

Mr. JOHNSON. Now, even in a situation where exigent circumstances exist, technology has now brought us to the point where law enforcement or the government is preempted from being able to search and seize. Is that correct? Technology has produced this result.

Mr. COMEY. Yeah, I think technology has allowed us to create zones of complete privacy, which sounds like an awesome thing until you really think about it. But those zones prohibit any government action under the Fourth Amendment or under our search authority.

Mr. JOHNSON. Well, it's actually a zone of impunity, would it not be, a zone where bad things can happen and the security of Americans can be placed at risk?

Mr. COMEY. Potentially, yes, sir.

Mr. JOHNSON. And that is the situation that we have with end-to-end encryption. Is that not correct?

Mr. COMEY. I think that's a fair description, where we have communications where, even with the judge's order, can't be intercepted.

Mr. JOHNSON. Now, you said that you were not a constitutional scholar, and neither am I, but does it seem reasonable that the Framers of the Constitution meant to exempt any domain from its authority to be able to search and seize if it's based on probable cause or some exigent circumstance allows for a search and seizure with less than a warrant and a showing of probable cause?

Mr. COMEY. Yeah, I doubt that they—obviously, I doubt that they imagined the devices we have today and the ways of communicating. But I also doubt that they imagined there would be any place in American life where law enforcement with lawful authority could not go. And the reason I say that is, the First Amendment talks about the people's homes. Is there a more important place to any of us than our homes?

So from the founding of this country, it was contemplated that law enforcement could go into your house with appropriate predi-

cation and oversight. So, to me, the logic of that tells me they wouldn't have imagined any box or storage area or device that could never be entered.

Mr. JOHNSON. So, from that standpoint, to be a strict constructionist about the Constitution and the Fourth Amendment, it's ridiculous that anyone would think that we would not be able to take our present circumstances and shape current law to appreciate the niceties of today's practical realities. I know I am rambling a little bit. But did you understand what I just said?

Mr. COMEY. I understand what you said, sir.

Mr. JOHNSON. Would you agree or disagree with me?

Mr. GOODLATTE. The time of the gentleman has expired. The Director may answer the question.

Mr. COMEY. I think it's the kind of question that democracies were built to wrestle with and that the Congress of the United States is fully capable of wrestling with in a good way.

Mr. JOHNSON. Well, in prior times, we have been.

Mr. GOODLATTE. The time of the gentleman has expired.

Mr. JOHNSON. Thank you.

Mr. GOODLATTE. The Chair recognizes the gentleman from Pennsylvania, Mr. Marino, for 5 minutes.

Mr. MARINO. Thank you, Mr. Chairman.

Mr. Director, it's always a pleasure.

Mr. COMEY. Same, sir.

Mr. MARINO. I am going to expand a little bit on one of Judge Poe's questions. Is the Bureau asking Apple to simply turn over the penetration code for the Bureau to get into or that you want the penetration code at your disposal? Do you understand what I am saying?

Mr. COMEY. As I understand the judge's order, the way it could work out here is that the maker of the phone would write the code, keep the phone and the code entirely in their office space, and the FBI would send the guesses electronically. So we wouldn't have the phone. We wouldn't have the code. That's my understanding of it.

Mr. MARINO. That's good point to clarify, because there's some—there's a lot of rumors out there.

I am going to switch to the courts a little bit here. Do you see the Federal court resolving the warrant issue that the Bureau is presently faced with, whatever way that decision eventually comes down, or should Congress legislate the issue now, if at all?

Mr. COMEY. I don't—I appreciate the question. I don't think that's for me to say. I do think the courts—because some people have said so in the middle of this terrorism investigation, why didn't you come to Congress? Well, because we're in the middle of a terrorism investigation. And so I think the courts will sort that out faster than any legislative body could, but only that particular case.

The broader question, as I said earlier, I don't see how the courts can resolve this tension between privacy and public safety that we're all feeling.

Mr. MARINO. Another good point.

Given that most of our social, professional, and very personal information is on our desktop computers, on our laptops, on our pads, and now more than ever on these things, what is your position on

notching up the level at which members of the Federal judiciary can approve a warrant to access critically valuable evidence to solve a horrific felony, particularly when fighting terrorism?

Mr. COMEY. Do you mean making the threshold something above probable cause?

Mr. MARINO. No, no, not the threshold, the Federal judicial individuals making this decision. Right now, I understand it's a magistrate. When I was at the State level, we could do some things at sort of the magistrate level or the district court, but then we had to go to the superior court, and working in the Federal system with you, we had to go to one or two different levels. What's your position on that?

Mr. COMEY. I see what you are saying. So, instead of having magistrate judges decide these questions, the district court might?

Mr. MARINO. Yeah. And no disrespect to magistrate courts. I am very good friends with a lot of those brilliant people who will eventually, I know, go to the bench. But from a perspective of the public that a more narrowly defined, limited number of people making that decision concerning the electronics that we have.

Mr. COMEY. Honestly, Congressman, I haven't thought about that. I agree with you. I have a number of friends who are magistrate judges, and they are awesome. And they think well, and they rule well. I think they are fully capable of handling these issues, but I haven't thought about it well enough to react, other than that.

Mr. MARINO. Okay. And just for the record, I have managed a couple of prosecution offices, and I have never gone to the experts, whether it's in DNA or whether it's in these electronics, and ask them, did you complete everything that you should have completed?

Mr. COMEY. Thank you, Mr. Marino.

Mr. GOODLATTE. The Chair recognizes the gentlewoman from California, Ms. Chu, for 5 minutes.

Ms. CHU. Director Comey, my district is next to San Bernardino. After the terror attack, we mourned the loss of 14 lives and empathized with the 22 wounded, and there is indeed fear and anxiety amongst my constituents. So our discussion here today is particularly important to the people back home. There are many in our area that want answers, but there are also many that feel conflicted about putting their own privacy at risk.

So my first question to you is: Under Federal law, we do not require technology companies to maintain a key to unlock encrypted information in the devices they sell to customers. Some of the witnesses we will hear from today argue that if such a key or software was developed to help the FBI access the device used by Syed Farook, it would make the millions of other devices in use today vulnerable. How can we ensure that we're not creating legal or technical backdoors to U.S. technology that will empower other foreign governments in taking advantage of this loophole?

Mr. COMEY. It's a great question. I think what you have to do is just talk to people on all sides of it who are true experts, which I am not, but I have also talked to a lot of experts. And I am an optimist. I actually don't think we've given this the shot that it de-

serves. I don't think the most creative and innovative people in our country have had an incentive to try and solve this problem.

But when I look at particular phones, in the fall of 2014, the makers of these phones could open them. And I don't remember people saying the world was ending at that point and that we're all exposed. And so I do think judgments have been made that are not irreversible. But I think the best way to get at it is talk to people about, so why do you make the phone this way, and what is the possibility?

The world I imagine is a world where people comply with warrants. How they do it is entirely up to them. Lots of phone makers and providers of email and text today provide secure services to their customers, and they comply with warrants. That's just the way they have structured their business. And so it gives me a sense of optimism that this is not an impossible problem to solve. Really, really hard, and it will involve you all talking to the people who really know this work.

Ms. CHU. Well, I would like to ask about law enforcement finding technical solutions. I understand that there may be other methods or solutions for law enforcement when it comes to recovering data on a smartphone. Professor Landau argues in her testimony later today that solutions to accessing the data already exist within the forensic analysis community, solutions which may include jail breaking the phone, amongst others. Or she says other entities within the Federal Government may have the expertise to crack the code.

Has the FBI pursued those other methods or tried to get help from within the Federal Government, such as from agencies like the NSA?

Mr. COMEY. Yes is the answer. We've talked to anybody who will talk with us about it, and I welcome additional suggestions. Again, you have to be very specific: 5C running iOS 9, what are the capabilities against that phone. There are versions of different phone manufacturers and combinations of model and operating system that it is possible to break a phone without having to ask the manufacturer to do it. We have not found a way to break the 5C running iOS 9.

And, as I said, in a way, this is kind of yesterday's problem because the 5C, although I am sure it's a great phone, has been overtaken by the 6 and will be overtaken by others that are different in ways that make this relief yesterday.

Ms. CHU. So let me ask you this: Like smart phones, safes can be another form of storage of personal information. Similarly to how technology companies are not required to maintain a key to unlock encryption, safe manufacturers are not required to maintain keys or combinations to locks.

Given this, law enforcement has been able to find a way to get into safes under certain circumstances or obtain critical information through other avenues. So how does this differ from unlocking a smartphone? It's clear that technology is outpacing law enforcement's ability to get information from devices like the iPhone, even with a proper warrant, but isn't it the FBI or the law enforcement agency who bears the responsibility to figure out the solution to unlock the code?

Mr. COMEY. I will take the last part first. Sure, if we can figure it out. The problem with the safe comparison is there's no safe in the world that can't be opened. And if our experts can't crack it, we will blow it up. We will blow the door off. And so this is different. The awesome, wonderful power of encryption changes that and makes that comparison, frankly, inept.

And so, sure, where law enforcement can appropriately lawfully figure out how to do it, we will and should. But there will be occasions, and it's going to sweep across—again with the updating of phones and the changing of apps where we communicate end-to-end encrypted—it's going to sweep across all of our work and outstrip our ability to do it on our own.

Ms. CHU. Thank you. I yield back.

Mr. GOODLATTE. The Chair thanks the gentlewoman.

The gentleman from South Carolina, Mr. Gowdy, is recognized for 5 minutes.

Mr. GOWDY. Thank you, Mr. Chairman.

Director, thank you for your service to the country.

And I do appreciate your acknowledgment and that of my colleagues of the difficulty in reconciling competing binary constitutional principles like public safety, national security, and privacy. And I confess upfront: my bias is toward public safety.

Because of this loosely held conviction I have that the right to counsel, the right to free speech, the right to a jury trial just isn't of much use if you are dead, so I reconcile those competing principles in favor of public safety.

And my concern as I hear you testify is that I have colleagues and others who are advocating for these evidence-free zones. They are just going to be compartments of life where you are precluded from going to find evidence of anything.

And I am trying to determine whether or not we as a society are going to accept that, that there are certain—no matter how compelling the government's interest is in accessing that evidence, we are declaring right now this is an evidence-free zone; you can't go here no matter whether it's a terrorist plot—and I am not talking about the Feng case. That's a drug case. The case the magistrate decided yesterday in New York is a drug case. Those are a dime a dozen.

National security, there's nothing that the government has a more compelling interest in than that, and we're going to create evidence-free zones? Am I missing something? Is that how you see it? You just can't go in these categories unless somebody consents?

Mr. COMEY. That's my worry, and why I think it's so important we have this conversation. Because even I on the surface think it sounds great when people say: Hey, you buy this device; no one will ever be able to look at your stuff. But there are times when law enforcement saves our lives, rescues our children, and rescues our neighborhoods by going to a judge and getting permission by looking at our stuff.

And so, again, I come to the case of a Baton Rouge 8-month pregnant woman, shot when she opens her door. Her mom says she keeps a diary on her phone. We can't look at the diary to figure out what might have been going on in her life. Who was she texting with? That's a problem. I love privacy. But all of us also love public safety, and it's so easy to talk about. Buy this amazing

device; you will be private. But you have to take the time to think: Okay. There's that, and what are the costs of that? And that's where this collision is coming in.

Mr. GOWDY. Well, I love privacy too, but I want my fellow citizens to understand that most of us also, in varying degrees, also love our bodies and the physical integrity of our body. But since Schmerber, the government has been able to access orders for either blood against the will of the defendant or, in some instances, surgical procedures against the will of the defendant.

So when I hear my colleagues say, have you ever asked a non-government actor to participate in the securing of evidence, absolutely. That's what the surgeon does. If you have a bullet from an officer who was shot in a defendant, you can go to a judge and ask the judge to force a nurse or surgeon to anesthetize and remove that bullet. So if you can penetrate the integrity of the human body in certain categories of cases, how in the hell you can't access a phone, I just find baffling.

But let me ask you this: If Apple were here—and they are going to be here—how would they tell you to do it? If there were a plot on an iPhone to commit an act of violence against, say, hypothetically, an Apple facility, and they expected you to prevent it, how would they tell you to access the material on this phone?

Mr. COMEY. I think they would say what they have said, which I believe is in good faith, that we have designed this in response to what we believe to be the demands of our customers to be immune to any government warrant or our, the manufacturer's, efforts to get into that phone. We think that's what people want.

And that may be so, except I would hope folks will look at this conversation and say, "Really, do I want that?" and take a step back and understand that this entire country of ours is based on a balance. It's a hard one to strike, but it's so seductive to talk about privacy as the ultimate value. In a society where we aspire to be safe and have our families safe and our children safe, that can't be true. We have to find a way to accommodate both.

Mr. GOWDY. So Apple, on the one hand, wants us to kind of weigh and balance privacy, except they have done it for us. They have said at least as it relates to this phone, we've already done that weighing and balancing, and there is no governmental interest compelling enough for us to allow you to try to guess the password of a dead person's phone that is owned by a city government. There's no balancing to be done. They have already done it for us.

I would just—I will just tell you, Director, in conclusion: We ask the Bureau and others to do a lot of things, investigate crime after it's taken place, anticipate crime, stop it before it happens. And all you are asking is to be able to guess the password and not have the phone self-destruct. And you can go into people's bodies and remove bullets, but you can't go into a dead person's iPhone and remove data. I just find it baffling.

But I am out of time.

Mr. GOODLATTE. The gentleman's time has expired.

The Chair recognizes the gentleman from Florida, Mr. Deutch, for 5 minutes.

Mr. DEUTCH. Thank you, Mr. Chairman.

Director Comey, thank you for being here. Thank you for your service and that of the men and women who work for you. We're all grateful for what they do.

And I just wanted to take a moment before I ask you a couple questions here to let you know that Bob Levinson, who was an agent for over 20 years, 28 years, at the Justice Department, continues to be missing. I want to thank you for what you have done. I want to thank you for the Facebook page in Farsi that you have put up. I would love a report on the effectiveness and what you have heard from that.

And I want to, more than anything else, on behalf of Bob's family, I want to thank you for never forgetting this former agent, and I am grateful for that.

Mr. COMEY. Thank you, sir. He'll never be forgotten.

Mr. DEUTCH. Now, I want to agree with Mr. Gowdy that if this were as easy as public safety or privacy, I think most of us, probably all of us, if we had to make the choice, we're going to opt for public safety for the very reason that Mr. Gowdy spoke of.

I have some questions. What I am confused about is this: The tool that you would need to take away the dogs, take away the vicious guard dogs, it's a tool that would disable the auto-erase. There's some confusion as to whether there's an additional tool that you are seeking that would allow you to rapidly test possible passcodes. Is there a second tool as well?

Mr. COMEY. Yeah. I think there's actually three elements to it. And I have spoken to experts. I hope I get this right. The first is what you said, which is to disable the self-destruct, auto-erase type feature. The second is to disable the feature that, between successive guesses—as I understand iOS 9, it spreads out the time, so even if we got the ability to guess, it would take years and years to guess. So do away with that function. And the third thing, which is smaller, is set it up so that we can send you electronic guesses so we don't have to have an FBI agent sit there and punch in 1-2-3-4, like that.

Mr. DEUTCH. And once they created that, would you expect them, after this case, would you expect them to preserve that or destroy it?

Mr. COMEY. I don't know. It would depend on what the judge's order said. I think that's for the judge to sort out. That's my recollection.

Mr. DEUTCH. So here is the issue: I think that vicious guard dog that you want to take away so you can pick the lock is one thing. But in a world where we do—I mean, it's true: there are awful people, terrorists, child predators, molesters who do everything on here. But so do so many of the rest of us, and we would like a pack of vicious guard dogs to protect our information to keep us safe, because there's a public safety part of that equation as well.

And the example of surgical procedures, the reason that that I don't think applies here is because, in that case, we know the only one doing the surgical procedure is the doctor operating on behalf of law enforcement. But when this tool is created, the fear, obviously, is that it might be used by others, that there are many who will try to get their hands on it and will then put at risk our information on our devices.

And how do you balance it? This is a really hard one for me. This isn't an either/or. I don't see it as a binary option. So how do you do that?

Mr. COMEY. I think it's a reasonable question. I also think it's something the judge will sort out. Apple's contention, which, again, I believe is made in good faith, is that there would be substantial risk around creating this software. On the government side, count us skeptical, although we could be wrong, because I think the government's argument is that's your business to protect your software, your innovation. This would be usable in one phone. But, again, that's something the judge is going to have to sort out. It's not an easy question.

Mr. DEUTCH. If it's the case, though, that it's usable in more than one phone and that it applies beyond there, then the public safety concerns that we may have, that a lot of us have about what would happen if the bad guys got access to our phones and our children's phones, in that case, those are really valid. Aren't they?

Mr. COMEY. Sure. The question that I think we're going to have litigation about is how reasonable is that concern. And, you know, slippery-slope arguments are always attractive, but I mean, I suppose you could say, well, Apple's engineers have this in their head. What if they are kidnapped and forced to write software? That's why the judge has to sort this out between good lawyers on both sides making all reasonable arguments.

Mr. DEUTCH. And, finally, Mr. Chairman, I just worry, when we talk about the precedential value, the discussion is taking place wholly within a domestic context. There are countries around the world where we know very well that the governments do their best to monitor what happens in their country and, through people's cell phones, are able to squash dissent, are able to take action to throw people in jail and to torture people.

And I think that precedential value is something else that we have to bear in mind as we engage in this really important and really difficult debate.

And I yield back, Mr. Chairman.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Florida, Mr. DeSantis for 5 minutes.

Mr. DESANTIS. Good afternoon, Director Comey. When you are looking at a case like the Apple case, and you want to be able to, as you said, remove the guard dogs and the FBI go in, are you concerned about preserving the evidentiary value that can then be used, or are you more interested in just getting the information for intel purposes so that you can use that for counterterrorism?

Mr. COMEY. Our hope is to do both, but if we have to choose, we want the information first, and then we would like it, obviously, to be in a form that could be used if there was a court proceeding against somebody someday.

Mr. DESANTIS. I guess, are there instances in which maybe a company would provide the data but would provide it to you in a way that you would not necessarily be able to authenticate that in court?

Mr. COMEY. Sure. That happens all the time.

Mr. DESANTIS. And that's something that the FBI, if that's what you get, then you are fine with that?

Mr. COMEY. Depends upon the case, but in general, that's a tool that we use, private cooperation where we may not be able to use the information in court.

Mr. DESANTIS. And in terms of the guy in San Bernardino, it wasn't even his phone, and then the owner of the phone has consented for the FBI to have the information. Is that correct?

Mr. COMEY. Right. We have a search warrant for the phone. The guy who was possessing it is obviously dead. And the owner of the phone has consented.

Mr. DESANTIS. What's the best analogous case to what you are trying to do here? Because people will look at it and say: Well, you are basically commandeering a company to have to do these things. That's typically not the way it works. So what would you say is—outside of the technology context, what would be an analogous case?

Mr. COMEY. Well, everyone in the United States, to some degree, has an obligation to cooperate with appropriate authority. The question that the court has to resolve under the All Writs Act is, what are the limits of that? Apple's argument is that might be okay if it requires us to hand you something we've already made to open a phone, but if we're going to make something new, that's beyond the scope of the law.

As you know, that's something the courts do every day in the United States, trying to understand the law and interpret its scope based on a particular set of facts. So that's what will be done in San Bernardino in a different context. It's being done in Brooklyn, in the drug case in Brooklyn. I think it's being done in different stages all over the country, because in investigation after investigation, law enforcement is encountering these kinds of devices.

Mr. DESANTIS. In your cases, have you gotten an order under the All Writs Act to just have a defendant, if you have a search warrant, produce the code?

Mr. COMEY. I don't know of a—I don't know of a similar case.

Mr. DESANTIS. In terms of, I know some of the technology companies are concerned about if they are creating ways to, I guess, penetrate their systems, that's creating like a back door. And I guess my concern is terrorists, obviously, when operating in a variety of spheres, one of the ways that they get a lot of bang for their buck is cyber attacks.

And so if companies were creating more access for law enforcement in some of these situations, would that create more vulnerability for people and be more likely that they were subjected to a potential cyber attack?

Mr. COMEY. Potentially, sure. If there were access tools that got loose in the wild or that could be easily stolen or available to bad people, it's a concern. As I said, a huge part of the Bureau's work is protecting privacy by fighting against those cybercriminals. So it's something we worry about every day.

Mr. DESANTIS. Well, how would you then provide a assurances, if you are requesting a company to work with you, that this doesn't get out into the wild, so to speak?

Mr. COMEY. I think in the particular case, we have confidence—and I think it is justified—that Apple is highly professional at protecting its own innovation, its own information. So the idea here

is: You keep it. You figure out how to store it. You figure—you even take the phone and protect it. I think that's something they do pretty well, but, again, that is something the judge will sort out.

Apple's argument, I think, will be that's not reasonable because there are risks around that. Even though we're good at this, it could still get away from us. And the judge will have to figure that out, what's reasonable in that circumstance.

Mr. DESANTIS. Thank you.

I yield back the balance of my time.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Illinois, Mr. Gutierrez.

Mr. GUTIERREZ. Thank you, Mr. Chairman.

And thank you, Director Comey, for coming and being with us here this afternoon. I won't take my 5 minutes, so I will make a couple of comments and beginning by saying that I hope that all of the Members of the Committee would take note that the Director is actually answering our questions, and that is obviously very refreshing in that we get a lot of witnesses here. And if they bring them, we might not like them; if we bring them, they don't seem to like them. And it's good to get information without passing judgment.

And I think that's what you have done very well here today. You are not passing judgment on Apple and their motivation. And I think in not questioning people's motivation, it's easier to get a solution, because once you do that, everybody kind of says: "Okay, let's get all our defenses up." And, really, what we need to be doing is defending the American people, not Apple or any company or the FBI for that matter, but defending the American people. So I want to thank you for that.

And I just want to suggest that we continue these conversations. I buy a house. I have no reasonable expectation that if you get a warrant, you are going to go into my—any drawer in my bedroom. When I buy the house, I don't have any expectation of privacy once you get a warrant to come. I do expect you to get one.

I come from a time when I wasn't quite sure the Chicago Police and law enforcement was actually getting warrants in the city of Chicago in the 1960's to get that, so we want to be a little careful and make sure. I am trusting of you. If you were the FBI agent, I would say, no problem, Director Comey, come on in.

But, unfortunately, there are human beings at all the different levels of government, and I just want to say that I am happy you came because I don't have that expectation in my car. I don't have that expectation—I don't use the computer a lot to—I still write. I don't have any expectation.

But the difference is—and I think you have made and I think this Committee should take it into consideration—we do put a lot of information in these contraptions, and the reason we put them there is because we don't want to put them on a notebook; we want to keep them private. But I really don't have any expectation that once I put this, if you have a lawful warrant, that you should be able to get it, even from my computer. I think that's where you are going.

Could you—is that where you think—have I heard you right?

Mr. COMEY. I do. I agree with you, except I think the case for privacy is even stronger than you said. You do have a reasonable expectation to privacy in your home, in your car, and in your devices. The government, under our Constitution, is required to overcome that by going to an independent judge, making a showing of probable cause, and getting a warrant.

What we need to talk about as a country is we're moving to a place where there are warrant-proof places in our life, and yes, these devices are spectacular, because they do hold our whole lives. They are different than a briefcase. They are different than a drawer. So it is a source with—a place with a tremendous reasonable expectation of privacy.

But if we're going to move to a place where that is not possible to overcome that, that's a world we've never lived in before in the United States. That has profound consequences for public safety. And all I am saying is we shouldn't drift there, right? Companies that sell stuff shouldn't tell us how to be. The FBI shouldn't tell us how to be. The American people should say: "The world is different. How do we want to be?" And figure that out.

Mr. GUTIERREZ. Yeah, I think we're in the same place then, because I do have a reasonable expectation of privacy in my home. But if you go to court, you convince the judge, and you overcome it, I have never had any expectation that a court order, because I bought something, I am going to be able to overcome a court order. So I think we're in the same place.

So thank you so much, Director, for coming and sharing time. I hope to share more time with you so we can talk some more. Thank you.

Mr. GOODLATTE. The Chair recognizes the gentleman from Iowa, Mr. King, for 5 minutes.

Mr. KING. Thank you, Mr. Chairman.

Director, thanks for your testimony here and your leadership with the FBI.

I am curious about this from a perspective that has to do with our global war against radical Islamic terrorists. And I have laid out a strategy to defeat that ideology. I would take it back to our ability some years past to be able to identify their cell phones and get into their cell phones in such a way that we also got into their heads, which drove them into the caves and really diminished a lot of their otherwise robust activity that Al Qaeda might have carried out against us. I think that was a successful effort.

Now we have global cyber operations going on with, I think by your numbers from a previous report I read, well over 100,000 ISIS activities on Twitter and other cyber activity in a single day. And so I am interested in how the parameters that have been examined thoroughly by a lot of the lawyers on this panel might apply to an all-out cyber warfare against ISIS and any of their affiliates or subordinates that I think is necessary if we're going to defeat that ideology.

And so I am thinking in terms of if this Congress might diminish, slow down, or shut down access to this phone, that also means access to any other phone that they might be using; they would have a high degree of confidence that they could operate with a level of impunity in the cyber world out there.

Do you have any comments you would like to make on the implications that being locked out of an opportunity to unlock this phone might mean to the global war on terror that could be prosecuted in the next Administration aggressively across the fields of cyber warfare? And I would just add to that for the sake of enumerating them: financial warfare, educational warfare, and human intelligence, and the network that would be necessary, not just the kinetic activity, to defeat radical Islamic terrorism.

Mr. COMEY. Thank you, Mr. King.

This conversation we're having today and that I hope will continue is really important for domestic law enforcement, but it has profound implications for, among other things, our counterterrorism work. Because since Mr. Snowden's revelations, terrorist tradecraft changed, and they moved immediately to encrypted apps for their communication in trying to find devices that were encrypted, wrap their lives in encryption, because they understand the power of encryption.

And so there's no place we see this collision between our love for privacy and the security of encryption and public safety than in fighting terrorism, especially ISIL. Because for the FBI's responsibility, which is here in the United States, every day we're looking for needles in a hay stack. And, increasingly, the most dangerous needles go invisible to us, because that's when ISIL moves them to an encrypted app that's end-to-end encrypted and a judge's order is irrelevant there.

That's why this is such an urgent feature of our work. It has huge implications for law enforcement overwhelmingly, but it has profound implications in the fight against terrorism.

Mr. KING. Do you get any signals that the American public or the United States Congress is contemplating some of the things that you discussed here to the depth that it would be a component in the decisionmaking?

Mr. COMEY. I don't know. I know everybody's interested in this and everybody, all thoughtful people see both sides of this and are trying to figure out how to resolve it, how to resolve it practically, how to resolve it technically. And the other challenge is—not to make it harder—there is no it. There isn't a single it. There's all different kinds of manifestations of this problem we call going dark.

So what I see is people of good will who care about privacy and safety wrestling with this. Court cases are important, but they are not going to solve this problem for us.

Mr. KING. Let me suggest that—I will just say: I think it's a known and a given that ISIS or ISIL is seeking a nuclear device and has pretty much said that publicly. If we had a high degree of confidence that they had—that they were on the cusp of achieving such capability and perhaps capability of delivering it, if that became part of the American consciousness, do you think that would change this debate that we're having here today?

Mr. COMEY. I do worry that it's hard to have nuanced, complicated conversations like this in an emergency and in the wake of a disaster, which is why I think it's so important we have this conversation now, because in the wake of something awful happening, it will be hard to talk about this in a thoughtful, nuanced

way. And so I think that's why I so welcome the Chairman having this hearing, and having further conversations about it.

Mr. KING. Thank you, Director. And I will just state that my view is that I want to protect the constitutional rights of the American people, and I would like to be able to have this framed in law that reflects our constitutional rights. But I would like to have us consider how we might keep a nation safe in the face of this and how we might prosecute a global war against radical Islam, even in the aftermath of a decision that might be made by either a judge or the United States Congress.

I thank you, Mr. Chairman, and I yield back the balance of my time.

Mr. GOODLATTE. The Chair thanks the gentleman.

The gentlewoman from California, Ms. Bass, is recognized for 5 minutes.

Ms. BASS. Thank you, Mr. Chair.

And thank you, Director Comey, for your time and your patience with us today.

I had a townhall meeting in my district on Sunday, and actually a couple hundred people showed up, and it was a general townhall meeting talking about issues that Congress is dealing with, and much to my surprise, this was a burning issue. And many of my constituents came to ask me questions, and I told them that they could suggest some questions and I would ask you. So maybe you could speak to some of my constituents today so I can send them a clip of your testimony.

Basically, in general, they had a hard time believing—I mean, they were not supportive. They don't want, you know, Apple to comply. But they had a hard time believing that the FBI couldn't already do this. And so a couple of the questions were: How have so many others cracked iPhones and shared their findings with videos and how-to articles?

And given that you described it, not as a back door but getting the dogs, you know, away so that you can pick the lock, their question was: What other intelligence community agencies has the FBI worked with, considering there's at least 12 in the government? Between all of these agencies, how is it that you haven't been able to call the dogs off and pick the lock?

Mr. COMEY. There are actually 16 other members of the U.S. intelligence community. It pains me to say this, because I—in a way we benefit from the myth that is the product of maybe too much television. The only thing that's true on television is we remain very attractive people, but we don't have the capabilities that people sometimes on TV imagine us to have. If we could have done this quietly and privately, we would have done it.

Ms. BASS. Right.

Mr. COMEY. This litigation is difficult. It's especially difficult, as I said, for the people who were victimized in San Bernardino, and so we really can't. As I said, there may be other models, other permutations and combinations where we have different capabilities, but I'm here to tell you here—and, again, maybe tonight someone will call us and say: I've thought of something. Apple is very good at what it does. It's a wonderful company. It makes wonderful products, right? They have set out to design a phone that can't be

opened, and they're darn near succeeding. I think with the 6 and beyond, they will have succeeded. That doesn't make them bad people, that just poses a challenge for us that we're not yet up to meeting without intervention from courts.

Ms. BASS. Since you can clone iPhone contents to compatible hardware and test passwords on the clones without putting the original at risk, can't you use so-called brute force methods to guess the passcode?

Mr. COMEY. Not with the—I think this is what Mr. Issa was asking about. I think a lot of tech experts ask, why can't you mirror the phone in some way and then play with the mirror? For reasons I don't fully understand, not possible in this circumstance. So we do want to try and brute force the phone; that is the multiple guesses. But we need first—we'll do that ourselves, but we need removed the auto-erase function and the delay-between-guesses function, which would make us take 10 years to guess it. If we have those removed, we can guess this phone's password with our computing power in 26 minutes, is what we're told, because we have enormous computing power in the U.S. Government, but we need to be able to bring it to bear without the phone killing itself.

Ms. BASS. Thank you. I yield back the balance of my time.

Mr. GOODLATTE. The Chair recognizes the gentleman from Idaho, Mr. Labrador, for 5 minutes.

Mr. LABRADOR. Thank you, Mr. Chairman.

And thank you, Director, for being here. Thank you for what you're doing. I know you have a very difficult job as you're trying to balance both security and privacy.

I do have a few questions. As you're looking at the laws that are in place, like CALEA and FISA, or the other different avenues that we're talking about, something that concerns me is that this is very different than some of the examples that have been given here. For example, when you have—when you're going into a home, if you're asking for a key, if you go to the landlord, that key's already made, and you can go to the landlord and you can say, "I have a warrant here," and that key is made, "Can you please give me a key for that," where the method of creating that key, even if the key does not exist, is already—does already exist. This is very different than that. Would you agree?

Mr. COMEY. Yes. You're exactly right. There's a difference between, "Hey, landlord, you have this spare key; the judge directs you to give it to us," and, "Hey, landlord, we need you to make a key for this lock."

Mr. LABRADOR. Yeah.

Mr. COMEY. And that's a legal question as to whether the particular statutory authority we're using here, the All Writs Act, extends to that.

Mr. LABRADOR. Correct.

Mr. COMEY. We think in the government there's a reasonable argument to be made it does and should, and on the other side, lawyers for Apple argue it doesn't, and that's what the judge will sort out.

Mr. LABRADOR. But this goes even one step further. In this scenario, the landlord can create the key, has the ability to create the key, and the technology to create the key already exists. In the

Apple case, that's not the case. They have never created the key that you're asking for. Isn't that correct?

Mr. COMEY. I don't know whether that's correct or not.

Mr. LABRADOR. Well, as far as we know, as far as they're letting us know, there's no way for them, as they're telling us—because if not, I think they would be violating the judge's order. If they have an ability to do this, I do agree with you that they would be violating the judge's order, but what they're telling us is that ability does not exist. Isn't that correct?

Mr. COMEY. I think that's right. I think, obviously, their general counsels are very smart guys here; he can talk about this. But I think what they're saying is: We can do it, but it would require us to sit at a keyboard and write new code that doesn't currently exist.

Mr. LABRADOR. Correct.

Mr. COMEY. Whether there's a meaningful distinction between that, and someone who already has a key legally is something a judge will have to sort out.

Mr. LABRADOR. So what concerns me is the old legal maxim that, you know, bad cases make bad law. This is clearly a bad case. We all want you to get access to this phone through legal means, because maybe it would uncover some of the problems that we have in the Middle East; maybe there's some evidence in there that could really lead us to take some terrorists down. I think we are all there, but the problem is that this is a bad case. This is a person who, obviously, is dead, who has never given his code to somebody else.

And I'm concerned that, as we're looking down this road, what we're doing is we're opening the door for other things that could actually be detrimental to our safety and security. For example, I think you've testified many times that we're getting hacked all the time. Isn't that correct?

Mr. COMEY. Yes.

Mr. LABRADOR. So maybe one of the reasons that Apple is refusing to do this or is hesitant to do something like this, because they know that even they get hacked, and when you open—when you create that key that doesn't exist at all right now, you're actually opening up every other phone that's out there. Do you see how that could be a concern?

Mr. COMEY. I see the argument. The question the judge will have to decide is, is that a reasonable argument?

Mr. LABRADOR. Because you——

Mr. COMEY. Sorry.

Mr. LABRADOR. No. I'm sorry.

Mr. COMEY. Go ahead.

Mr. LABRADOR. You said that Apple is highly—they are highly professional in keeping secrets. Would you say that the Federal Government also has very good people that are highly professional in keeping secrets?

Mr. COMEY. Parts of it.

Mr. LABRADOR. Me too.

Recently, we've learned that there's been a hacking incident at the IRS. Are you familiar with that?

Mr. COMEY. Yes.

Mr. LABRADOR. So that's what I'm concerned about. The moment that you open up that door, the moment that you open up that key that doesn't currently exist, you're actually allowing all these hackers that are out there—and some of them are our enemies that are trying to do us harm, whether it's economic harm or whether it's actual terrorism. They're out there looking for ways to actually get into your iPhone, into my iPhone, into everybody else's iPhone, and at some point—that's why you have such a difficult job—is we have to balance that safety and security.

Do you think that this capability that you're asking for can only be used pursuant to a warrant?

Mr. COMEY. The capability that the judge has directed Apple to provide?

Mr. LABRADOR. Correct.

Mr. COMEY. I think that's the way it's—that's the procedural posture of it. There's a warrant and the judge has issued an order.

Mr. LABRADOR. That's how it is issued right now, but do you think that that can only be obtained through a warrant? Are you seeking to obtain it later through other means other than warrants?

Mr. COMEY. I don't know how we would if it's in Apple's possession. Unless they voluntarily gave it to someone, there would have to be a judicial process——

Mr. LABRADOR. Okay.

Mr. COMEY [continuing]. If they maintained it afterwards.

Mr. LABRADOR. Thank you very much. I've run out of time. Thank you.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Louisiana, Mr. Richmond, for 5 minutes.

Mr. RICHMOND. Thank you, Mr. Chairman.

Before I start, I'd like to enter into the record two articles. One is from the Toronto Star, titled "Encrypted Evidence Is Increasingly Hampering Criminal Investigations, Police Say." And another one is from the Baton Rouge Advocate, which says, "The Brittney Mills Murder Case Has Put Baton Rouge in the Middle of the National Cell Phone Encryption Debate."

Mr. GOODLATTE. Without objection, they will be made part of the record.

[The information referred to follows:]

Encrypted evidence is increasingly hampering criminal investigations, police say

Not even search warrants make a difference

BY: Mark Greenblatt, Scripps News, and Robert Cribb, The Toronto Star
POSTED: 2:58 PM, Nov 4, 2015
UPDATED: 3:54 AM, Nov 6, 2015

WASHINGTON, D.C. - Barbara Mills, a retired nurse in Baton Rouge, has been tormented for seven months by questions no mother should have to ask: Who killed her 29-year-old daughter Brittney in cold blood, and why is new privacy technology allowed to potentially stop the police from finding out?

Brittney's murder is only one of many serious crimes in the United States and Canada that could go unsolved because Apple and Google are deploying strong encryption on cell phones and messaging applications that even the cops can't break through. The advanced privacy technology, introduced after Edward Snowden revealed the NSA's warrantless surveillance, is designed to keep all prying eyes away from files or messages if the correct password is not used.

In a joint investigation, Scripps News and The Toronto Star have found the very encryption that has become so prized by technology firms and many consumers is also becoming a critical tool for child molesters, drug dealers and other criminals who can hide evidence the authorities say they can no longer access, even with a search warrant. Even a law-abiding citizen who loses a loved one, like Barbara Mills, is now unable to recover files stored on the fully encrypted phones if they didn't obtain their relative's password in advance.

It's a battle being waged between law enforcement in the U.S., Canada and other

countries and privacy advocates, with both sides claiming they're trying to protect your safety. Police agencies contend they are losing critical tools to track and arrest criminals. Privacy advocates argue that governments around the world have lost the trust of the public, while arguing encryption protects vulnerable groups. They often say that investigators have other tools at their disposal to solve crimes and do not need access to text messages or stored data.

At this stage of the battle, law enforcement is losing. Scripps and the Toronto Star made numerous requests over several months across all levels of government asking for specific cases where investigations were thwarted because of encryption. Law enforcement agencies had many anecdotes, but are just now starting to collect data.

But in Baton Rouge, local authorities have no hesitation blaming Apple's latest encryption for bringing their search for the person who shot Brittney Mills to a near halt. Mills, a single mother who was eight months pregnant with her second child, opened her apartment door late one evening last April. Police believe she knew the killer. She refused to let the still unknown person borrow her car, they believe, and was shot shortly after. Her unborn but nearly full-term baby boy clung to life for a week before dying. Mills leaves behind a daughter, now 10 years old.

Police are convinced clues to the murderer's identity lie inside the victim's Apple iPhone. "She did say she had a diary in her phone and that everything negative that happened to her was in that diary," her mom Barbara said. "If that phone could help solve that case then I think law enforcement and law enforcement alone should be able to go into those phones and access whatever it is they need to access. You have two murders here. Not one, but two."

But like many consumers, Brittney Mills never shared her phone's password with anyone. Baton Rouge authorities obtained her family's permission to look inside of it but could not get past Apple's encryption even after reaching out to the FBI and the Secret Service for help.

"I'm at a dead end right now and I need that information to make sure we fully investigate this case and try to bring justice to this family and our community," East

Baton Rouge District Attorney Hillar Moore said.

Compounding the problem, if police or any user enters the wrong password in to an iOS device six times in a row, a message will display saying the device is disabled.

So with the Mills murder case going cold, Baton Rouge authorities obtained a search warrant this September in an attempt to force Apple to help them break through the company's encryption. But two days after receiving the court-ordered search warrant, Apple's Privacy & Law Enforcement Compliance team delivered the bad news to homicide investigators, concluding in a brief email that stated, "Since the device is running iOS version 8 or a later version, the iOS extraction cannot be completed."

Investigators were able to successfully retrieve a trove of information from Brittney's Apple iCloud account, but they say the last time a backup of her phone occurred was months before the crime, meaning her most recent communications and activities remain unknown to police, and her personal diary was not included in any of the files recovered from the iCloud backup.

"This encryption just tells you, tells drug dealers, tells killers, (to) do what you want with impunity because law enforcement can't get into your phone," Moore said.

Apple declined repeated requests to comment on the record about the Mills murders, or any related issues.

But in an open letter to customers that addresses the topic more broadly, Apple's CEO Tim Cook explains on the company's Website "we respect your privacy and protect it with strong encryption."

Google has announced full-disk encryption in its newest Android 6.0 Marhshmallow operating system, which was launched in late October. Law enforcement officials remain in early stages of collecting information about the impact of Apple's iOS8, released one year ago, but in some jurisdictions the numbers are beginning to trickle out.

In Manhattan, the office of District Attorney Cyrus R. Vance Jr. says that in less than 12 months "roughly 111 iPhones running iOS 8 or newer were inaccessible" to its staffers.

Joan Vallero, a spokesperson for Vance, says the time period tracked was from last October 2014 to this September.

Vallero says the lack of access disrupted active investigations into the attempted murder of three individuals, the repeated sexual abuse of a child, an ongoing sex trafficking ring, and numerous assaults and robberies, among other everyday crimes. She said not every disrupted crime will be unsolvable, but says the delays experienced by investigators can keep criminals in communities for longer periods.

The battle over encryption crosses international borders. The Toronto Police Service revealed to Scripps News and The Star how pedophiles are catching on and even coaching each other on how to use the latest encryption advances to conceal evidence from authorities. Toronto Detective Paul Krawczyk of the child exploitation division entered one of the "boy love" online communities he regularly monitors that he says is one of many virtual meetup spots for pedophiles.

From his desk, he located a conversation taking place that explained how American "boy lovers" have an advantage over those in some other nations, noting how no U.S. laws exist that compel criminals to hand over their private passwords that police would use to decode their files. The online user wrote, "in the U.S. (not turning over passwords) won't get you jail time. It will get the cops to abandon the investigation against you without filing charges. Just invoke the 5th Amendment and that's the end of it."

Another user provided advice to another "boy lover," instructing him to begin using a specific text messaging service that encrypts text messages, so that if police ever come knocking with a search warrant "they won't get anything off of your phone when it comes to chat."

The Federal Bureau of Investigation has been trying to raise the alarm in the United States with repeated trips to Capitol Hill, but has so far been rebuffed. Technology firms and privacy advocates pushed back strongly, launching a number of campaigns, such as SaveCrypto. The initiatives petitioned the White House to side against groups advocating for a key for law enforcement to unlock encrypted devices if officers have a search warrant. In September, Twitter signed on to the petition, joining Dropbox and

others. Last month, the White House signaled it would not, for now, push for the legislation.

Privacy advocates such as the Silicon Valley-based Electronic Frontier Foundation declared victory.

"You can't make a back door in a house that only law enforcement can enter," said EFF staff attorney Nate Cardozo. "If Apple were to compromise the encryption on the behest of the FBI for instance, and I was travelling in China or France or Israel or Russia or Brazil, I would no longer be secure in knowing that my iPhone wasn't being intercepted by the local authorities there."

Cardozo says that domestically businesses also could face an increased risk of corporate espionage if a back door were built in.

A research paper published this July by the Massachusetts Institute of Technology and co-written by 15 of the world's top cryptographers and computer scientists concluded that requiring a back door for law enforcement would be akin to "mandating insecurity."

Investigators, left to deal with encrypted operating systems on cell phones, face other mounting challenges. Popular new messaging applications such as Apple's iMessage and Facebook's WhatsApp also automatically encrypt messages by default.

"I think encryption is a good thing. I think it provides security for the public in their online behaviors," said Scott Tod, deputy commissioner of the Ontario Provincial Police. "I also think that there's an issue in regards to building a wall too high and a moat too deep."

Tod says about 80 percent of the digital communications officials in his Ontario office now obtain as evidence after a court-issued search warrant are "as good as garbage."

The Royal Canadian Mounted Police cites another case in which it attempted to intercept and read encrypted e-mails among a group of high-level drug traffickers. Other law enforcement agencies wanted the Canadian police agency to either dismantle the

communication network or decrypt the messages.

"With judicial authorization in hand, the RCMP dedicated thousands of hours to this effort, but was ultimately not successful because of various technical and jurisdictional challenges," Sgt. Harold Pfleiderer, a spokesperson for the RCMP, wrote in an email.

Last week, a working group of local, state and federal officials formed that will begin to collect statistics across the nation, said David Matthews, the chair of the technology and digital evidence committee of the Association of State Criminal Investigative Agencies. Matthews admits the law enforcement community as a whole has not prioritized collecting the statistics needed to communicate what they are seeing on the ground.

If you have a tip or an update about encryption's impact on criminal investigations, email mark.greenblatt@scripps.com *and* rcribb@thestar.ca.

Angela M. Hill (@AngelaMHill), Scripps National Investigative Producer, contributed to this report.

(This project was jointly reported by Scripps News and The Toronto Star.)

The Brittney Mills murder case has put Baton Rouge in the middle of the national cellphone encryption debate

Slaying draws BR into national debate

By Danielle Maddox

dmaddox@theadvocate.com

Photo from Facebook -- Brittney Mills

Baton Rouge detectives can't get into murder victim Brittney Mills' iPhone, which they hope holds clues to a killing that so far has stumped them.

Why would a cellphone be encrypted in a way that thwarts local police investigating a homicide?

The answer lies in the fallout from Edward Snowden's disclosure that the National Security Agency was vacuuming up Internet data and information from the several billion phone calls Americans made each day. The revelation prompted Apple and Google to allow people to make it impossible to open their smartphones without a pass code — drawing Baton Rouge into a national debate.

If the owner of a phone dies, as in Mills' case, and hasn't told anyone the pass code, the manufacturers claim even they cannot access the device. And if the owner of a phone is a criminal who simply refuses to tell authorities the pass code, the same could hold true.

That can lock the contents — photos, text messages, voicemail, email, contacts, call history, iTunes material and notes — inside the phone for good.

If you don't put in the pass code, "you can't extract human readable data from the phone," said Jonathan Rajewski, associate professor of digital forensics at Champlain College in Vermont. "Even if you took the chip and hooked it up to another device, the information would still be encrypted."

Now, government and the tech industry are at loggerheads: Should companies guarantee the government, particularly law enforcement, access to these fully

encrypted devices, or will that weaken the encryption software, rendering it useless against hackers and foreign governments?

From FBI Director James Comey to East Baton Rouge Parish District Attorney Hillar Moore, law enforcement has told Congress that companies must find a way to give access to police agencies with a search warrant.

But tech industries have asked President Barack Obama to embrace encryption in its policies and resist regulating their security software.

In August 2013, Obama created an advisory committee on cybersecurity after Snowden, a former government contractor, publicized government programs that collect electronic data on Americans and foreign governments. The committee concluded the government and U.S. companies should not only embrace encryption but also should increase their use of it to better protect data.

Despite law enforcement and intelligence concerns, the committee further recommended the U.S. government should not "subvert, undermine, weaken, or make vulnerable" encryption software widely available on the market.

Those who support strong encryption claim it prevents crime, specifically hacking, and protects personal property. Apple and other players in the tech industry say the encryption upgrades made to their software mends the trust they had with international companies that was damaged during the Snowden leaks.

Critics of the upgraded encryption argue that while privacy is important, law enforcement needs legal access to encrypted phones when an investigation requires it. Criminals, like the one who shot Mills, go free when vital clues remain locked away on digital devices, they say.

The East Baton Rouge Parish Sheriff's Office said it has begun to see more encrypted phones during investigations, and Moore, the parish district attorney, recently wrote to Congress in opposition to Apple's latest encryption upgrade.

"Apple advertises this as a plus for people who buy their phones," Moore said, noting such encryption makes the phone ideal for criminals.

U.S. Sen. David Vitter, a Republican, said lawmakers are looking for a way to balance privacy with public safety but have not found a comprehensive solution.

The debate expanded well beyond individual privacy at a July hearing before the U.S. Senate Judiciary Committee, on which Vitter sits.

Peter Swire, a professor at the Georgia Institute of Technology, supports encryption. Swire argued at the committee hearing that secure communications play a vital role

in national security.

Jim Pasco, executive director of the National Fraternal Order of Police, says it's "convoluted logic" to believe that providing a way for police to open a cellphone could cause a national security problem, noting that encryption can stymie efforts to prevent terror attacks or investigate such crimes after they occur.

"It causes a much bigger national security issue when law enforcement can't get in," he said. "In making that technology available to criminals, you inadvertently make them harder to catch.??

Harley Geiger, senior councilman of the Center for Democracy and Technology, a nonprofit that advocates on Internet issues, argues that encryption makes us safer even though it can make information more difficult for law enforcement to access.

"Our smartphones and our Internet communications carry a great deal of sensitive content, and it's important to protect that content from unauthorized parties," he said. "There is a safety trade-out no matter which way you go."

Geiger said companies like Apple and Google are simply responding to market demand.

"Users, consumers and businesses that use digital service are demanding strong security," Geiger said.

Requiring U.S. companies to allow access for government surveillance would put them at a competitive disadvantage in an international industry, he said.

Manhattan District Attorney Cyrus R. Vance Jr. claims encryption has changed the dynamic between law enforcement and the public, and the change is for the worse, saying 74 investigations in his jurisdiction have been disrupted because of encryption.

"As it stands today, Apple and Google have decided who can access key evidence in criminal investigations," he told the Judiciary Committee hearing in July.

He added that he'd like Apple and Google to come to the table to discuss the problem, but as of now, they won't.

Pasco is on the same page.

"This is the kind of situation that tends to just simmer until there's some sort of horrible tragedy or we've reached our crisis stage in sheer numbers of crimes not solved because of a lack of available data," Pasco said.

Moore, Baton Rouge's district attorney, says the encryption problem "hits home quickly with the Mills family."

Mills, 29, and eight months pregnant, was fatally shot April 24 at her Ship Drive apartment. Authorities believe Mills opened the door for someone who wanted to use her car and was shot when she refused. Doctors delivered her son, Brenton Mills, who died a week later .

Investigators said the shooter likely was someone Mills knew. They have looked to her cellphone for evidence, but her iPhone uses iOS8 software that blocks anyone without the pass code.

IPhone owners can choose to use Touch ID, which unlocks the phone with the owner's fingerprint, but Mills used only a pass code, Moore said.

Apple allows only a few consecutive pass code guesses before it returns the phone to factory settings — with none of the user's information on it.

Moore said investigators are increasingly encountering problems with encryption. On several occasions, police have tried to search for information about drug dealers from the phones of people who fatally overdosed but did not know the access codes, he said.

Sgt. Brian J. Blache, of the East Baton Rouge Sheriff's Office, said as more people use cellphones for everyday tasks, the information stored in them will be increasingly useful.

About 90 percent of the Sheriff's Office cases involves some type of cellphone or computer analysis, Blache said.

If nothing can be extracted from a cellphone, Blache said, the Sheriff's Office will lock it up in evidence with the hope that technology down the line will allow them to open it later.

Law enforcement officers can check other devices, including computers, to see if people backed up cellphone data there, or virtual platforms where people may store emails, call logs and, in some cases, old text messages from their phone. Often, information about where someone has been is available from cellphone service providers or from Internet app companies that serve up information based on the user's location.

Getting that information can be obtained with a warrant. But Blache noted some of that data depends on what location settings people select.

Also, Rajewski said Internet companies and mobile service providers keep such

information for business purposes, not specifically for law enforcement's benefit, and the retention period varies from company to company. He said the higher level of security will be more widespread moving forward as people buy new phones with the software needed to run the encryption programs.

Moore said a law should be passed prohibiting manufacturers from selling smartphones and mobile devices that the government cannot access.

Pasco, the director of the National Fraternal Order of Police, agrees that some sort of law needs to be put in place.

"Every day and week that we waste time means more crimes unsolved and more terrorist incidents unprevented," he said.

Mr. RICHMOND. Thank you, Mr. Chairman.

And let me just say, and Director Comey, you have mentioned the Brittney Mills case a number of times, and I just want to paint the scenario for everyone in the room and put a face with it. This is Brittney Mills, and this is Brittney Mills almost 8 months pregnant with her daughter. In May of last year, Brittney was murdered in my district. She was a mother. She was 8 months pregnant with her second child at the time. Someone came to her door and killed her, and a couple days later, her unborn child—or born child also died. And according to her family and her friends, she kept a very detailed diary in her phone. And her family, who are here today, Ms. Mills, Ms. Barbara Mills, will you please stand, and Tia and Roger, her family would like the phone opened so that our district attorney, who is also here today—thank you for standing—our district attorney, who is also here today, Hillar Moore, can use that to attempt to find the murderer who committed this crime.

And I guess my question is, we balance privacy, public safety, and criminal justice, but are we in danger of creating an underground criminal sanctuary for some very disturbed people, and how do we balance that?

Mr. COMEY. We are in danger of that. Until these awesome devices—and that's what makes it so painful. They're wonderful. Until this, there was no closet in America, no safe in America, no garage in America, no basement in America that could not be entered with a judge's order. We now live in a different world, and that's the point we're trying to make here. Before we drift to a place where a whole lot of other families in incredible pain look at other district attorneys and say, "What do you mean you can't; you have a court order," before we drift to that place, we've got to talk about it, because privacy is awesome, but stopping this kind of savagery and murder and pedophilia and all the other things that hide in the dark spaces in American life is also incredibly important to us.

That's why this conversation matters so much, but it's also why we have to talk to each other. There are no demons in this conversation; we care about the same things. But it is urgent, and there's no more painful circumstance to demonstrate it than in the death of that beautiful woman and her baby.

Mr. RICHMOND. Well, and I do appreciate your saying we have to talk to each other, because just in the small time that I was able to put the representatives of Apple and the district attorney in the room, I think we made some progress and maybe some alternatives, and maybe we'll get somewhere. But it is a very difficult balancing act, and I think the people from Apple are very well intentioned and have some real concerns.

But let me ask you this. I took a congressional delegation trip over to the Ukraine. And when we landed our plane, we were on the runway, and our security advisors came on to the back and said, if you don't want your phone hacked and people to have access to your text messages, your pictures, your emails, and everything else, we advise you to power your phone off and leave it on the plane. And no one is in close enough proximity right now to do it, so if you need to make a call, make a call, but when we get closer to the terminal, you need to power that phone down.

So does Ukraine have better technology—well, they were really worried about Russian hackers. But does Russia have that much of a technology advantage over us that they can get into my phone while I'm on it and it's in my possession, and we can't get into a phone that we have in our possession?

Mr. COMEY. The difference—and I'm going to be careful what I say in an open setting—is that some countries have different control over their infrastructure and require providers in their country to make accommodations that we do not require here to give them greater surveillance capabilities than we would ever imagine in the United States. That's the first thing.

The second thing is we are a rule of law country. The FBI is not cracking into your phone or listening to your communications except under the rule of law and going to a judge. Those are the two big differences.

But countries have capabilities and, in part, based on accommodations that device makers and providers have made in those countries that are different than in this country.

Mr. RICHMOND. Thank you, Mr. Chairman. I see my time has expired.

Mr. GOODLATTE. The Chair recognizes the gentlewoman from Washington State, Ms. DelBene, for 5 minutes.

Ms. DELBENE. Thank you, Mr. Chairman.

And thank you, Director Comey, for being with us and for all of your time.

I've worked my career in technology on email and mobile communications and constantly heard from customers, both consumers and businesses and even the government, to make sure that information was protected and that devices were secure. And in your testimony, you state that you're simply asking to ensure that you can continue to obtain electronic information and evidence, and you seem to be asking technology companies to freeze in place or revert back to systems that might have been easier to access, but don't you think in general that that's much—an oversimplification of this issue, because we all know that bad actors want to exploit vulnerabilities to break in to any number of things, from a phone, a personal device, to our power grid? These things aren't static. They're changing constantly, and they're getting smarter every day. The bad actors are getting smarter every day, and we need to be smarter every day in terms of protecting information.

So, in that type of environment, how would you expect the technology company not to continue to evolve their security measures to keep up with new threats that we see?

Mr. COMEY. First of all, I would expect security companies and technology companies to continue to try and improve their security. That's why it's important that all of us talk about this, because it's not the company's job to worry about public safety, right? It's the FBI's job, Congress's job, and a lot of other folks in the government, so I don't put that on the companies. But the other thing that concerns me a little bit is this sense that if we have a world where people comply with government warrants, it must be insecure. And I don't buy that, because there are lots of providers today of email service, of tech service who have highly secure systems who, because of their business models, visualize the information in plain

text on their servers so they comply with court orders. I have not heard people say their systems are insecure. They simply have chosen a different business model.

So I actually don't think it's—again, a lot of people may disagree with me. I actually don't think in the main it's a technological problem. It's a business model problem. That doesn't solve it, but that gets us away from this it's impossible nonsense.

Ms. DELBENE. But we know more and more, in fact, we're seeing—we're talking about phones today, but we are talking about the growth in the Internet of things of more and more personal devices where security will be even more critical, and so it's hard to say—you're talking about a world where it's confined to the way the world works today. I think that absolutely is not the situation that we're facing. We're seeing evolution every day, and these are devices that are connected to networks, and information is flowing, and that information might be someone's financial information or personal information that if it is exploited would create a security issue itself.

Mr. COMEY. I agree.

Ms. DELBENE. So don't you believe that encryption has an important role to play in protecting security?

Mr. COMEY. Vital.

Ms. DELBENE. So, now, when we've talked about what role Congress plays versus what role the courts would play, and you've kind of talked about both in different scenarios. You've talked about privacy versus security and that Congress should play a role there but that the courts should decide whether or not there's a security breach if there's a piece of technology that breaks into a device and whether or not there's a concern that that will be widely available. Yet the tension isn't really between just privacy and security. It's between security and security and protecting people's information. So how do you—where do you think Congress plays a role versus the courts when you've talked about both of them in your testimony today?

Mr. COMEY. I think the courts have a job to, in particular cases, interpret the laws that Congress has passed throughout the history of this country to try and decide: The government is seeking this relief; does that fit within the statute? That's the courts' job, and they're very, very good at it.

The larger societal problem we have is this collision—that I think you've said well—between privacy and security; very difficult to solve it case by case by case. We have to ask ourselves, how do we want to govern ourselves? If you are a manufacturer of devices in the United States or you provide communication services in the United States, what are our, as a country, what are our expectations of you and demands of you? It's hard for me to see that being worked out on a common law basis, honestly, but it's going to be, because the issue is joined every single day in our law enforcement work. If nobody else gets involved, the courts will have to figure it out.

Ms. DELBENE. This isn't just an issue of U.S. companies alone, because clearly there's access to technology that could be developed in other countries that we'll not have access to and that's widely available today and people can use. But, also, then it is important,

we have laws that are centuries and decades old that have not kept up with the way the world works today, and so it is very important that Congress plays a role, because if courts are going to be interpreting those laws and those laws were written with no awareness of what's happening today, then Congress needs to play a role of making sure we have laws that are up-to-date and setting that standard so that courts can then follow.

Thank you. I yield back, Mr. Chair.

Mr. GOODLATTE. The Chair thanks the gentlewoman and recognizes the gentleman from New York, Mr. Jeffries.

Mr. JEFFRIES. Thank you, Mr. Chairman.

And thank you, Mr. Comey, for your presence here today. And as one of my colleagues mentioned, your candor and open dialogue and communication is much appreciated, and it's not always the case with high-level government witnesses and others.

You testified today that you don't question Apple's motives in connection with the San Bernardino case. Is that correct?

Mr. COMEY. Correct.

Mr. JEFFRIES. And you also testified that there are no demons in this conversation, true?

Mr. COMEY. Correct. I hope not.

Mr. JEFFRIES. But the Department of Justice has questioned the company's motives in defending the privacy of the American people. Isn't that right?

Mr. COMEY. I don't know that they've questioned their motives, in the sense that attributed sort of that they're acting with evil intent or something. I think they've—I remember a filing the department said where they think a lot of Apple's position has to do with its market power, which I, frankly, is not an illegitimate motive.

Mr. JEFFRIES. In fact, in the motion to compel that you referred to, I believe the prosecutor said that: "Apple's current refusal to comply with the court's order, despite the technical feasibility of doing so, appears to be based on its concern for its business model and public brand marketing strategy."

Is that the statement that you're referring to, sir?

Mr. COMEY. Yeah. And I think that's—that's fair. I bet that's accurate. Apple has a legal obligation—because I used to be the general counsel of a public company—to maximize shareholder value. They're a business, and so I would hope that's part of their motivation. And it's not a bad thing if it's entirely their motivation. Their job is not to worry about public safety. That is our job, all of us in this room who work for the government.

Mr. JEFFRIES. William Bratton is the police commissioner of the New York City Police Department. Is that right?

Mr. COMEY. Yes.

Mr. JEFFRIES. That's the largest department in the country?

Mr. COMEY. Yes.

Mr. JEFFRIES. And he's one of the most respected law enforcement professionals in the country. Would you agree with that?

Mr. COMEY. I agree with that very, very much.

Mr. JEFFRIES. Now, at a February 18 press conference in New York City, publicly accused Apple of corporate irresponsibility. Are you familiar with that remark, sir?

Mr. COMEY. I'm not.

Mr. JEFFRIES. Okay. Do you agree with that strident statement, that Apple is engaging in corporate irresponsibility——

Mr. COMEY. I'm——

Mr. JEFFRIES [continuing]. By vindicating its——

Mr. COMEY. I don't know that Bill said that, but I'm not going to characterize it that way. I don't think they're acting irresponsibly. I think they're acting as a corporation in their self-interest, which is the way—which is the engine of innovation and enterprise in this country.

Mr. JEFFRIES. Fundamentally, as it relates to the position of those of us who are on the Judiciary Committee, as well as Members in the House and in the Senate, guardians of the Constitution, this is not about marketing or corporate irresponsibility, correct, this debate?

Mr. COMEY. I hope not. I mean, I hope part of it is, and that's a voice to listen to, but they sell phones. They don't sell civil liberties. They don't sell public safety. That's our business to worry about.

Mr. JEFFRIES. Right. But in terms of our perspective, this is really about fundamental issues of importance as it relates to who we are as a country, the Fourth Amendment of the United States Constitution, the reasonableness of government intrusion, the rule of law, the legitimate centuries-old concern as it relates to government overreach and the damage that that can do. This is fundamentally a big picture debate about some things that are very important to who we are as a country, correct?

Mr. COMEY. I agree completely.

Mr. JEFFRIES. Okay. Now, in terms of the technology that's available today, Americans seem to have the opportunity to choose between privacy or unfettered access to data which can reveal the far reaches of their life to a third party, to a government, to a bad actor. Would you agree that there's an opportunity that the technology is providing for Americans to choose privacy?

Mr. COMEY. I don't agree with that framing, because it sounds like you're framing it as we either have privacy or we have unfettered access by bad actors. I don't accept that premise.

Mr. JEFFRIES. Okay. So let me ask a few questions. One of the obstacles to unfettered access is the passcode, correct? The passcode.

Mr. COMEY. Yeah.

Mr. JEFFRIES. A four-number or a six-number passcode.

Mr. COMEY. I naturally quibble because I'm a lawyer, but I'm just stuck on "unfettered"——

Mr. JEFFRIES. Okay.

Mr. COMEY [continuing]. But one of the obstacles to access to a device——

Mr. JEFFRIES. Let me drop "unfettered."

Mr. COMEY. Okay.

Mr. JEFFRIES. The passcode is an obstacle, correct?

Mr. COMEY. Correct. Correct.

Mr. JEFFRIES. Now, you can choose a passcode or choose not to activate a passcode, correct?

Mr. COMEY. I think that's right.

Mr. JEFFRIES. Okay. Now, whether you back up your system or not is an issue as it relates to access, correct? In other words, if you don't back up your system, you don't have access, correct, to the cloud?

Mr. COMEY. Yeah. I think if you don't back up your system to the cloud, there's nothing in the cloud that could be obtained by a warrant.

Mr. JEFFRIES. Right. Now, with respect to auto erase, that is a choice that's being made. In other words, you have to actually affirmatively choose auto erase. If you didn't choose it, in this particular case or in any other case, eventually your computer is powerful enough to get access to the data, correct?

Mr. COMEY. I think that's right for the 5C. I think that's right. And folks from Apple could tell you better. I think for the later models, it's not a choice, but I think it's a—I'm reasonably confident it's a choice for the 5C.

Mr. JEFFRIES. My time has expired, but I think it's important as we frame this debate to understand that it is actually the American citizen that is choosing on at least three different occasions in three different ways the value of privacy, and that's something that we should respect as Congress attempts to craft a solution.

Mr. COMEY. Okay.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Rhode Island, Mr. Cicilline, for 5 minutes.

Mr. CICILLINE. Thank you, Mr. Chairman.

Thank you, Director Comey, for your service to our country. Thank you for being here today and for the outstanding work of the men and women at the FBI.

We all, of course, acknowledge the incredible horrors of the San Bernardino attack, but I think, in many ways, what we're struggling with, as Ms. DelBene said, not necessarily security versus privacy, but security versus security. And the real argument that the danger that exists for the misuse of this new technology by foreign agents, by terrorists, by bad actors, by criminals will actually make us less safe in the long term. And while it might achieve your objective in the short term in this particular case, that the implications in terms of our own national security and personal security pose greater dangers. I think that's what at least I'm struggling with.

I appreciate you said this is the hardest question you've confronted, because I think it is a hard one. But the first thing I want to ask is, this is different, would you agree, than all the examples that have been used about producing items in your custody. This is a different kind of one, because it's actually compelling a third party to produce and create intellectual property which doesn't exist today.

Mr. COMEY. I understand that to be Apple's argument. I don't know enough about the other possible comparisons to give you a thoughtful response, but, yes, I understand that.

Mr. CICILLINE. But don't you think it's hard to even imagine how a court ultimately enforces that, because you have to sort of get into the head of the engineers to figure out did they actually comply with what the government order is directing them to create.

I mean, I'm not saying it's not something you're not allowed to ask for, but it is different, it seems to me, than simply asking people to produce that which they are in possession of, custodians of.

Mr. COMEY. I see that. I mean, I heard someone earlier say there's a difference between a landlord who has a key in his pocket and you say, "You got to give us the key," and, "You don't have one. Go make one for that door."

Mr. CICILLINE. Well, this will be more than——

Mr. COMEY. And the question for the judge is what's——

Mr. CICILLINE. Not just go make one, because that knowing how to make keys exists, but to develop a whole new technology and intellectual property. So I just want—I raise that because I think we have to acknowledge it's different and then decide what to do with it.

Mr. COMEY. Yeah.

Mr. CICILLINE. But in addition to that, you said repeatedly that the government doesn't have the ability to do this already. And, as you know, there was a decision yesterday by Magistrate Judge Orenstein—I'd ask unanimous consent that that memorandum and order be made part of the record—in which he actually——

Mr. GOODLATTE. It already is part of the record.

Mr. CICILLINE. Okay. Which he—and he goes through and says the All Writs Act doesn't apply. CALEA prohibits this by omission, and I think in a very clear way. But in addition to that, he goes on to say that the government argued in an unrelated case that the government actually has the ability to do this, the Department of Homeland Security Investigations, that they are in possession of technology that would allow its forensic technicians to override the passcode security feature on the subject iPhone and obtain the data.

So I think this is a very important question for me. If, in fact—is it in fact the case that the government doesn't have the ability, including the Department of Homeland Security Investigations, and all of the other intelligence agencies to do what it is that you claim is necessary to access this information?

Mr. COMEY. Yes.

Mr. CICILLINE. Because it is very—the answer's yes?

Mr. COMEY. That is correct. And I don't know. I think—I could be wrong, but I think the phone in the case from Brooklyn is different, maybe both the model and the IOS, the operating system is different, but for this—I can tell you, and, again, people know the sound of my voice—if you've got an idea, let us know, but 5C IOS 9, we do not have that capability——

Mr. CICILLINE. Okay.

Mr. COMEY [continuing]. Again, to disable. The problem is we can get into that phone with our computing power if they take off the auto-erase and the delay-between-guesses function. We will get into that phone.

Mr. CICILLINE. So do you agree, Director Comey, that if there is authority to be given to do what you're asking, that that authority has to come from Congress?

Mr. COMEY. No, I don't agree with that.

Mr. CICILLINE. So where do you think the authority comes from?

Mr. COMEY. Well, the government's already asked the court and made the argument under the court that the All Writs Act vests in the judiciary the ability to order this relief. That's what the court case is going to be about.

Mr. CICILLINE. So if the ruling made yesterday remains, which rejects the notion that the All Writs Act applies and that CALEA, in fact, is congressional intention on this, and the fact that we didn't act on it means you have authorization has not been provided, then would you agree that Congress is the only place that can authorize this, and if so, what would you recommend we do? What would that look like as we grapple with this question? Because I can tell you, for me, having read that, I think CALEA is clear; it doesn't authorize it. It's clear the All Writs Act doesn't. So if there is to be authority, assuming we decide that there should be, it seems it must come from Congress. As the Director of the FBI, what do you think that would—what would your recommendation be that would respond to what you see as your needs but also the national security interests of our country?

Mr. COMEY. Yeah. I'm not prepared to make a recommendation, but I think I get your question now. If the judges are right you that can't use the All Writs Act for this relief, what should Congress do to grant the relief? And I'm not prepared to tell you specifically what to do. I do think it's something that Congress is going to have to wrestle with.

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

Thank you, Director.

Mr. GOODLATTE. The Chair would ask unanimous consent that letters from the Computer Communications Industry Association, dated February 29; a statement for the record from Reynaldo Tariche, President of the FBI Agents Association; and a letter, dated February 29, from the American Civil Liberties Union all be made a part of the record.

[The information referred to follows:]

Computer & Communications Industry Association
Tech Advocacy Since 1972

February 29, 2016

The Honorable Bob Goodlatte
Chairman, Judiciary Committee
United States House of Representatives

The Honorable John Conyers
Ranking Member, Judiciary Committee
United States House of Representatives

Dear Chairman Goodlatte and Ranking Member Conyers:

The technology industry consistently cooperates with law enforcement in its important work to deter and investigate crimes and terrorism. Companies large and small comply with lawful and appropriately scoped legal orders, and devote significant resources to responsibly aiding government efforts to combat extremist and exploitative content.

The ongoing debate about the availability and use of encryption and other security technologies in digital devices and services often focuses on a narrowly defined trade-off between users' privacy and our collective security. That framing underrepresents other vital and legitimate equities at stake.

Our system of limited government is predicated on the principle that ends do not justify all means. While the government's goal is to obtain possibly important investigative information, it seeks to do so through methods that will undermine other goals that both the government and the public often consider to be of equal or greater importance, including personal safety, security, and freedom online.

The public has chosen to keep significant portions of their personal and financial lives in digital services and devices. But users worldwide also see the growing dangers of criminals, hackers, terrorists, and oppressive or intrusive regimes. As a result, they have demanded that the caretakers of their personal information develop the tools to stay a step ahead of those bad actors. Internet users are growing increasingly vigilant, but fundamentally the public must be able to trust that companies will do their part to keep sensitive data safe.

That trust, and more importantly, the aggregate personal well-being and security of the public, are risked when service providers and device manufacturers can be asked or compelled to weaken the digital security technologies that users demand. Safety, expression, and commerce online are all threatened by creating vulnerabilities desired by the same bad actors from whom the government seeks to protect us.

I recognize the government's desire to test the limits of the law in its efforts to prevent and investigate serious crimes. However, a fulsome consideration of the public interest makes clear

900 17th Street NW Suite 1100 Washington, DC 20006 P: (202) 783-0070 F: (202) 783-0534 www.ccianet.org

Computer & Communications
Industry Association
Tech Advocacy Since 1972

that the government's efforts should not come at the expense of the rights and overall security of the public and digital ecosystem.

Thank you for your attention.

Sincerely,

Ed Black
President & CEO
Computer & Communications Industry Association

Cc: House Judiciary Committee

900 17th Street NW Suite 1100 Washington, DC 20006 P: (202) 783-0070 F: (202) 783-0534 www.ccianet.org

Statement for the Record
Reynaldo Tariche
President
FBI Agents Association
The Encryption Tightrope: Balancing Americans' Security and Privacy
United States House of Representatives
Committee on the Judiciary

March 1, 2016

Fourteen innocent people were killed in San Bernardino on December 2, 2015 in the nation's deadliest terrorist attack since 9/11. Evidence relating to that crime might exist on the iPhone used by the terrorist Syed Rizwan Farook. FBI Agents—thousands of whom I am honored to represent—are investigating this crime and others like it. In this case, Apple has refused to abide by a federal court order requiring the company to assist the FBI with accessing the data on Farook's iPhone pursuant to a warrant. Apple's decision reflects a blatant disregard for the work of FBI Agents and constitutes a threat to national security.

First, Apple has failed to acknowledge that their customers are also our customers. It is our sworn duty to keep our customers, the American people, safe. Our duty is undertaken while adhering to Constitutional provisions barring unreasonable searches and seizures, protecting privacy. Apple's job is undertaken while adhering to an economic principle: a return on investment. While profits may dictate Apple's decisions, the Constitution dictates ours.

Second, Apple's actions now will embolden criminals, providing a safe haven for their activities. This includes the cyber-criminals. It would be unwise to disregard established search and seizure procedures to give Apple products special treatment. Terrorists, child pornographers, and others criminals should not escape lawful warrants because corporations use the promise of secure communications as a marketing tool.

Third, while Apple now claims openness to public dialogue about the company's technology, their actions belie their words. In November 2015, the FBI Agents Association, the Attorney General of Ohio, the National District Attorneys Association, and the National Sheriffs' Association jointly wrote to Apple to engage in the discussion you now seek. However, Apple did not bother to respond to that request. Rather, Apple and other technology companies have spent millions on lobbying and public relations, and have attempted to leverage the industry's significant influence to derail Congressional debate.

Fourth, if Apple is unwilling to act, then we urge Congress to do so. There are ways to resolve this problem, and the solution is not based on the false choice between absolutely secure communications and a wide-open door. Apple has worked with law enforcement to extract data from iPhones scores of times previously, and we urge the company to do so again. Absent this, Congress should enact legislation requiring companies to incorporate options into their technology that prevent smartphones from serving as barriers to lawfully-issued search warrants. Given existing technologies, this is a reasonable and practical request.

Finally, the ability to lawfully obtain the private records of criminal conspiracies is a time-tested and indispensable part of effective law enforcement. The papers and letters of the past are being replaced by the electronic data held on Apple devices. Apple is choosing to provide modern criminals with a tool that past generations of criminals never had: an impenetrable door that is booby-trapped to destroy evidence. A homeowner could not reject law enforcement officers executing a warrant by claiming they don't want to unlock the door. Likewise, Apple should not be able to stonewall the FBI and the courts simply because the company has decided not to unlock its iPhones.

We applaud Apple's innovative spirit and customer dedication. Please bear in mind that their customers are also our customers—customers who FBI Agents are sworn to protect from criminals and terrorists. Our customers deserve a means of ensuring that the drive for profits does not come at the cost of public safety.

The FBI Agents Association (FBIAA) *is an organization dedicated to providing support and advocacy to active and former Special Agents of the Federal Bureau of Investigation. Membership includes more than 13,000 active and former Special Agents of the FBI. For more information, please visit www.fbiaa.org. Contact: Paul Nathanson, 202-828-1714, media@FBIAA.org.*

WASHINGTON
LEGISLATIVE OFFICE

February 29, 2016

The Honorable Bob Goodlatte
Chairman, House Judiciary Committee
2138 Rayburn House Office Bldg.
Washington, D.C. 20515

The Honorable John Conyers, Jr.
Ranking Member, House Judiciary Committee
2138 Rayburn House Office Bldg.
Washington, D.C. 20515

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

KARIN JOHANSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

RE: House Judiciary Committee Hearing on "The Encryption Tightrope: Balancing Americans' Security and Privacy."

Dear Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee,

On behalf of the American Civil Liberties Union ("ACLU"[1]), we submit this letter in connection with the March 1, 2016 hearing, "The Encryption Tightrope: Balancing Americans' Security and Privacy."

Over the last decade, the technology industry has made significant progress in protecting the security of Americans' private data, including electronic communications, through enhanced security features and encryption technologies. This increased security has not only paved the way for advanced technological and economic development, but has been critical to ensuring free expression and an open Internet. Unfortunately, there have been calls by some to undermine– rather than support– these security advances. Specifically, the FBI is currently seeking to compel Apple to develop new software that would allow the FBI to hack into the work phone of one of the San Bernardino shooters.[2] One magistrate judge in New York has already ruled that such a request is not authorized by the law, noting that Congress has explicitly declined to provide this authority.[3] Another case on this issue is pending.

---

[1] For nearly a century the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

[2] In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0415M (C.D. Cal. Feb. 16, 2016).

[3] Devlin Barrett, *Judge Sides With Apple in Drug Case Involving Locked Phone,* W.S.J. Feb. 29, 2016, http://www.wsj.com/articles/judge-sides-with-apple-in-drug-case-involving-locked-phone-1456785910; Memorandum and Order, *In Re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 2015 WL 5920207 (E.D.N.Y 2016), *available at* http://www.politico.com/f/?id=00000153-2f2b-d640-a7fb-7fbb72380001.

The ACLU opposes the FBI efforts in the Apple case. They are unauthorized, unconstitutional, and unwise. We urge the Committee to reject any proposal that would grant the FBI the authority to conscript technology suppliers into hacking or building a backdoor into the devices of users.

I. Advancements in Encryption and Other Security Features

In recent years, Apple has added security features and enhanced encryption on its mobile devices. – responding to increased consumer demands for greater privacy and security. These features are designed to protect consumers from criminals, hackers, or even malicious foreign governments. The more recent versions of the Apple iOS operating system:

- Allow consumers to turn on a feature that makes the contents of the phone inaccessible in the event that a PIN code is incorrectly entered ten times;
- By default, create a time lag between incorrect PIN entries, to prevent a malicious actor from bombarding the phone with numerous PIN attempts in a row;
- Require the user's PIN to unlock and decrypt the data stored on the phone. In other words, without a user's PIN, no one, including Apple, can unlock an iPhone; and
- Expand the categories of data protected by industry-standard encryption to include photos, text messages, the address book, and several other forms of previously less-protected private data.[4]

Many of these changes mirror the industry trend of providing consumers enhanced security through encryption. Last September Google announced it would turn on disk encryption by default in the next version of its Android operating system, though this currently remains an opt-in feature due to reduction in speed suffered by many Android devices when encryption is used.[5] In addition, encryption is being adopted to protect data as it is transmitted over the Internet. Major companies like Google, Facebook, and Twitter all use HTTPS and other transport encryption technologies to ensure that communication between their customers and their own servers are secure. The federal government has followed the technology industry's lead, and announced that all U.S. government websites will use HTTPS encryption within two years.[6] Similarly, 76 members of Congress use HTTPS encryption by default on their official websites.[7]

---

[4] Apple had for several years included such strong encryption technology in its mobile operating system; however, prior to last year, this method of encryption only protected a few categories of data stored on devices, such as email messages and data created by third party apps. Cyrus Farivar, *Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot*, ARS TECHNICA (Sept. 18, 2014), http://arstechnica.com/apple/2014/09/17/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/.

[5] Andrew Cunningham, *Google Quietly Backs Away from Encrypting New Lollipop Devices by Default*, ARS TECHNICA (Mar. 2, 2015), http://arstechnica.com/gadgets/2015/03/02/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/.

[6] *See The HTTPS-Only Standard*, CHIEF INFORMATION OFFICER, https://https.cio.gov/ (last visited Apr. 29, 2015) ("The American people expect government websites to be secure and their interactions with those websites to be private. Hypertext Transfer Protocol Secure (HTTPS) offers the strongest privacy protection available for public web connections with today's internet technology. The use of HTTPS reduces the risk of interception or modification of user interactions with government online services.").

[7] Eric Mill (@konklone), TWITTER (Apr. 18, 2015, 4:18PM), https://twitter.com/konklone/status/589538454352097282.

The adoption of these encryption technologies has yielded significant benefits to consumers, businesses, and government agencies, providing greater protection from the ever-increasing threat posed by cyber criminals and foreign governments.

II. The Apple Case

Currently, the FBI seeks to create legal precedent that would enable it to force private companies to develop software to hack into its customers' devices and access encrypted data. In the case at hand, the FBI argues that the 1789 All Writs Act grants it the authority to compel Apple to create a mechanism that allows the FBI to circumvent the existing security features in the iPhone to access to contents of the recovered phone. As a practical matter, to comply with this order, Apple will need to do three things:

- Create new software designed to circumvent security features, which create a time lag between incorrect PIN attempts or make the contents of the phone inaccessible following ten incorrect PIN entries;
- Cryptographically "sign" the software, which indicates that the software has been developed and validated by Apple. Such a signature is necessary to push the new software onto the target phone, since, as an added security feature, iPhones will not run software that has not been validated by Apple and
- Take steps to transmit the newly developed software onto the target phone.

If the FBI is successful, the legal precedent established by this case would apply to all companies, devices, or criminal investigations. Thus, it could be used to compel other companies to build mechanisms to hack into smart televisions, computers, or even medical devices. For example, law enforcement could require a company to remotely turn on a camera in a smart television to assist with a drug investigation, or require a car company to deliver malicious software to a car's GPS system to allow tracking as part of a tax evasion investigation.

III. The FBI Efforts to Compel Apple Would Place an Unconstitutional Burden on Private Companies

If successful, the FBI's efforts in this case would represent an unauthorized and unconstitutional expansion of the government's authority. While the government can demand the production of relevant evidence, the giving of truthful testimony, or the entry necessary to search for and seize evidence, law enforcement does not hold the general power to enlist private citizens or companies as its agents.

In this case, Apple manufactured the iPhone, but it does not possess or control the personal data stored on it or even have existing software or capabilities capable of accessing such data. Thus, in order to comply with the request, Apple's engineers would have to write new software specifically designed to subvert the security measures they built into the phone. Forcing Apple to take such action would violate the Fifth Amendment. The Fifth Amendment protects innocent third parties from being conscripted by law enforcement, except in narrow circumstances. The present case clearly extends beyond these limits, and raises troubling questions about the authority of law enforcement officials.

Proposals like the FBI's are also a dramatic expansion of a dangerous idea– that the private sector should be responsible for building the government's surveillance infrastructure. Such proposals

switch the burden for surveillance from the government to companies (and through them to their customers, the American people). Consumers would be forced to purchase fundamentally insecure products, with little ability to protect their communications and stored data from cybersecurity threats. Not only does this represent an improper government intrusion, but it threatens to eliminate one of the primary privacy protections that Americans have enjoyed for the last two centuries—namely, the sheer difficulty of mass surveillance. As a practical matter, the cost to law enforcement of surveillance has provided real privacy protection by forcing law enforcement to determine whether investigations merit the use of scarce resources. Shifting the costs and burdens of surveillance onto the private sector weakens this critical protection.

IV. The FBI Efforts to Compel Apple Threaten Free Expression and Human Rights

The FBI's actions in this case also pose a threat to free expression and global human rights. The legal precedent the FBI seeks to establish in this case would ensure that the government is able to demand access to virtually any electronic communication or piece of data, regardless of the device or software that an individual uses. Opening all electronic communication to the possibility of government scrutiny, or making such communication more easily subject to private hacking, could have a chilling effect on free speech, dissuading the public, journalists, or activists from engaging in protected speech. In the past, we have seen how the fear of outside scrutiny, whether by government or otherwise, has made it more difficult for prominent journalists to communicate with sources, leading to self-censoring and hindering reporting on critical issues, especially those related to national security where government secrecy and the potential for the abuse of civil liberties are at their highest.[8]

Indeed, U.S. foreign policy has also long supported efforts to ensure anonymous and secure communication, as a way of promoting free expression, human rights, and an open internet around the world. As part of this policy, the U.S. government has supported projects that provide secure communications to journalists and human rights activists who are often targeted by repressive regimes.[9] For example, the U.S. government has helped to create tools that provide end-to-end encryption, which provide greater security to users.[10] The FBI's attempts in this case are contrary to this policy, and open the door to repressive regimes demanding that American companies take the same burdensome actions to provide access to their citizens' devices in order

---

[8] *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN AMERICA (Nov. 12, 2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; ACLU & Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law, and American Democracy* 22–48 (2014), https://www.aclu.org/sites/default/files/assets/dem14-withlibertytomonitorall-07282014.pdf; Jesse Holcomb & Amy Mitchell, *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior*, PEW RESEARCH CTR. (Feb. 5, 2015), http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/.

[9] *See, e.g.*, *About the Program*, OPEN TECH. FUND, https://www.opentechfund.org/about (noting creation of the Open Technology Fund ("OTF") with U.S. government funding, and OTF's goal of securing access to the Internet with "encryption tools").

[10] WhatsApp is adopting encryption mechanisms developed by Open Whisper Systems, which is funded by the Open Technology Fund. See *Projects*, OPEN TECH. FUND, https://www.opentechfund.org/projects; *Open Whisper Systems Partners with WhatsApp to Provide End-to-End Encryption*, OPEN WHISPER SYSTEMS BLOG (Nov. 18, 2014), https://whispersystems.org/blog/whatsapp/; see also White House, National Security Strategy 21 (Feb. 2015), http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf ("The United States is countering this trend by providing direct support for civil society and by advocating rollback of laws and regulations that undermine citizens' rights. We are also supporting technologies that expand access to information, enable freedom of expression, and connect civil society groups in this fight around the world.").

to target dissenters, suppress free expression, or commit other human rights violations

V. The FBI Efforts to Compel Apple Would Harm Cybersecurity

The FBI's efforts to compel Apple to undermine the security of its product will erode consumer confidence and put customers at risk. Forcing Apple to use its software update capability to undermine the security of one of its devices will make consumers wary of software updates, resulting in decreased cybersecurity. In recent years, there have been enormous strides in pushing software updates to consumers. In many cases, these updates help to patch or repair vulnerabilities in consumers' devices that leave them vulnerable to hackers. The viability of this software update apparatus depends, in part, on consumers having confidence that these updates are genuine, and not malicious code in disguise. Should consumers fear that these are not legitimate updates verified by companies, they may simply stop downloading them. In an age when data breaches and identity theft are increasingly common, such a shift in consumer behavior would have disastrous results for cybersecurity.

Moreover, simply by creating this software, Apple is putting its customers at risk. Should anyone be able to replicate or steal such software, it could leave all iPhones vulnerable. Such a risk is not theoretical – prominent technology companies are routinely targeted by malicious actors. In 2009, Google and Microsoft's law enforcement surveillance teams were compromised by Chinese hackers who gained access to a sensitive database with years' worth of information about the U.S. government's surveillance targets.[11] In 2014, Microsoft's surveillance team was compromised again, this time by the Syrian Electronic Army.[12] In 2012, a backdoor that was inserted into JuniperOS software in 2008 was compromised, opening customers' network traffic to an unknown adversary.[13] This is, in part, why Apple's recent move toward strong device encryption is so critical – it ensures that consumers' information is secure even if Apple's own security systems are compromised.

At a time when cybersecurity threats are at the top of our national security agenda, the government should be encouraging companies to enhance security, not calling on companies to take actions that undermine the security and privacy of their users. Thus, we urge the committee to press the FBI to abandon these misguided efforts and instead invest in policies that encourage the adoption of strong encryption and other digital security technologies.

If you have any questions, please feel free to contact Legislative Counsel Neema Singh Guliani at 202-675-2322 or nguliani@aclu.org.

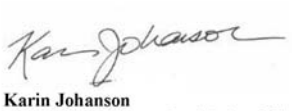
Sincerely,

---

[11] Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, WASH. POST, May 20, 2013, http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

[12] Tom Warren, *Microsoft Confirms Syrian Electronic Army Hacked into Employee Email Accounts*, THE VERGE, Jan. 15, 2014 http://www.theverge.com/2014/1/15/5312798/microsoft-email-accounts-hacked-syrian-electronic-army.

[13] Dr. Matthew D. Green, Assistant Professor, Dept. of Computer Science, Johns Hopkins Univ., Keynote Address: "On Subverting Trust," at the Network and Distributed System Security Symposium (Feb. 22, 2016).



Karin Johanson
Director, Washington Legislative Office

Neema Singh Guliani
Legislative Counsel

Mr. GOODLATTE. Director Comey, you've given us 3 hour—oh, I'm sorry. I'm jumping the gun here.

The gentleman from California, Mr. Peters, is recognized for 5 minutes.

Mr. PETERS. Director Comey—I want to, first of all, thank you, Mr. Chairman. I want to thank you for being here. I wanted to just conclude by saying that I did hear very—did listen carefully to your opening statement. I thought it was very constructive. I think you appreciate the two objectives we have here, which is to both preserve privacy and to deal with San Bernardino. You've heard the comment: hard cases make bad law. They're still hard cases, and the problem we see in terrorism now is the onesies and the twosies. And the notion that we would have invulnerable communications, I think, is something that we should all be concerned about.

I hope that you and the panel to follow you will all be part of a constructive discussion to figure out a way to serve both objectives and that the lines won't be too hard drawn on either side so we can do that.

And I appreciate, Mr. Chairman, the chance to thank Director Comey for being here, and look forward to the next panel.

Mr. COMEY. Thank you.

Mr. PETERS. Yield back.

Mr. GOODLATTE. The Chair thanks the gentleman.

Director, you've donated 3 hours of your time to our efforts today, or more, I'm sure, in getting ready, so we thank you very much for your participation and for answering a multitude of questions. And we are looking for answers, so if you have more to add to the record later, we would welcome that as well. Thank you very much.

Mr. COMEY. Thank you, sir.

Mr. ISSA. Mr. Chairman, would you entertain a unanimous consent while we're changing panels?

Mr. GOODLATTE. I would.

Mr. ISSA. Then I would ask unanimous consent that a letter I received late yesterday from a constituent in the technology business concerning this case be placed in the record. This is Emily Hirsch.

Mr. GOODLATTE. Without objection, that will be made a part of the record.*

Mr. ISSA. Thank you.

Mr. GOODLATTE. We ask the witnesses on the second panel to please come forward and be seated.

And now that Mr. Sewell has been afforded similar attention to the attention previously accorded to Director Comey, I'd ask that the press move back so we can begin the second panel.

Ms. LOFGREN. Mr. Chairman, I would not assume it was not directed to Ms. Landau, this photography.

Mr. GOODLATTE. Thank you.

We welcome our distinguished witnesses for today's second panel. And if you would all please rise, I'll begin by swearing you in.

Do you and each of you swear that the testimony that you are about to give shall be the truth, the whole truth, and nothing but the truth, so help you God?

---

*__Note:__ The material referred to was not available at the time this hearing record was finalized and submitted for printing on August 5, 2016.

Thank you very much. Let the record reflect that all of the witnesses responded in the affirmative. And I will now introduce the witnesses.

Bruce Sewell is senior vice president and general counsel of Apple. Mr. Sewell serves on Apple's legal team and oversees all legal matters, including global security and privacy. Prior to joining Apple, Mr. Sewell was deputy general counsel and vice president of Intel Corporation. He received his bachelor's degree from the University of Lancaster, and a J.D. From George Washington University.

Dr. Susan Landau is professor of cybersecurity policy at Worcester Polytechnic Institute. Originally trained as a theoretical computer scientist, Dr. Landau is an expert in cryptographic applications. Within cybersecurity policy, her work focuses specifically on communications surveillance issues. Dr. Landau earned a bachelor's degree from Princeton University, a master's from Cornell University, and a Ph.D. From the Massachusetts Institute of Technology.

Our final witness, Mr. Cyrus Vance, Jr., is the district attorney of New York County. Mr. Vance is currently serving his second term as district attorney after being reelected in 2013. He also serves as co-chair of the New York State Permanent Commission on Sentencing. Previously, Mr. Vance worked in private practice and taught at Seattle University School of Law. He's a graduate of Yale University and the Georgetown University Law Center.

All of your written statements will be entered into the record in their entirety. And we ask that each of you summarize your testimony in 5 minutes or less. To help you stay within that time, there's a timing light on the table. When the light switches from green to yellow, you have 1 minute to conclude your testimony. When the light turns red, that's it; your time is up.

And we'll begin with you, Mr. Sewell. Welcome.

TESTIMONY OF BRUCE SEWELL, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, APPLE, INC.

Mr. SEWELL. Thank you very much, Mr. Chairman. Thank you Members of the Committee and Ranking Member.

Mr. GOODLATTE. Make sure that microphone is on and pulled close.

Mr. SEWELL. Thank you for that technology hint.

Thank you, Mr. Chairman. It's my pleasure to appear before you and the Committee today on behalf of Apple. We appreciate your invitation and the opportunity to be part of the discussion of this important issue, which centers on the civil liberties that are at the foundation of our country.

I want to repeat something that we've said since the beginning, that the victims and the families of the San Bernardino attacks have our deepest sympathies. We strongly agree that justice should be served. And Apple has no sympathy for terrorists.

We have the utmost respect for law enforcement and share their goal of creating a safer world. We have a team of dedicated professionals that are on call 24 hours a day, 7 days a week, 365 days a year, to assist law enforcement.

When the FBI came to us in the immediate aftermath of the San Bernardino attacks, we gave them all the information we had related to their investigation. And we went beyond that by making Apple engineers available to advise the FBI on a number of investigative alternatives, but now we find ourselves at the center of a very extraordinary circumstance.

The FBI has asked the court to order us to give them something that we don't have, to create an operating system that does not exist. The reason it doesn't exist is because it would be too dangerous. They are asking for a backdoor into the iPhone: specifically, to build a software tool that can break the encryption system which protects personal information on every iPhone.

As we have told them and as we have told the American public, building that software tool would not affect just one iPhone. It would weaken the security for all of them. In fact, just last week, Director Comey agreed, and I think we heard the same here today, that the FBI would likely use this as precedent for other cases involving other phones. We've heard from District Attorney Vance, who's also said that he absolutely plans to use this tool on over 175 phones that he has in his possession. We can all agree this is not about access to one iPhone.

The FBI is asking Apple to weaken the security of our products. Hackers and cybercriminals could use this to wreak havoc on our privacy and personal safety. It would set a dangerous precedent for government intrusion into the privacy and safety of its citizens.

Hundreds of millions of law-abiding citizens trust Apple's products with the most intimate details of their daily lives: photos, private conversations, health data, financial accounts, and information about a user's location, and the location of that user's family and friends.

Some of you may have an iPhone in your pocket right now. And if you think about it, there's probably more information stored on that device than a thief could steal by breaking into your house. The only way we know to protect that data is through strong encryption.

Every day, over a trillion transactions occur safely over the Internet as the result of encrypted communications. These range from online banking and credit card transactions to the exchange of healthcare records, ideas that will change the world for the better, and communications between loved ones.

The U.S. Government has spent tens of millions of dollars through the Open Technology Fund and other U.S. Government programs to fund strong encryption. The Review Group on Intelligence and Communications Technology, convened by President Obama, urged the U.S. Government to fully support and not in any way subvert, weaken, or make vulnerable generally available commercial software.

Encryption is a good thing. We need it to keep people safe. We have been using it in our products for over a decade. As attacks on our customers' data become more sophisticated, the tools we need to use to defend against them need to get stronger too. Weakening encryption would only hurt consumers and well-meaning users who rely on companies like Apple to protect their personal information.

Today's hearing is entitled "Balancing America's Security and Privacy." We believe we can and we must have both. Protecting our data with encryption and other methods preserves our privacy and keeps people safe.

The American people deserve an honest conversation around the important questions stemming from the FBI's current demand. Do we want to put a limit on the technology that protects our data and, therefore, our privacy and safety in the face of increasingly sophisticated cyber attacks? Should the FBI be allowed to stop Apple or any company from offering the American people the safest and most secure products it can make? Should the FBI have the right to compel a company to produce a product it doesn't already make to the FBI's exact specifications and for the FBI's use?

We believe that each of these questions deserves a healthy discussion, and any decision should only be made after a thoughtful and honest consideration of the facts. Most importantly, the decision should be made by you and your colleagues as Representatives of the people rather than through warrant requests based on a 220-year-old statute. As Judge Orenstein concluded yesterday, granting the FBI's request would thoroughly undermine fundamental principles of the Constitution.

At Apple, we are ready to have this conversation. The feedback and support we're hearing indicate to us that the American people are too. We feel strongly that our customers, their families, their friends, and their neighbors will be better protected from thieves and terrorists if we can offer the best protections for their data; at the same time, our freedoms and liberties we all cherish will be more secure.

Thank you for your time, and I look forward to your questions.

[The prepared statement of Mr. Sewell follows:]

Statement for the Record

"The Encryption Tightrope: Balancing Americans' Security and Privacy"

United States House of Representatives

Committee on the Judiciary

Bruce Sewell

Senior Vice President and General Counsel

Apple

March 1, 2016

Thank you, Mr. Chairman. It's my pleasure to appear before you and the Committee today on behalf of Apple. We appreciate your invitation and the opportunity to be part of the discussion on this important issue which centers on the civil liberties at the foundation of our country.

I want to repeat something we have said since the beginning — that the victims and families of the San Bernardino attacks have our deepest sympathies and we strongly agree that justice should be served. Apple has no sympathy for terrorists.

We have the utmost respect for law enforcement and share their goal of creating a safer world. We have a team of dedicated professionals that are on call 24 hours a day, seven days a week, 365 days a year to assist law enforcement. When the FBI came to us in the immediate aftermath of the San Bernardino attacks, we gave all the information we had related to their investigation. And we went beyond that by making Apple engineers available to advise them on a number of additional investigative options.

But we now find ourselves at the center of an extraordinary circumstance. The FBI has asked a Court to order us to give them something we don't have. To create an operating system that does not exist — because it would be too dangerous. They are asking for a backdoor into the iPhone — specifically to build a software tool that can break the encryption system which protects personal information on every iPhone.

As we have told them — and as we have told the American public — building that software tool would not affect just one iPhone. It would weaken the security for all of them. In fact, just last week Director Comey agreed that the FBI would likely use this precedent in other cases involving other phones. District Attorney Vance has also said he

would absolutely plan to use this on over 175 phones. We can all agree this is not about access to just one iPhone.

The FBI is asking Apple to weaken the security of our products. Hackers and cyber criminals could use this to wreak havoc on our privacy and personal safety. It would set a dangerous precedent for government intrusion on the privacy and safety of its citizens.

Hundreds of millions of law-abiding people trust Apple's products with the most intimate details of their daily lives – photos, private conversations, health data, financial accounts, and information about the user's location as well as the location of their friends and families. Some of you might have an iPhone in your pocket right now, and if you think about it, there's probably more information stored on that iPhone than a thief could steal by breaking into your house. The only way we know to protect that data is through strong encryption.

Every day, over a trillion transactions occur safely over the Internet as a result of encrypted communications. These range from online banking and credit card transactions to the exchange of healthcare records, ideas that will change the world for the better, and communications between loved ones. The US government has spent tens of millions of dollars through the Open Technology Fund and other US government programs to fund strong encryption. The Review Group on Intelligence and Communications Technology, convened by President Obama, urged the US government to fully support and not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software.

Encryption is a good thing, a necessary thing. We have been using it in our products for over a decade. As attacks on our customers' data become increasingly sophisticated, the tools we use to defend against them must get stronger too. Weakening encryption will only hurt consumers and other well-meaning users who rely on companies like Apple to protect their personal information.

Today's hearing is titled Balancing Americans' Security and Privacy. We believe we can, and we must, have both. Protecting our data with encryption and other methods preserves our privacy and it keeps people safe.

The American people deserve an honest conversation around the important questions stemming from the FBI's current demand:

Do we want to put a limit on the technology that protects our data, and therefore our privacy and our safety, in the face of increasingly sophisticated cyber attacks? Should the FBI be allowed to stop Apple, or any company, from offering the American people the safest and most secure product it can make?

Should the FBI have the right to compel a company to produce a product it doesn't already make, to the FBI's exact specifications and for the FBI's use?

We believe that each of these questions deserves a healthy discussion, and any decision should be made after a thoughtful and honest consideration of the facts.

Most importantly, the decisions should be made by you and your colleagues as representatives of the people, rather than through a warrant request based on a 220 year-old-statute.

At Apple, we are ready to have this conversation. The feedback and support we're hearing indicate to us that the American people are ready, too.

We feel strongly that our customers, their families, their friends and their neighbors will be better protected from thieves and terrorists if we can offer the very best protections for their data. And at the same time, the freedoms and liberties we all cherish will be more secure.

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

Mr. GOODLATTE. Thank you, Mr. Sewell.
Ms. Landau, welcome.

TESTIMONY OF SUSAN LANDAU, Ph.D., PROFESSOR OF CYBERSECURITY POLICY, WORCESTER

Ms. LANDAU. Thank you. Mr. Chairman and Members of the Committee, thank you very much for the opportunity to testify today.

The FBI has pitched this battle as one of security versus privacy, but as a number of the Members have already observed, it's really about security versus security. We have a national security threat going on, and we haven't solved the problem at all. What have smartphones got to do with it? Absolutely everything. Smartphones hold our photos and music, our notes and calendars, much of that information sensitive, especially the photos.

Smartphones are increasingly wallets, and they give us access to all sorts of accounts, bank accounts, Dropbox, and so on. Many people store proprietary business information on their smartphones—their personal smartphones—even though they know they shouldn't.

Now, NSA will tell you that stealing login credentials is the most effective way into a system. In fact, Rob Joyce of the Tailored Access Operation said so in a public talk a month ago.

Here's where smartphones are extremely important. They are poised to become authenticators to a wide variety of systems—services. In fact, they're already being used that way, including at some high-placed government agencies.

Now, District Attorney Vance will tell you that law—has said that large scale data breaches have nothing to do with smartphone encryption, but that's not true. Look at today's New York Times, where there's a story about the attack on the Ukrainian power grid. How did it start? It started by the theft of login credentials of system operators. We've got to solve the login authentication problem, and smartphones are actually our best way forward to do it, but not if it's easy to get into the data of the smartphones.

Now, the Committee has already observed that there are many phones that will go through the process of being unlocked, not just the one in San Bernardino. And what that means for Apple is that it's going to have to develop a routine to do so.

Now, what happens when you have—when you sign a piece of code to update a phone and you're signing a piece of code that's an operating system or firm where you do it once—you do it occasionally. It's a whole ritual, and there are very senior people involved. But if you're dealing with phones that are daily being updated in order to solve law enforcement cases, then what happens is you develop a routine. You get a Web page, you get a low level employee to supervise it, and then it becomes a process that's easy to subvert. I have lots of respect for Apple's security, but not when it becomes a routine process to build an update for a phone. And what will happen is organized crime or a nation-state will do so using an update to then hack into a phone, maybe the phone of the Secretary or the chief of the Federal Reserve, maybe a phone of an HVAC employee who's going to go service a powerplant. What

we're going to do is decrease our security. That's the security risk that's coming from the requests.

Now, I get that law enforcement wants data protection that allows them access under legal authorization, but an NSA colleague once remarked to me that, while his agency had the right to break into certain systems, no one ever guaranteed that that right would be easy to do so.

The problem is when you build a way in for someone who isn't the owner to get at the data, well, you've built a way in for somebody else to get in as well.

Let me go to CALEA for a moment. CALEA is a security nightmare. I know that Congress didn't intend it that way, but that's what it is. If you ask the signals intelligence people, they will tell you: there are many ways for nefarious sorts to take advantage of the opening offered by law enforcement.

Instead of embracing the communications and device security we so badly need, law enforcement has been pressing to preserve 20th century investigative techniques; meanwhile, our enemies are using 21st century technologies against us.

The FBI needs to take a page from the NSA. You may recall that, in the late 1990's, the NSA was complaining it was going deaf from encrypted calls. Well, they've obviously improved their technology a great deal. According to Mike McConnell, from that time until now, NSA has had better SIGINT than any time in history.

What we need is law enforcement to develop 21st century capabilities for conducting electronic surveillance. Now, the FBI already has some excellent people and expertise, but FBI investment and capacity is not at the scale and level necessary. Rather than asking industry to weaken protections, law enforcement must instead development the capability for conducting sophisticated investigations themselves. Congress can help. The FBI needs an investigative center with agents with deep technical understanding of modern telecommunications technology and also, because all phones are computers, modern computer—deep expertise in computer science. There will need to be teams of researchers who understand various types of fielded devices. They'll need to know where technology is and where it will be in 6 months and where it will be in 2 to 5 years, communications technology in 2 to 5 years, so that they can develop the surveillance technologies themselves.

Expertise need not be in-house. The FBI could pursue a solution where they develop some of their own expertise and closely managed contractors to do some of the work, but however the Bureau pursues a solution, it must develop modern, state-of-the-art capabilities. It must do rather than trying to get industry to weaken security.

Your job is to help the FBI build such capabilities, determine the most efficient and effective way that such capabilities could be utilized by State and local law enforcement, for they don't have the resources to develop that themselves and to also fund that capabilities. That's the way forward that does not put our national security at risk. It enables law enforcement investigations while encouraging industry to do all it can do to develop better, more effective technologies for securing data and devices. That is a win-win and where we should be going. Thank you.

[The prepared statement of Ms. Landau follows:]

Testimony for
House Judiciary Committee Hearing on
"The Encryption Tightrope: Balancing Americans' Security and Privacy"
March 1, 2016

Susan Landau, PhD
Professor of Cybersecurity Policy
Worcester Polytechnic Institute
100 Institute Road
Worcester MA 01609

Testimony for

House Judiciary Committee Hearing on

"The Encryption Tightrope: Balancing Americans' Security and Privacy"

March 1, 2016

Mr. Chairman and Members of the Committee:

Thank you very much for the opportunity to testify today on "The Encryption Tightrope: Balancing Americans' Security and Privacy." My name is Susan Landau, and I am professor of cybersecurity policy at Worcester Polytechnic Institute. I have previously been a Senior Staff Privacy Analyst at Google and a Distinguished Engineer at Sun Microsystems. I am the author of two books on the issues of today's hearing: *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (MIT Press, 2011) and *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 1998); the latter is co-authored with Whitfield Diffie. I have written about these issues in the *Washington Post, the Chicago Tribune, Scientific American*, and other venues. I am a Fellow of the Association for Computing Machinery and of the American Association for the Advancement of Science, and I was recently inducted into the Cybersecurity Hall of Fame.[1]

My comments represent my own views and not those of the institutions with which I am affiliated.

Today I will speak on security threats, encryption, and securing smartphones.

It would seem to be a fairly straightforward issue: the smartphone of one of the two San Bernardino terrorists had its data encrypted. Because Apple designed the phone to be secure—and to destroy its data if there were ten incorrect tries of the PIN to unlock it—the FBI cannot unlock the smartphone (or at least cannot without risking destroying the data). The court has ordered Apple to create a phone update that

[1] Additional biographical information relevant to the subject matter to the hearing: I am also a Visiting Professor of Computer Science at University College London. For over two decades I have been studying encryption policy and the risks that occur when wiretapping capabilities are embedded in communications infrastructures. At Sun I was involved in issues related to cryptography and export control, security and privacy of federated identity management systems, and in developing our policy stance in digital rights management. I serve on the National Research Council Computer Science and Telecommunications Board, and recently participated in an Academies study on *Bulk Signals Intelligence Collection: Technical Alternatives* (2015). I have served on the advisory committee for the National Science Foundation's Directorate for Computer and Information Science and Engineering (2009-2012), the Commission on Cyber Security for the 44th Presidency (2009-2011), and the National Institute of Standards and Technology's Information Security and Privacy Advisory Board (2002-2008). I hold a PhD in applied math/theoretical computer science from MIT.

will undo this and other security aspects of the software, thus enabling the FBI to brute force the key to reveal whatever information is on the phone.

But little in cyber is straightforward. Despite appearances, this is not a simple story of national security versus privacy. It is, in fact, a security versus security story although there are, of course, aspects of privacy embedded in it as well.

The way we use our phones is very different than a decade ago; they are, as the Supreme Court observed in *Riley v. California,*[2] "minicomputers that also happen to have the capacity to be used as a telephone. [The phones] could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers'." Smartphones are already holders of account information (financial and otherwise), and are poised to become authenticators to a wide variety of services we access via the Internet.

And that is why we have a security versus security story. The Internet has brought huge benefits, but it has also vastly simplified attacks and exploits.[3] Cyberespionage netted Chinese military a "huge amount of design and electronics data on the F-35,"[4] Russian intrusions[5] into law firms[6] (the target here likely to be patent filings), an Iranian hacker probing US critical infrastructure (with possible intent to attack)[7] are examples. Each day brings more news of such attacks and exploits.

The cyberexploitation of US companies, in which attackers from overseas have reaped vast amounts of intellectual property, threatens the US economic strength. In the last decade, the United States has been under an unprecedented attack, one that NSA Director Keith Alexander has called "the greatest transfer of wealth in history."[8]

---

[2] 134 S. Ct. 2473 (2014).

[3] It might be hard to understand why a network on which society has become so dependent is so insecure. The short answer is history. The ARPANet, the precursor to the Internet, began as a research network on which everyone was a trusted partner. When the NSFnet, the follow-on network to the ARPANet, was opened up to commercial traffic, it relied on the same protocols. These assumed a trusted user body, which was not really sensible for a network that would support financial transactions, manage critical infrastructure, and the like.

[4] David Alexander, "Theft of F-35 design data is helping US adversaries—Pentagon," *Reuters*, June 19, 2013.

[5] Director of National Intelligence James Clapper views Russia as the top cyber threat. See, e.g., Siobhan Gorman, "Intel Chief: Russia Tops China as Cyber Threat," *Wall Street Journal*, October 17, 2014.

[6] Mandiant Consulting, "M-Trends 2016: Special Report," p. 45, https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

[7] Stephanie Gosk, Tom Winter, and Tracy Connor, "Iranian Hackers Claim Cyber Attack on US Dam," NBC News, December 23, 2015.

[8] Josh Rogin, "NSA Chief: Cybercrime constitutes 'greatest transfer of wealth in history'," *The Cable*, July 9, 2012.

Stealing your login credentials provides criminals and nation states the most effective way into your system—and a smartphone provides one of the best ways of securing ourselves.

That's why Apple's approach to securing phone data is so crucial.

But law enforcement continues to see electronic surveillance in twentieth century terms, and it is using twentieth-century investigative thinking in a twenty-first century world. Instead of celebrating steps industry takes to provide security to data and communications, the FBI fights it.

I should note that this response is different from NSA's, which over the last two decades, has, despite public perception, both encouraged and aided industry's efforts in securing communications.[9]

Instead of embracing the communications and device security we so badly need for securing US public and private data, law enforcement continues to press hard to undermine security in the misguided desire to preserve simple, but outdated, investigative techniques.

There is another way. Law enforcement should embrace the protections that industry is implementing to secure private—and, because of wide adoption, also government—sector data and develop substantive advanced capabilities to conduct investigations when needed. In the late 1990s, the NSA faced similar challenges and overcame them.[10]

We need twenty-first century technologies to secure the data that twenty-first century enemies—organized crime and nation-state attackers—seek to steal and exploit. Twentieth century approaches that provide law enforcement with the ability to investigate but also simplify exploitations and attacks are not in our national-security interest.[11] Instead of laws and regulations that weaken our protections, we should enable law enforcement to develop twenty-first century capabilities for conducting investigations.

Now I should note that the FBI already has some excellent capabilities in this area. But FBI investment and capacity in this area is not at the scale and level necessary to be as effective as it needs to be.

---

[9] This is true despite the fact that the NSA has also sought to undermine some protections; see later in this testimony as well as Susan Landau "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law and Policy*, Vol. 7, No. 3 (2014).

[10] See, e.g., Seymour Hersh, "The Intelligence Gap," *The New Yorker*, December 6, 1999.

[11] For a humorous take on these issues, see The Strip, New York Times, February 28, 2016, http://www.nytimes.com/slideshow/2012/07/08/opinion/sunday/the-strip.html#1

That's where Congress can help. Law enforcement must develop the capability for conducting such investigations themselves (or through a combination of in house and carefully managed contracting). Though there have been nascent steps in this direction by law enforcement, a much larger and complete effort is needed. Help the FBI build such capabilities, determine the most efficient and effective way that such capabilities can be utilized by state and local law enforcement, and fund it.

This is the way forward that does not put our national security at risk. It enables law enforcement investigations while encouraging industry to do all it can to develop better, more effective technologies for securing data and devices. This is a win/win, and where we should be going.

The rest of my testimony presents details of these concerns. Thank you very much for the opportunity to address you on this critical national-security topic.

Understanding our Security Threat

When terrorists wearing tactical gear and black masks and armed with guns and bombs attack a concert hall or Christmas party, our immediate emotional reaction is that we must move heaven and earth to prevent future such attacks. The role of leadership includes making choices. Here we are faced with a situation where logic and analysis lead to a different calculus on safety and security than do emotions. So while FBI Director James Comey has argued that, "We could not look the survivors in the eye if we did not follow this lead,"[12] this view is a mistaken view of where our most serious risks as a nation lie. Page one of the 2016 Department of Defense Threat Assessment states: "Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems."[13]

This is why securing communications and devices is so very crucial, and it is where the situation grows complicated. Despite our deeply human tendency to react to the attack that is occurring right now, we must focus and analyze to determine what our most dangerous threats are. This can be difficult. Yet measured, carefully considered responses will be what secures this nation and its people.

In the last decade, the United States has been under an unprecedented attack. . In 2010, Department of Defense Deputy Under Secretary William Lynn said the theft of US intellectual property "may be the most significant cyberthreat that the United

---

[12] Lawfareblog, February 21, 2016, https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead.

[13] James Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," February 9, 2016, p. 1.

States will face over the long term."[14] The cyberexploitation of US companies, in which attackers from overseas have reaped vast amounts of intellectual property, threatens the US economic strength. Make no mistake about it: this is an extremely serious national-security threat.

Protecting US intellectual property is critical for US economic and national security. In a July 2015 *Washington Post* op-ed, former NSA Director Mike McConnell, former DHS Secretary Michael Chertoff, and former Deputy Defense Secretary William Lynn concurred, observing that,

> Strategically, the interests of U.S. businesses are essential to protecting U.S. national security interest ... If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential."[15]

Messers Chertoff, McConnell, and Lynn concluded that the security provided by encrypted communications was more important than the difficulties encryption present to law enforcement.

As the Court noted in *Riley,*[16] the smartphones in our pockets are computers. They are, in fact, the most common device for accessing the network. So the cybersecurity threat applies as much to smartphones as it does to laptops, servers, and anything in between.

Securing Society

I'd like to turn now to encryption. I alluded earlier to NSA's efforts over the last two decades to secure private-sector telecommunications. Let me now present some detail.

Since the mid 1990s the NSA has actively been promoting the use of encryption in the private sector. This began with a 1995 incident in which NSA helped private-sector adoption of a new, more efficient cryptographic algorithm for securing low-powered, small devices.[17]

---

[14] William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, September/October 2010.

[15] Mike McConnell, Michael Chertoff, and William Lynn, "Why the fear over ubiquitous data encryption is overblown," *Washington Post*, July 28, 2015.

[16] 134 S. Ct. 2473 (2014).

[17] An NSA representative present at an ANSI standards meeting spoke up to note that a new public-key cryptographic algorithm, whose security had been sharply questioned by the current provider of such algorithms, was in fact, secure. He said that it was sufficiently secure that the US government was adopting it for communications among all U.S. government agencies, including the Federal

NSA participated in the Advanced Encryption Standards (AES) effort by vetting submitted proposals. This algorithm was chosen through an international effort run by the National Institute of Standards and Technology, and is an extremely strong system. In November 2001, two months after the attacks of September 11th, NSA concurred in the approval of AES as a Federal Information Processing Standard (FIPS). Designation as a FIPS means an algorithm or protocol must be in systems sold to the U.S. government or contractors; such a designation increases industry and international acceptance.

A year and a half later, the NSA approved the use of AES to protect classified information as long as it was in an NSA-certified implementation.[18] The decision had great impact, for it vastly increases the market for products running the algorithm, thus ensuring wider availability for non-classified users as well. From there the NSA went on to approve a set of publicly available algorithms for securing a network.[19]

Why would the NSA go to such great efforts to support the deployment of strong cryptography in the private sector? Since the mid 1990s the Department of Defense (DoD) has relied on Commercial Off the Shelf (COTS) products for DoD communications and computer equipment. Use of COTS is required by law, but it is also good security practice.[20] The speed of innovation by industry means that DoD must use COTS products in order to be cutting edge. iPhones and iPads have been cleared for DoD use since 2013.[21]

This is not to say every soldier must carry a locked iPhone, but rather, on balance, the US government has had much to gain from the security improvements of private-sector communications technologies. It is thus no surprise that the NSA supported many of these, including the widespread use of strong encryption technologies.

Reserve. The result was that the algorithm was approved, and is now widely used. It was the first time anyone could recall the NSA endorsing a private-sector system in this way. See Ann Hibner Koblitz, Neal Koblitz & Alfred Menezes, "Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift," Journal of Number Theory, Vol. 131 (2011), pp. 781-814.

[18] Committee on National Security Systems, National Security Agency, Policy No. 15, Fact Sheet No. Sheet No. 1, National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, 2003.

[19] Center for Secure Services, Information Assurance Directorate, National Security Agency, Suite B Algorithms, http://www.nsa.gov/ia/programs/suiteb_cryptography/ (accessed by searching the archived copy of an older version of the website, available at: http://archive.today/mFaN)

[20] The Clinger-Cohen Act requires that DoD purchases of information technology use COTS whenever possible. See, more generally, Susan Landau, "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law and Policy*, Vol. 7, No. 3 (2014).

[21] Defense Information Systems Agency, "DISA Approves STIG for Government-Issued Apple iOS 6 Mobile Devices," May 17, 2013, http://www.disa.mil/News/PressResources/2013/STIG-Apple

Are We "Going Dark"?

Our hearing concerns whether the wiretapping world is actually "going dark." And here the story does not appear to be quite the way the FBI sees it. For although the FBI has been expressing great concern since the early 1990s that encryption would prevent law enforcement from wiretapping,[22] the sky has apparently not fallen—at least for the NSA.

In the wake of the San Bernardino shootings, the *Washington Post* reported that,

> Mike McConnell, who headed the NSA in the 1990s during the first national debate over federal encryption policy, recalled how 20 years ago, he was for back-door access to encrypted communications for the government.
>
> "NSA argued publicly, 'We're going deaf'" because of encrypted calls, said McConnell, who now serves on the board of several cybersecurity companies. The agency wanted a third party to hold a key to unlock coded calls. But the resulting outcry — similar to the one heard in today's debate over smartphone and text message encryption — caused the government to back down.
>
> "We lost," McConnell said simply. And what happened? "From that time until now, NSA has had better 'sigint' than any time in history," he said.[23]

Nor is Director McConnell an outlier in this view. In the same article, former NSA Director Michael Hayden[24] was quoted as saying that, "this is far more of a law enforcement issue than it is intelligence."[25] Hayden noted, "I'm not saying that NSA should not try to bust what Apple thinks is unbreakable encryption. All I'm saying is Apple should not be required" [to hold keys to decrypt data for the government].[26]

Now it is not surprising that some of the ex-NSA directors might hold this opinion. The NSA has two roles: signals intelligence and information assurance. The NSA has grown more concerned about the latter as the theft of US IP has reached

---

[22] In 1992 the FBI's Advanced Telephony Unit warned that within three years Title III wiretaps would no longer work: at least 40% would be intelligible and in the worst case all might be rendered useless (Advanced Telephony Unit, Federal Bureau of Investigation, "Telecommunications Overview, slide on Encryption Equipment," 1992. FOAIed document available at https://www.cs.columbia.edu/~smb/Telecommunications Overview 1992.pdf).

[23] Ellen Nakashima, "Former national security officials urge government to embrace rise of encryption," *Washington Post*, December 15, 2015.

[24] Director Michael Hayden was, also, of course Director of the CIA.

[25] Nakashima, "Former national security officials urge government to embrace rise of encryption," Ibid.

[26] Ibid.

astronomical levels. The FBI continues to remain focused on investigations rather than prevention—a very serious mistake, in my opinion.

The other reason for the split, of course, is that the NSA has far more resources and capabilities for conducting signals intelligence than law enforcement has. But that is exactly the point. In a technological world in which virtually every crime has a cyber component, the FBI needs technical expertise; it needs vastly more technical expertise than it has at present.

The Role of Smartphones

Not so long ago everyone in an important job with confidential information carried a Blackberry. This was the communication device of choice for those in high positions in government and the corporate world. Unlike the recent iPhones and Androids, Research in Motion, the manufacturer of Blackberrys, enables the phone's owner (the corporation for whom the user works) to have access to the unencrypted text of communications. If Syed Farook had been carrying a Blackberry,[27] there wouldn't be a break-into-the-phone issue.

But in the last decade Blackberrys lost popularity, losing the market to iPhones and Androids (that's because apps drive the smartphone business). Most people don't like to carry two devices. So instead of a Blackberry *and* an iPhone or Android, consumers choose to use a single consumer device for *all* their communications—and it happens to be a personal one. (Of course, that's not true for everyone. I am sure that many on this committee do carry two devices, one for government work, one for their personal stuff. People who work in the Department of Defense, or for defense contractors, the financial or other industries where keeping proprietary work data secure is crucial, may carry two devices.)

As a society we have largely moved to a world of BYOD (Bring Your Own Device) to work. And what that means is not only is your personal stuff—your notes and calendars and contacts—on your smartphone, so is proprietary information from work. And so access to US intellectual property lies not only on corporate servers —

---

[27] If the FBI had not asked the San Bernardino Health Department to reset the password on the phone's iCloud account, there would not be a break-into-the-phone issue (Paresh Dave, "Apple and feds reveal San Bernardino's iCloud password was reset hours after the attack," *Los Angeles Times*, February 19, 2016). It is also the case that if the San Bernardino Health Department had installed "Mobile Device Management" on the phone it gave to Farook, there would not be a break-into-the-phone issue. (Tami Abdollah, "Apple CEO: Feds Should Withdraw Demand for iPhone Hack Help," ABC News, February 22, 2016, http://abcnews.go.com/Technology/wireStory/basic-software-held-key-shooters-iphone-unused-37106947)

which may or may not be well protected — but on millions of private communication devices.

Smartphones bear little relation to the simple rotary dial devices that once sat on hallway tables. Not only are smartphones the recipients of "our photos, our music, our notes, our calendars and contacts,"[28] much of it sensitive data (this is often especially true of photos). Our smartphones are used for conducting transactions of monetary value— ordering and paying for Uber rides and extra moves on Candy Crush, transferring balances between bank accounts, etc. People are also increasingly using their personal smartphones for business, and as a result, these smartphones store important proprietary information.

Smartphones are increasingly becoming wallets, providing access to accounts (not only financial, but also various online accounts, such as Dropbox), and storing emails and notes, including ones from meetings or design drawings and the like. For many people their personal smartphone acts as a convenient temporary repository for proprietary work information, information they know they ought to protect but rarely do as carefully as they ought. There are other ways of using phones for authentication; these rely on the device's security."

These smartphones are also used for authentication, that is, as a form of authentication to a device, an account, etc. And that means that the authentication information itself must be highly secured. Otherwise people in possession of the phone and with access to the data on it can break into other accounts. In short, smartphones are rapidly becoming a data repository of highly sensitive information, information that must be secured.

Thus Apple's secure by default provides an important improvement in security.

Smartphones and Long-Term Strategies for Security

Data theft through the Internet began three decades ago, starting with break-ins into military sites and the Defense Industrial Base.[29] As US companies began connecting their systems to the Internet, they, too, became targets. The scale of cyberexploition (data theft through networked systems) is what matters here. That scale is huge, and greatly worries General Alexander, Deputy Secretary Lynn, and many others in our government.

---

[28] Tim Cook, "A Message to Our Customers," February 16, 2016, https://www.apple.com/customer-letter/

[29] See, for example, Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace*, 1986-2012, CCSA Publication, 2013.

In the early days of the network, systems were poorly secured and data exfiltration was often the work of unsophisticated hackers. While aspects of that world still exist, the thieves are now far more sophisticated. Virtually every nation has its version of Cyber Command whose purpose includes spying via the network.

How do the spies get in? In a public presentation in January,[30] the Chief of NSA's Tailored Access Operations organization, Rob Joyce, observed that the most valuable data for attackers is your login credentials. Once an attacker has your login credentials—however briefly—he or she can establish a beachhead on your system that they can later use to exfiltrate data.

What has this got to do with securing phones? Everything. Using phones for secure login has the potential to rescue us from much of the mess created by the ease with which login credentials—typically passwords—are stolen. Currently our smartphones are our date books and our wallets, but they are well poised to become our authentication devices.

Smartphones already act as a "second factor" for authentication to accounts (e.g., Gmail); you log onto your email account with a password and an SMS to your phone provides a one-time PIN that you also type in. The security advantage is that someone needs two things to log into your account: your password and the SMS message.[31]

There are tremendous advantages to this approach. First, a smartphone is something you have, which makes it more secure than the "something you know" of a password. (The latter is easily used without your being aware that someone else has the authenticator—while you'd notice quickly that your phone is missing.) As Google explains, "It's an extra layer of security."[32] And a phone is something you already carry *all the time,* which means you're not carrying an extra device for authentication.

A Michigan start-up, Duo, provides two-factor authentication apps for companies that need fast, easy ways to ensure secure logins for their employees. Facebook is a good example. Its software engineers needed a *very secure* way to log on their development servers to write and submit code. The login process had to be fast—

---

[30] USENIX ENIGMA, https://www.youtube.com/watch?v=bDJb8WOJYdA, January 28, 2016.

[31] In fact, someone could intercept the SMS and, if they knew your password, log in instead of you. That would be a relatively highly targeted attack, meaning that Gmail's two-factor authentication system substantially improves on the more frequently used single factor of a password. There are other alternatives, including a "Security Key," that would be even stronger.

[32] Google, "Stronger Security for Your Google Account," https://www.google.com/landing/2step/#tab=how-it-protects.

and simple; programmers have little patience and will find workarounds if a process is complicated.[33]

There were various potential solutions: time-based tokens, one-time passwords, biometrics, smart cards and public keys. Each had serious problems,[34] and Facebook instead chose the Duo phone-based authentication solution for its developers.

Smartphones are used for security in other ways as well. Some of you have experienced Google's notification system that informs you about logins to your email account that are outside your normal behavior. The "Duo authentication feed" takes this security effort to a new level; it allows you to authenticate a transaction—for example, a login to an account—through a notification on your phone. You can respond while continuing your normal phone activity. This is security with convenience, meaning it is usable and effective security.

New technology means that smartphones are beginning to be used in even more creative ways to provide better security for authentication. This solves the problem that Rob Joyce says is his (and presumably other nations') most valuable way to gain access to your system.

Google is experimenting with a project where you log on by responding to a notification from a smartphone.[35] The holder of the smartphone gets the notification, responds, and then logs on to their account.

The private sector is not the only place using these approaches. Some high-placed agencies within the government are also adopting such solutions (and no, no details are available). Where security matters, authenticating through the device that is always in your pocket and owned by you is a much more secure way to handle your login credentials than the systems we've been using up until now.

If the information on the phone is accessible to Apple, it will be accessible to others—and this promising and important solution to protecting login credentials (which is, by NSA's description the most valuable way to break into systems)—will be ineffective. That's why locking down the data is so crucial for security. Rather than providing us with better security, the FBI's efforts will torpedo it.

---

[33] If only for this reason alone, security must be built in so that trusted but careless programmers don't make it easy to breach a system.

[34] Time-based tokens timed out when a developer was authenticating to two machines at once; one-time passwords had synchronization problems; biometrics are not trustworthy if the user is remote; and the smart card solution had interception problems. See: Facebook's Security Philosophy, and How Duo Helps, https://duo.com/assets/ebooks/Duo-Security-Facebook-Security-Philosophy.pdf

[35] Sarah Perez, "Google Begins Experimenting with Password-Free Logins," February 22, 2015, http://techcrunch.com/2015/12/22/google-begins-testing-password-free-logins/

Securing the Smartphones Does Not Prevent Investigations

Even though Apple has engineered excellent security for the iPhone, there are workarounds to access the encrypted data that do not involve Apple creating an update that circumvents its security protections.

If a locked iPhone is brought to a WiFi network it knows, then the phone will automatically sync its contents with Apple's iCloud if the phone is charging and the phone and iCloud passwords match. Unfortunately the San Bernardino Health Department changed the iCloud password on Farook's phone the evening of the attack, and so the mismatching passwords (the ones on the iPhone and iCloud account) eliminated this potential solution. Synchronization won't occur if the passwords for the phone and iCloud account differ. The iCloud password reset was done at the behest of the FBI, which was concerned that someone else might try to access or otherwise affect the phone's iCloud backup.[36]

But there are other solutions.

There are, of course, lots of sites that discuss jailbreaking the phone.[37]

The Chaos Computer Club is a well established group of European hackers that has, for over thirty years, exposed security flaws in well-known systems. Their technical expertise is well respected. They ran a meeting last summer in which they demonstrated physical means, including the use of electron microscopes, to recover the data on security chips. Such techniques may well enable the recovery of the data on the iPhone, and would come cheap (as in well under fifty thousand dollars).

The security in the iPhone stems from the DMA chip, a piece of hardware that can access main memory without going through the CPU. The iPhone DMA is using AES; what the FBI really wants is the key. There are firms that do forensic work in "decapping" chips to expose information on them. Rough estimate of costs are around half a million dollars. I've heard other estimates that come in much lower, say in the one hundred thousand dollar range.

The point is that solutions to accessing the data *already exist within the forensic analysis community.*

There's another way of addressing the issue about whether Apple is impeding an investigation. That's to look at what information might be only be on the phone,

---

[36] Paresh Dave, "Apple and feds reveal San Bernardino's iCloud password was reset hours after the attack," *Los Angeles Times*, February 19, 2016.

[37] Breaking into a locked iPhone would likely require technical skills at the level of a signals-intelligence agency.

keeping in mind that this phone was Farook's work phone and that he and Malik had destroyed their personal phones.

Let's start with might be only on the smartphone. There are likely to be text messages between Farook and his wife, there might be photos that Farook took of documents or people that might be of interest to the FBI, there might be communications between Farook and some of the Health Department employees he attacked.

Now I understand due diligence, and I especially understand due diligence in a terrorist attack that could conceivably have connections with other potential terrorists. But aside from self-professed statements in support of terrorist organizations, Farook and Malik do not appear to have been communicating with other terrorists. If they had been, the information about whom they are communicating with was available not only on their phones (personal or work), but also at the phone company and/or the ISP. (Farook might have been communicating via iMessage on his work phone. In that case, if the FBI made the request of Apple, they would have gotten iMessage metadata available from Apple servers.[38]) It is, however, extremely unlikely that Farook used his work phone rather than his personal one to conduct the private communications of interest.

Farook's communications with his coworkers are presumably available on their smartphones; one assumes these did not have passwords reset and their contents are accessible. It would thus appear that the only useful information that is potentially on Farook's smartphone is his communications with Malik.

In weighing the FBI request, one has to look at the potential gain and weigh it against the potential cost. In this case, the gain appears to be the possibility of developing a greater understanding of these self-radicalized terrorists.

The Security Risks Arising from Apple's Unlocking the Phone

Beginning with iOS 8, Apple iPhones encrypt by default, that is, all data on the smartphone is automatically encrypted unless the phone is unlocked. The key to unlock the phone data consists of an "entanglement" of the smartphone PIN and a hardware key physically embedded in the device. That means to get at the data, one has to have the phone. Apple's operating system protects the security of the data in other ways as well: with each incorrect guess of the phone PIN, the phone delays the

---

[38] The Manhattan DA report on smartphones notes that "iMessage detail (dates, times, phone numbers involved") does not appear at the phone company (Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, p. 12). That's correct. It is because an iMessage is an IP-based communication that goes through Apple servers.

time until the next guess is allowed. In addition, iOS may wipe the smartphone clean after too many incorrect tries. The system is designed to "protect user data if the device is lost or stolen, or if an unauthorized person attempts to use or modify it."[39]

Farook's work phone, an iPhone 5c, is an earlier device, but many of these protections are present on it as well. So at the FBI's request, the Central California District Court ordered Apple to create software that provides the FBI with:

> a Software Image File (SIF) that can be loaded onto [Farook's phone]. The SIF will load and run from Random Access Memory ("RAM") and will not modify the iOS on the actual phone, the user data partition or system partition on the device's flash memory. The SIF will be coded by Apple with a unique identifier of the phone so that the SIF would only load and execute on [Farook's phone]. The SIF will be loaded via Device Firmware Upgrade ("DFU") mode, recovery mode, or other applicable mode available to the FBI.[40]

The software is to:

> by-pass or disable the auto-erase function whether or not it has been enabled, ... enable the FBI to submit passcodes to [Farook's phone] via the physical device port,[41] ... and ensure that when the FBI submits passcodes to the [phone], software running on the device will not purposefully introduce any additional delay beyond what is incurred by Apple's hardware.[42]

In other words, the judge was asking Apple to create an Apple-signed device-specific software update tied to Farook's work phone.[43] The update would enable brute-force testing of PINs without erasing the content of the smartphone.

Let me briefly explain signing. Any complex digital device—a smartphone, a laptop, a thermostat, a car—will need software updates. Such updates are particularly important for patching newly discovered software vulnerabilities, but they have other functions as well. They provide new functionality (which means you don't need a new phone every six months). They also patch errors (all large software

---

[39] Apple Inc., *iOS Security: iOS 9.0 or Later*, September 2015, p. 4.

[40] United States District Court for the Central District of California, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant of a Black Lexus IS300 California License Plate 35KGD203, No ED15-0451M, Order Compelling Apple to Assist Agents in Search, February 16, 2016, p.2.

[41] This would vastly speed up the time to try different PINs.

[42] Order Compelling Apple to Assist Agents in Search, p.2.

[43] Signing is a cryptographic operation that validates the authenticity of a digital object; in this case, it is that the code came from Apple.

systems have errors). And they keep complex digital systems working as the other systems around them change as they themselves are updated and improved.

In order to assure your device that the smartphone software update is coming from Apple, the company "signs" the update, employing a cryptographic process using information only Apple has. This enables a smartphone (or laptop, thermostat, car, etc.) to know that the update is coming from a legitimate provider and prevents malicious actors from presenting so-called "updates" to your machine that are actually attempts to install malware.

The FBI has argued that there is no security risk in Apple building and signing a device-specific software update tied to Farook's work phone. The update will be fully under Apple's control and will be tailored to work only on the smartphone in question.

These statements are both true and incorrect at the same time. That is, the FBI statements that the update will be under Apple's control and can be tied to work only on Farook's phone are factually correct. But they miss the point of the risks involved.

The fact is that the software cannot be developed, used, and deleted. Given that the phone's data may be used in investigations and court cases, the "break-in" software must remain available for examination. The longevity of the update code constitutes the first risk for Apple's iPhone users.

While the FBI affidavit says this is a one-time use, other cases make that highly unlikely. A November 2015 report from the Manhattan District Attorney's Office states that, "Between September 17, 2014 and October 1, 2015, the District Attorney's Office was unable to execute approximately 111 search warrants for smartphones."[44] Were Apple to develop the code that the FBI is requesting, shortly afterwards the company would be inundated with requests from state and local law enforcement for the same capability.

The frequent use that the code may be expected to have gives rise to the risk that Apple CEO Tim Cook described in a recent Q&A with the Apple employees:

> Law enforcement agents around the country have already said they have hundreds of iPhones they want Apple to unlock if the FBI wins this case. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks. Of course Apple would do our best to protect that key, but in a world where all of our data is

---

[44] Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, November 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf p. 9. The 111 phones were all running iOS 8.

> under constant threat, *it would be relentlessly attacked by hackers and cybercriminals.*[45] (emphasis added)

At present each OS and firmware update is signed by Apple, enabling an Apple device to recognize the proffered update is approved by Apple and not We-Break-into-You.com. This signing key ensures the integrity of Apple updates, but it seems very likely that US law enforcement will frequently want to search locked iPhones. Each search will be targeted to a particular phone, which means Apple must update the code to include the serial number of the target. Each particularized version of the code will need to be signed by Apple. That's where the risk arises.

Signing code is not technically hard. But a process that happens relatively rarely (e.g., when signing updates to the OS or firmware occur) is very different from the process for an event that occurs routinely (e.g., signing updates to accommodate frequent law-enforcement requests for access to the smartphones). Everyday use of signing updates to unlock smartphones means the signing process must become routinized. Though that doesn't sound like much of an issue, it actually presents a serious problem.

I am concerned that routinizing the signing process will make it too easy to subvert Apple's process and download malware onto customers' devices. My concern is not that the FBI will download rogue software updates onto unsuspecting customers; there is a rigorous wiretap warrant process to prevent government wiretaps from being abused. Rather I am concerned that routinization will make it too easy for a sophisticated enemy, whether organized crime or a nation attempting an Advanced Persistent Threat attack, to mislead the Apple signing process.

A process that is used rarely—such is now the case in signing updates—is a process that can be carefully scrutinized each time it occurs; the chance for malfeasance is low. But make things routine, and instead of several senior people being involved in the signing process, a web form is used, and a low-level employee is placed in charge of code signing. Scrutiny diminishes. No one pays a great deal of attention, and it becomes easy for rogue requests to be slipped into the queue.

All it takes for things to go badly wrong is a bit of neglect in the process or the collaboration of a rogue employee. And if the FBI, CIA, and NSA can suffer from rogue employees, then certainly Apple can as well. A phone that an unfriendly government, a criminal organization, or a business competitor wants to examine receives a signed security update from Apple. This enables the government, criminal group, or competitor to probe the smartphone and read its data when the

---

[45] Matthew Panzarino, "In Employee Email, Apple CEO Tim Cook Calls for Commission on Interaction of Technology and Intelligence Gathering," Techcrunch, February 22, 2016, http://techcrunch.com/2016/02/22/in-employee-email-apple-ceo-tim-cook-calls-for-commission-on-interaction-of-technology-and-intelligence-gathering/

smartphone is taken during a customs inspection, a theft, or a meeting in which all electronic devices are kept outside the room.

A different issue is that smartphone owners may begin to distrust the automatic update process. One of the greatest improvements to consumer device security has been automatic security updates, what we in the trade call a "push" instead of a "pull." Would people stop automatic updates if they were concerned that law enforcement were using the updates as a surreptitious technique to search their devices, not for terrorist activity but, say, for tax fraud?

Using updates that appear to have been signed by the company to deliver malware or surveillance technologies is likely to undermine one of the few success stories of cybersecurity: automatic updates to correct flaws. How many people would stop automatic smartphone updates from Apple if they knew that the update could steal their bank account information? How many people would stop using virus scanners on their PCs if they knew that these programs were sometimes used by law enforcement to spy on their users? If this activity were to cause people to back away from using automatic updates for patching and the like, the impact on security is likely to be disastrous.

Cryptography—and security technologies in general—protect data. Within that obvious statement lies a conundrum for the FBI. It would appear, that in its effort to use all tools to conduct investigations, the FBI has not fully considered the impact of its efforts on technologies that secure data (the lifeblood of the information economy).

There are potentially severe adverse cybersecurity consequences of the FBI approach. Apple has been carefully working to secure the data on customers' phones. Most security experts consider iOS to be the most secure platform—the last things we should be doing is seeking to weaken it. Were the District Court decision to be upheld, it will seriously undermine industry efforts in security. I don't doubt that Apple will continue to further engineering work to further secure the data on the smartphones[46] (and other devices), but the government's actions would give serious pause to other companies pursuing that direction.

International Impact of Forcing Apple to Unlock its Secured Phones

There are also serious international consequences that would stem from Apple's developing code to unsecure its iPhone's operating system. As I'm sure members of the committee are aware, when members of the US government and businesspeople

[46] Matt Apuzzo and Katie Benner, "Security 'Arms Race' as Apple Is Said to Harden iPhone," *New York Times*, February 25, 2016.

travel to certain countries, they bring "loaner" devices with them—phones and laptops that are wiped clean before they leave the US and wiped clean on return.[47] That's the case even though the devices never have their network connections turned on, at least by the owner. Recommendations for security include such steps as removing batteries from a phone when at meetings (in order to prevent a microphone being turned on remotely)[48] and keeping the device with you at all times.[49]

Apple's efforts to secure the data on the iPhone should be viewed in this light.

There is another international aspect to the FBI's efforts to unsecure the phone. United States support of human rights is a cornerstone of US foreign policy. It includes strong support for private and secure communications, for such capabilities are a necessity for human rights workers in repressive nations.

There is no question that authoritarian governments in such countries as Russia and China will demand Apple deliver the same software that is it has been ordered to develop to handle Farook's work phone.[50] Apple's ability to resist such demands is made much more difficult if it has already created the code for US government use.

Securing the iPhone follows in US government tradition of developing secure communication and data storage solutions for private-sector use. The US Naval Research Laboratories developed Tor, The Onion Router, an Internet-based tool for obscuring communications metadata (thus hiding who is communicating with whom). At first glance, this might seem counterproductive; after all, criminals hide their tracks that way. But Tor is also remarkably useful for the military (obscuring that personnel in safe houses are communicating with US command), for law-enforcement investigators (obscuring that a participant in a child porn chat room is actually an investigator from fbi.gov), enabling human-rights workers and journalists working in repressive regimes a modicum of safety, etc. Tor functions most effectively in protecting users' identities if more users are on the system (and if not all users are government employees).

Another project, one that has resonances with the iPhone, is a US Department of State Bureau of Democracy, Human Rights, and Labor supported program that

---

[47] Nicole Perlroth, "Traveling Light in a Time of Digital Thievery," *New York Times*, February 20, 2012.

[48] Ibid.

[49] See, for example, North Dakota State University, "Cyber Security Tips for Traveling Abroad with Mobile Electronic Devices,"
https://www.ndsu.edu/its/security/traveling_abroad_with_electronic_devices/

[50] "And once developed for our government, it is only a matter of time before foreign governments demand the same tool." United States District Court for the Central District of California, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant of a Black Lexus IS300 California License Plate 35KGD203, No ED15-0451M, Order Compelling Apple to Assist Agents in Search, February 16, 2016, p.2.

developed an information management tool, Martus.[51] Martus enables a group to create a searchable, encrypted database (say of human rights violations), and *this database provides access only to members of the group that created the account.* [52]

Given the threats to US businesspeople traveling overseas, and the strong interest and support of the US government to secure communication and data storage tools for human-rights workers abroad, the FBI stance makes no sense. If the FBI succeeds in having Apple develop software to unlock the phone, the bureau will, in effect, have provided our enemies with tools to use against us. But this is not the first time that the law enforcement has mistaken difficulties in conducting investigations with technology that must be changed to accommodate its needs. That approach mistakes where actual solutions should lie.

We Have Been Down this Route Before — and It is Dangerous

Five years ago I testified to a House Judiciary Subcommittee, the Subcommittee on Crime, Terrorism, and Homeland Security. At the time, FBI General Counsel Valerie Caproni expressed grave concern that due to encryption being used for communications (as opposed to for devices), the FBI was "going dark." At the time, the FBI sought to extend the *Communications Assistance for Law Enforcement Act* (CALEA) to Internet, or IP-based, communications.

Now CALEA is a very problematic law. Wiretapping is a way for an unauthorized third party to listen in to a communication. By requiring that wiretapping capabilities be built into telephone switches, the government created a security breach. Indeed there are many ways for nefarious sorts to take advantage of the opening afforded by law enforcement.

The story of the ten-month wiretapping of the cellphones of one hundred senior members of the Greek government including the Prime Minister, the heads of the ministries of national defense, foreign affairs, and justice is well known.[53] Less well known is the fact that an IBM researcher found multiple security problems in a Cisco architecture for the equivalent type of switch for wiretapping IP-based communications.[54] *But much more disturbing than either of these stories is the fact that when the NSA tested CALEA-compliant switches that had been submitted prior to*

---

[51] The Department of State supported deployment and training, particularly in Uganda and Zambia where LGBTQ activists use Martus for contact lists, testimonies, and similar information.

[52] "Martus 4.5: Strong Security, Easy Configuration, Enhanced Usability," https://benetech.org/2014/06/17/martus-4-5-strong-security-easy-configuration-enhanced-usability/ . Benetech does not hold the keys and could not decrypt the data if requested to.

[53] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, Vol. 44, No. 7 (July 2007), pp. 26-33.

[54] Tom Cross, "Exploiting Lawful Intercept to Wiretap the Internet," Black Hat DC 2010.

use in DoD systems, NSA found security problems in every single switch submitted for testing.[55]

CALEA did not apply to "information services," but in 2010, the FBI proposed that the law be extended to IP-based communications. As the world, knows, the Internet is remarkably insecure. Building wiretapping capabilities into switches and routers is a move that would make things substantively worse. And it is unnecessary, for there are other solutions that would provide law enforcement with the capabilities it needs without introducing new security flaws.

Many Internet communications, such as those using Google or Facebook services, are available to the companies in the clear. Thus, these communications services, while not falling precisely under the CALEA umbrella, remain easy for law enforcement to access (as indeed they have under court order).

Instead of requiring by law that communications systems be built "wiretap capable," it is possible to take advantage of the vulnerabilities of any large software system—and these include phones and computers—to install a remote wiretap.[56] Called "lawful hacking" because it is legal (done under a court order) and "hacking" because it involves hacking into the devices, is a method that has been successfully adopted by the FBI. In fact, it is an approach that has been used by the Bureau since at least 2001.[57]

The idea is simple—and relied on by attackers all the time. Using a wiretap warrant to probe a suspect's smartphone—or other communications device you wish to wiretap—and find a vulnerability on the device. Unfortunately such vulnerabilities are easy to find. Then law enforcement will need a second wiretap warrant to install the actual wiretap; the wiretap is installed by taking advantage of the vulnerability to download onto the device.[58]

Now this is an ugly sounding business, and indeed, civil libertarians have expressed concern about a wiretap solution that involves breaking into peoples' devices. But the fact is that if law enforcement is to continue to wiretap, it can do so either by

---

[55] Private communication with Richard George, Former Technical Director for Information Assurance, National Security Agency (Dec. 1, 2011).

[56] See Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Going Bright: Wiretapping without Weakening Communications Infrastructure," *IEEE Security and Privacy*, Vol. 11, No. 1, January/February 2013, pp. 62-72 and also Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property*, Vol. 12, Issue 1, (2014).

[57] In the 2001 case, the FBI used software dubbed "Magic Lantern" to inject a virus into a remote computer and obtain the device's encryption keys. See B. Sullivan, "FBI Software Cracks Encryption Wall," NBC News, 20 Nov. 2001; www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall.

[58] This is the process by which criminals and other attackers download malware to extract data (of course, they do so without wiretap warrants).

taking advantage of vulnerabilities already present in the system to wiretap or by requiring all systems be made vulnerable (the CALEA solution). *Either you encourage security solutions that protect everyone by taking advantage of the security problems that already exist in the system, or you push everyone into less secure systems.* The former strengthens society's security while still enabling investigations; the latter only serves to weaken us badly.

A lawful hacking approach to wiretap investigations means that law enforcement must work a little harder.[59] Wiretapping investigations must be individually designed for each target (sometimes the same solution may work against more than one target). This is expensive, but that is not necessarily a bad thing; it means that we are not encouraging widespread wiretapping. I know that this is a value the Judiciary Committee holds dear.

The lawful hacking approach to wiretapping provides a roadmap for the locked smartphone situation.

Solutions for Locked Phones: FBI Investigatory Capabilities for the Twenty-first Century

Wiretap and search are extremely important tools for law enforcement, but encryption and locking down devices are extremely important security solutions for our data-driven, data-dependent society. But instead of embracing such technologies as an important and crucial security advance, law enforcement has largely seen such technologies as an impediment to lawfully authorized searches. This is a twentieth-century approach to a twenty-first century problem—but in that fact lies the possibility of a solution.

In the late 1990s, the NSA faced a similar crisis. Seymour Hersh detailed the situation in the *New Yorker*,

> The NSA, whose Cold War research into code breaking and electronic eavesdropping spurred the American computer revolution, has become a victim of the high-tech world it helped to create. Senior military and civilian bureaucrats ... have failed to prepare fully for today's high-volume flow of E-mail and fibre-optic transmissions—even as nations throughout Europe, Asia, and the Third World have begun exchanging diplomatic and national-security messages encrypted in unbreakable digital code ...[60]

---

[59] An NSA colleague once remarked to me that his agency had the right to break into certain systems, but no one ever guaranteed the right that it would be easy to do so.

[60] Seymour Hersh, "The Intelligence Gap," *The New Yorker*, December 6, 1999.

As we all know, the NSA adapted.

The FBI is where the NSA was in 1999, and it has been there for quite some time (certainly since well before CALEA's passage).

Given the types of adversaries the US faces, and the skills they have, we should be strengthening and securing all forms of cyber, including those in consumer hands. That's exactly what Apple has done. We should be praising Apple for this direction, and at the same time, we should help law enforcement to adopt a twenty-first century approach.

The Bureau has some expertise in this direction, but it will need more, much more, both in numbers, but also in the depth.

The FBI will need an investigative center with agents with a deep technical understanding of modern telecommunications technologies; this means from the physical layer to the virtual one, and all the pieces in between. Since all phones are computers these days, this center will need to have the same level of deep expertise in computer science. In addition, there will need to be teams of researchers who understand various types of fielded devices. This will include not only where technology is and will be in six months, but where it may be in two to five years. This center will need to conduct research as to what new surveillance technologies will need to be developed as a result of the directions of new technologies. I am talking deep expertise here and strong capabilities, not light.

This expertise need not be in house. The FBI could pursue a solution in which they develop some of their own expertise and closely manage contractors to do some of the work. But however the Bureau pursues a solution, it must develop modern, state-of-the-art capabilities for surveillance.

Such capabilities will not come cheap, but the cost annually will be in the hundreds of millions, not in the billions. But given the alternatives—insecure communications technologies that preserve law-enforcement's ability to search and wiretap at the cost of enabling others to do so as well—the cost is something we not only can afford, but must.

Developing such capabilities will involve deep change for the Bureau, which remains agent based, not technology based. But just as the NSA had to change in the late 1990s, so must the FBI. In fact, that change is long overdue. As many in law enforcement have said, many if not most crimes now have a cyber component. The FBI must develop advanced capabilities for such investigations, moving to a technology based investigation agency. It is not there now.

Because of the complexity involved, state and local law enforcement will not be able to develop their own solutions for some, or perhaps many, cases. They will need to rely on outsiders, either contractors or an effort put together by the FBI.

It is neither the time nor place to exactly map out the full solution of how such a law-enforcement advanced technologies surveillance center will work. That will take the expertise of law enforcement, technical leaders, and Congress to study and determine. But I place this before you not only as a solution to the conundrum that Director Comey and District Attorney Vance present you, but as *the only solution that protects our security and enables law enforcement to do its job in the face of advanced communications technologies.*

What we as a nation, and you as lawmakers, need to do is enable the Bureau to develop that expertise and, also, to simultaneously determine the best way to develop structures to enable state and local law enforcement to take advantage of that expertise.

Encryption and other protections (such as time delays as incorrect PINs are entered) secure our systems, and should never be undermined. Instead, the FBI must learn to investigate smarter; you, Congress, can provide it with the resources and guidance to help it do so. Bring FBI investigative capabilities into the twenty-first century. That's what is needed here—and not undermining the best security that any consumer device has to date. For that's what Apple's iOS is.

Summing Up

Privacy is a deeply held human value; it is what enables us to laugh, to love, to tell embarrassing stories about ourselves, to take risks and expose ourselves, and to be deeply human. But while I care very deeply about privacy, I think that the business of securing communications and devices is ultimately a security versus security story, not a security versus privacy story.

We have become highly dependent on our devices for conducting all parts of our lives, and this will only expand in the future. But instead of going forward, for a moment I want to look back, quite far back. I want to end by noting what the preamble to the Constitution says,

> We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence [sic], promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

Note that important phrase: "ensure the blessing of Liberty to ourselves and our Posterity." In the wake of the terrorist attacks in San Bernardino, it is easy to make a decision that argues in favor of short-term security by enabling this week's

investigation. It is much harder to make the decision that provides for long-term safety. But the preamble tells us to do so.

We have the option to press companies to develop as secure and private devices as they can, or to press them to go the other way. Let us make the right decision, for our safety, long-term security, and humanity.

Thank you.

Mr. GOODLATTE. Thank you, Ms. Landau.
Mr. Vance, welcome.

TESTIMONY OF CYRUS R. VANCE, JR., DISTRICT ATTORNEY, NEW YORK COUNTY

Mr. VANCE. Thank you. Good afternoon, Chairman Goodlatte, Ranking Member Conyers, and Members of the House Judiciary Committee. Thank you so much for allowing me to participate today. I'm testifying as a district attorney but on behalf of the National District Attorneys Association. And I'm very grateful for you giving us the opportunity to be here, because much of the discussion in the prior panel and in the comments by the other speakers here has been about the Federal Government and about the issue of security and cybercrime in the Federal context. But it's important, I think, for all of us to recognize that State and local law enforcement agencies handle 95 percent of the criminal cases each year around the country. So we have a very deep interest in the subject matter of this hearing today, and thank you for letting us participate.

Apple and Google's decision to engineer their mobile devices to, in essence, be warrant-proof has had a real effect on the traditional balance of public safety versus privacy under our Fourth Amendment jurisprudence. And I agree with the comments. I think of everyone here, including the many Members of the House, that we really need Congress to help solve this problem for us, and it's why it's so important that you're undertaking this effort. But I think in looking at this issue, there are some basic facts from the State law perspective that really are very important in this debate but are not in dispute.

And, number one, as Tim Cook said in his open letter to his customers of Apple of February 16 of this year: Smartphones, led by iPhone, have become an essential part of our lives. Nothing could be more true. We are all using our cell phones for every aspect of our lives.

Number two, is that smartphones are also essential to criminals. Our office investigates and prosecutes a huge variety of cases, from homicide to sex crimes, from international financial crime, and including terrorism cases, and criminals in each of those cases use smartphones to share information, to plan and to commit crimes, whether it's through text messages, photographs, or videos.

Number three, criminals know that the iOS 8 operating system is warrant-proof. Criminals understand that this new operating system provides them with the cloak of secrecy, and they are, ladies and gentlemen, quite literally laughing at us. And they are astounded that they have a means of communication totally secure from government reach. And I don't ask you to take my word for it. In one lawfully recorded phone conversation from Rikers Island in New York, an inmate, talking about the iOS 8 default device encryption, called it, and I'm quoting, "a gift from God."

Number four, the encryption Apple provided on its mobile devices prior to iOS 8, that is before October 2014, was represented to be both secure for its customers and, importantly, was amenable to court-authorized searches. We know this because Apple told us this. Apple characterized its iOS 7 operating system as the ulti-

mate in privacy. It touted its proven encryption methods and assured its users that iOS 7 could be used with confidence in any personal or corporate environment. During the time when iOS 7 was the operating system, Apple also acknowledged, and I think importantly, its responsibility to help, again in Apple's own words, "police investigating robberies and other crimes, searching for missing children, trying to locate a patient with Alzheimer's disease, or hoping to prevent a suicide." So Apple's experience, I believe, with iOS 7 demonstrated that strong encryption and compliance with court orders are not mutually exclusive.

A default device encryption has had a profound impact on my office and others like it. In November of 2015, my office published a white paper on public safety and encryption, and at that time, there were 111 iPhones from which we were locked out, having obtained search warrants for those devices. Now, 2½ months later, when we submitted our written testimony for this Committee, the number was 175. Today, it is 205, which represents more than one out of four of the approximately 700 Apple devices that have been analyzed by our office's own cyber lab since the introduction of iOS 8.

And, of course, that problem isn't just in Manhattan. Prosecutors in Houston have been locked out of more than 100 iPhones last year, 46 in Connecticut, 36 in Chicago since January, and those are just a few of the thousands of phones taken into evidence each year around the country.

So centuries of jurisprudence that have been talked about today have held that no item, not a home, a file cabinet, a safe, or even a smartphone, is beyond the reach of a court-ordered search warrant. But the warrant-proof encryption today gives two very large companies, we believe, functional control over the path to justice for victims of crime, including who could be prosecuted and, importantly, who may be exonerated.

So our point, Mr. Chairman, is that we believe this line being drawn between public safety and privacy is extremely important. It's affecting our lives. It's affecting our constituents' lives. And we believe that you should be drawing it, and we ask you to address this problem quickly. Time is not a luxury for State and local law enforcement, crime victims, or communities can afford. Our laws require speedy trials. Criminals have to be held accountable. And victims are, as we speak and we know in this audience, asking for justice.

[The prepared statement of Mr. Vance follows:]

Written Testimony of New York County District Attorney Cyrus R. Vance, Jr.
Before the United States House of Representatives
Committee on the Judiciary

"The Encryption Tightrope: Balancing Americans' Security and Privacy"

Washington, D.C.
March 1, 2016

Good afternoon Chairman Goodlatte, Ranking Member Conyers, and Members of the House Judiciary Committee. Thank you for your attention to this issue, and for the opportunity to testify today. This Committee had invited the National District Attorney's Association to participate in today's hearing, and my colleagues at the NDAA, in turn, asked me to serve as the organization's representative. I am grateful for this opportunity to speak with you on a topic of such importance and urgency to state and local law enforcement.

In recent weeks, the encryption debate has focused on the federal government's investigation into the heinous terrorist acts committed in San Bernardino, California on December 2, 2015. I applaud our federal colleagues for their commitment to justice for the 14 people killed, the 21 people injured, and all of their families. Law enforcement agencies at all levels, as well as crime victims' advocates and other concerned community leaders, are watching this case with great interest.

While the San Bernardino case is a federal case, it is important to recognize that 95 percent of all criminal prosecutions in this country are handled at the state and local level, and that Apple's switch to default device encryption in the fall of 2014 severely harms many of these prosecutions.

And that is why I am here today as a representative of the thousands of local and state prosecutors around the country: Smartphone encryption has real-life consequences for public safety, for crime victims and their families, and for your constituents and mine. In the absence of a uniform policy, our nation will effectively delegate the crafting of national security and law enforcement policy to boardrooms in Silicon Valley. That is, important responsibilities of our government will be carried out by Apple, Google,[1] and other technology companies, who will advance the best interests of their shareholders, not necessarily the best interests of our nation.

For the reasons set forth below, the line between personal privacy and public safety should be drawn by Congress, not Silicon Valley.

I. Smartphone Encryption's Impact on Law Enforcement and Crime Victims[2]

The United States Constitution provides that local law enforcement agents may obtain access to places where criminals hide evidence – including their homes, car trunks,

---

[1] Google, through its parent company Alphabet, has also announced that it will require default full disk encryption on its Android devices. As Apple has been the public leader among technology companies in the question of default full disk encryption, I shall focus on it in these remarks, even though many of the points may be applicable to Google and other technology companies.

[2] For background information on smartphone device encryption, *see* Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety (Nov. 2015), http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf. *See also* Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the U.S. Senate Judiciary Committee (July 8, 2015), http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf; and

storage facilities, computers, and digital networks – so long as the agents have a search warrant issued by a judge. Carved into the bedrock of the Fourth Amendment is a balance between the privacy rights of individuals and the public safety rights of their communities.

iPhones are now the first consumer products in American history that are beyond the reach of Fourth Amendment warrants. Like everyone else, I value my privacy. And I understand there is a fear arising out of mass security breaches, collection of bulk data, and warrantless surveillance. But that is not the access state and local law enforcement seek or expect. Police and prosecutors' access to electronic data is grounded in and limited by the Fourth Amendment, which (a) authorizes only "reasonable" searches, (b) based on probable cause, (c) supported by a particularized search warrant, and (d) approved by a neutral judge. I believe the high burden imposed by the Fourth Amendment – not warrant-proof encryption – is our best protection from abuse.[3]

Critics of law enforcement's position often point out that for centuries, we have successfully conducted investigations without evidence obtained from smartphones, and therefore, we should be able to continue to investigate crime without such evidence. But Apple itself explained why accessing evidence on smartphones is now so critical. In an open letter to customers dated February 16, 2016, Apple CEO Tim Cook stated that, "Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to

---

Response of Cyrus R. Vance, Jr. to the Berkman Center's Report, "Don't Panic: Making Progress in the 'Going Dark' Debate" (Feb. 5, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Letter_CyrusVance_Re_DontPanic.pdf.

[3] Apple itself states that "less than .00673% of customers have been affected by government information requests." http://www.apple.com/privacy/government-information-requests/.

our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going."[4]

This is precisely why default device encryption cripples even the most basic steps of a criminal investigation. In the past, criminals kept evidence of their crimes in safes, file cabinets, and closets. Today, criminals, like the rest of us, live their lives on smartphones and store evidence of their crimes on smartphones. And when you consider that Apple's iOS, together with Android, run 96.7 percent of smartphones worldwide, it should be clear why investigating a case without access to this evidence is doing so with one hand tied behind our backs.

Opponents of our position also ask why law enforcement agencies cannot simply rely on data stored in the cloud. First, not all data on devices are backed up to the cloud. Even data that can be backed up may not be because smartphone users are not required to set up a cloud account or back up to the cloud. Even minimally sophisticated users who use their phones to perpetrate crimes know to avoid backing up their data to the cloud. And even if a user chooses to use the cloud, data on a device will not be backed up unless the device is connected to Wi-Fi,[5] or for Android phones, a cellular connection. Additionally, although it may be possible to recover at least some deleted data from an Apple device, Apple states that once data has been deleted from an iCloud account, Apple cannot provide it in response to a search warrant.

---

[4] Tim Cook, "A Message to Our Customers" (Feb. 16, 2016), http://www.apple.com/customer-letter/.

[5] *See* Apple, "iOS Security: iOS 9.0 or later" (Sept., 2015), http://images.apple.com/business/docs/iOS_Security_Guide.pdf at p. 42.

Other opponents point to the availability of metadata, which often can be obtained through service of a search warrant on a telecommunications carrier. Metadata typically consists of (a) the time at which a call was placed or a message sent, (b) the phone number of the caller or message-sender, as well as the phone number of the recipient of the call or message, and (c) in the case of a phone call, the duration of the call. But metadata does *not* include the substance of a call or message. Thus metadata, while useful, is extremely limited. With it, I can show that two people spoke before a criminal incident, but I cannot show what they said, and that information, of course, will be critical for proving their intent and the scope of their agreement. For law enforcement to investigate, prosecute, and exonerate effectively, the most substantive evidence should be reviewed and utilized.

Likewise, iMessages – the default messaging platform between Apple devices – are transferred over Apple's servers rather than across telecommunications channels. Thus, telecommunications carriers are not privy to iMessages, their content, or their metadata. Additionally, Apple is not required by any regulation to retain that information. Indeed, Apple states that it does not retain the content of iMessages, and does not provide decrypted iMessage data in response to court orders.[6]

The real-world effect of all of this is that Apple's encryption policy frustrates the ability of law enforcement to prevent, investigate, and prosecute criminals, including the very hackers that Apple claims it wants to protect users against. It also impacts law enforcement's ability to exonerate those suspected of, but not responsible for crimes.

---

[6] *See* Apple, "iOS Security: iOS 9.0 or later" (Sept. 2015), http://images.apple.com/business/docs/iOS_Security_Guide.pdf, at p. 39: "Apple does not log messages or attachments, and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple cannot decrypt the data."

When Apple made the overnight switch to default device encryption in September 2014, my Office began tracking the number of cases in which we recovered iPhones that we could not unlock and that we reasonably believed contained data pertinent to the case that we were investigating. As of the November 2015 release of our Report on Smartphone Encryption and Public Safety, we were locked out of 111 Apple devices running iOS 8 or higher. That number is now 175 – comprising one quarter of the approximately 670 Apple devices received by our in-house Cyber Lab during that same period. As Apple users continue to migrate to the newer operating systems, the percentage of iOS devices that we are unable to access has increased significantly; in fact, in recent months, approximately one out of every two Apple devices collected by my Office's Cyber Lab is inaccessible. These numbers do not include Android devices or any devices that may have been processed by other district attorneys in New York City, or by the New York City Police Department.

The 175 Apple devices from which my Office is locked out represent investigations into the attempted murder of three individuals, the sexual abuse of a child, sex trafficking, child pornography, assault, robbery, identity theft, and all manner of other crimes. My colleagues from jurisdictions around the country have been running into the same road blocks in their efforts to investigate and prosecute serious crimes. For example, last year in Texas, Harris County District Attorney Devon Anderson's Office encountered more than 100 encrypted Apple devices from a variety of cases, including human trafficking, violent street crimes, and sexual assaults. In 2016, the problem continues with investigators unable to access eight to ten Apple devices every month. Similarly, in just the past two months in the Chicago area, Cook County State Attorney Anita Alvarez's Cyber Lab has received 30

encrypted devices that they are unable to access. The Connecticut Division of Scientific Services has encountered 46 encrypted Apple devices across a variety of criminal cases, including several matters involving child pornography.

As prosecutors, we have the extraordinarily difficult task of explaining to crime victims, or their surviving family members, that we have hit an investigative road block or dead end in their case, simply because Apple states that it will not comply with search warrants. In this debate among law enforcement leaders, intelligence officials, civil liberties proponents, and technology companies, one important voice has largely been left out – that of crime victims and their loved ones. Safe Horizon, the nation's leading victim assistance organization, recently explained how significantly encryption will hurt crime victims:

> It is important to note the devastating impact that smartphone encryption can have on victims of crime and abuse.... As a result [of default device encryption], perpetrators of child abuse and sexual assault are far less likely to be held accountable for these and other crimes. We recognize and respect a phone user's right to privacy. However, it is imperative that all evidence pertaining to criminal activity be available to law enforcement agencies with duly authorized search warrants. We owe no less to survivors of child abuse, human trafficking, domestic violence, and other violent crimes.[7]

II. Achieving a Balance Between Privacy and Security

My Office's Report — drafted in consultation with cryptologists, technologists, and law enforcement partners — proposed a solution that we believe is both technologically and politically feasible: *Keep the operating systems of smartphones encrypted, but still answerable to search warrants issued by neutral judges*. We do not want a backdoor for

---

[7] Safe Horizon, "Safe Horizon on Apple's Opposition to FBI Accessing Smartphones" (Feb. 18, 2016), http://www.safehorizon.org/page/in-the-news-125/news/safe-horizon-on-apples-opposition-to-fbi-accessing-smartphones-356.html.

the government to access users' information, and we do not want a key held by the government. We want Apple, Google, and other technology companies to maintain *their* ability to access data at rest on phones pursuant to a neutral judge's court order.

My Office has drafted, and provided to members of Congress, proposed federal legislation that requires designers of operating systems used on devices manufactured, leased, or sold in the United States to ensure that data on those devices, pursuant to a search warrant, are capable of being accessed in unencrypted form. Designers would not be responsible for decrypting, or ensuring the government's ability to decrypt, any data decrypted by a user, unless the encryption used was part of the operating system's design. This solution represents the reasonable, achievable, middle ground in this debate.

Throughout our history, the government has enacted statutory schemes to balance business concerns with law enforcement compliance, particularly when those businesses' products become an integral part of our lives. Those businesses recognize that they have a corporate responsibility to help protect victims from crime being perpetrated through the use of their products. One example is banks and financial institutions. As we learned more about how criminals were using banks to move money, Congress enacted statutes related to money laundering, fraud, and document preservation. Similarly, when it became clear that criminals were using phone lines to perpetrate crimes, Congress passed the Communications Assistance for Law Enforcement Act, requiring telephone companies to provide an access point for wiretaps.

Indeed, companies from every sector – finance, health care, transportation, energy, manufacturing, and telecommunications, to name a few – recognize and comply with the

obligation to respond to signed court orders arising out of criminal cases. For example, in 2014, Verizon received 287,559 United States law enforcement requests for data; they received 149,810 requests in the first half of 2015.[8] Facebook received 29,707 United States law enforcement requests for data in 2014; for the first half of 2015, they received 17,577 requests.[9] Now that smartphones have become as ubiquitous as landlines, it is time for Congress to enact legislation ensuring that law enforcement can access evidence of crime stored on smartphones with a judicial order.

Rather than accepting its corporate responsibility, Apple touted in its marketing of iOS 8 that "Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."[10] In refusing to assist law enforcement, Apple contends that doing so would leave their customers' information open to hackers, foreign dictatorships,[11] and other bad actors. Before I address that argument, I want to emphasize that there is probably no local law enforcement office in the country

---

[8] Verizon, "United States Report," https://www.verizon.com/about/portal/transparency-report/us-report/.

[9] Facebook, "United States Law Enforcement Requests for Data," https://govtrequests.facebook.com/country/United%20States/2015-H1/.

[10] This language was previously found at https://www.apple.com/privacy/government-information-requests/.

[11] Many in the technology industry claim that if the U.S. government seeks access to smartphone evidence, the government will "have little room to object" to requests from repressive regimes. *See* Open letter to Pres. Barack Obama (May 19, 2015), https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf. This assertion ignores the fact that local law enforcement in the U.S. seeks access to information only through a lawful judicial process. If a foreign nation's government, repressive or not, wanted information from an American company, it also would have to go through lawful processes in the U.S., either pursuant to a Mutual Legal Assistance Treaty (MLAT) or a letter rogatory. If the foreign government used the MLAT process, the executive branch of the federal government would decide whether, in its discretion, the foreign government's request was proper. If the foreign government used a letter rogatory, a federal court would make that determination. In either case, the request could be refused if the information was sought for use in a proceeding that would violate human rights.

that deals with more cybercrime and identity theft than mine, so of course we understand the importance of encryption. We want smartphone makers to offer the same strong encryption that Apple employed before iOS 8. Those previous mobile operating systems allowed data to be accessed on a seized device with a valid court order, and I am not aware of any documented security problems with those operating systems. Apple has never explained why its prior systems lacked security or were vulnerable to hackers and thus needed to be changed.

Indeed, Apple characterized its prior encryption as the ultimate in privacy. Apple's May 2012 guide to "iOS Security" – published before its switch to default device encryption – notes that "Apple is committed to incorporating proven encryption methods and creating modern mobile-centric privacy and security technologies to ensure that iOS devices can be used with confidence in any personal or corporate environment."[12] According to Apple, iOS 7 "provides solid protection against viruses, malware and other exploits that compromise the security of other platforms."

And yet, under iOS 7, Apple maintained the ability to help – in their own words – "police investigating robberies and other crimes, searching for missing children, trying to locate a patient with Alzheimer's disease, or hoping to prevent a suicide."[13] Apple itself has demonstrated that strong encryption and compliance with court orders are not incompatible.

---

[12] Apple, "iOS Security" (May 2012), https://web.archive.org/web/20121021133728/http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf.

[13] Apple, "Apple's Commitment to Customer Privacy" (June 16, 2013), http://www.apple.com/apples-commitment-to-customer-privacy/.

Furthermore, it is not entirely clear what cybersecurity problem Apple's new encryption is intended to solve. Individuals' phones were not being stolen *and* hacked into. Prior to iOS 8, to bypass the lock on a passcode-protected phone, Apple required both (i) possession of the phone[14] and (ii) its custom method to bypass the device encryption. We never held the key, we have never wanted to hold the key, and we have never heard about a key held by Apple being stolen. Even if a hacker were able to learn Apple's decryption process — which Apple guards closely — that hacker would also need to have the actual device to steal its data. Likewise, a thief who steals a person's locked smartphone would also need to know either the victim's passcode or Apple's highly guarded decryption process to obtain the device's data.

There has been much discussion and concern about large-scale, institutional data breaches involving Home Depot, Target, and other large companies. These breaches are deeply disturbing, of course, but they have nothing to do with the level of encryption on iPhones. These two issues – large-scale data breaches from servers, and smartphone encryption – should not be conflated. Apple's default device encryption would do nothing to protect against large-scale institutional data breaches or the use of malware.

Apple and other proponents of device encryption have portrayed the new policy as a response to the concerns raised by Edward Snowden about data collection by the National Security Agency. But, once again, data collection has nothing to do with smartphone encryption. Smartphone encryption would not have prevented the NSA's mass collection of phone-call data or the interception of telecommunications, as revealed by Mr. Snowden.

---

[14] Mr. Cook stated in his February 16, 2016 letter to customers that in the wrong hands, any software it creates for the government "would have the potential to unlock any iPhone in someone's *physical* possession." (Emphasis added.) http://www.apple.com/customer-letter/.

Likewise, Apple has not explained how any software it may create for purposes of responding to search warrants – software which Apple keeps in its sole possession – would fall into "the wrong hands." In its refusal to assist the government, Apple has not addressed the fact that it already can, and frequently does, bypass iPhone users' passcodes. For example, Apple has the ability to access an Apple device remotely, such as when it tracks the location of a device and erases its contents remotely ("Find My iPhone"), or when it sends iOS software updates to the customer's iPhone. Apple is able to do these things without knowing the particular device's passcode. But Apple has never contended that the existing means for tracking and wiping devices remotely or pushing software updates may be exploited by bad actors. Rather, Apple maintains that its customers' data is secure.

Furthermore, Apple allows corporate administrators and other employers, through mobile device management ("MDM") solutions, to access organization-owned and employee-owned devices remotely, and to modify the device's iOS software, settings, and data. According to Apple, "an MDM server can perform a wide variety of administrative commands, including changing configuration settings automatically without user interaction, locking or wiping a device remotely, or clearing the passcode lock so users can reset forgotten passwords."[15] Apple has never explained why MDMs – tools that Apple enables and promotes, and which allow third parties to access a user's iPhone without a passcode – do not compromise an iPhone user's security, while any software Apple develops in order to comply with a search warrant may fall into "the wrong hands."

I previously sought answers to a few of the questions raised in this testimony in letters sent to Apple and Google in April 2015. To date, I have not received a response

---

[15] *See* Apple, "iOS Deployment Overview for Enterprise," http://images.apple.com/business/docs/iOS_Enterprise_Deployment_Overview.pdf.

from either company. Those letters are annexed to my Office's Report on Smartphone Encryption and Public Safety.

III. Conclusion

Apple's influence can be felt in every corner of the globe. In its fiscal quarter ended December 26, 2015 alone, Apple reported record profits of $18.4 billion.[16] But Apple is not above the law,[17] and its bottom line is not more important than the safety of Americans.

In Mr. Cook's February 16, 2016 letter, he argues that the FBI's request for assistance in the San Bernardino case "threatens the security of our customers." Mr. Cook and his colleagues at Apple have effectively decided that they know better than our elected representatives and professionals in law enforcement how best to keep Americans safe. In the absence of laws that keep pace with technology, we have enabled Apple and other technology companies to upset the balance between privacy and public safety established by centuries of jurisprudence.

Technology companies should not be able to dictate who can access key evidence in criminal investigations. No device or company, no matter how popular, should be able to exempt itself from court obligations unilaterally. And they should not be able to write their own laws. I do not believe Americans would want to cede this vast authority to private enterprise. That authority should rest with the people's elected officials. I urge Congress to enact a national solution.

Thank you for the opportunity to participate in this critically important discussion.

---

[16] Apple, "Apple Reports Record First Quarter Results" (Jan. 26, 2016), http://www.apple.com/pr/library/2016/01/26Apple-Reports-Record-First-Quarter-Results.html.

[17] Notably, in testimony before the U.S. Senate Judiciary Committee in 2013, Mr. Cook told lawmakers: "We not only comply with the laws, but we comply with the spirit of the laws." https://www.apple.com/pr/pdf/timcookopeningstatement.pdf.

Mr. GOODLATTE. Thank you, Mr. Vance.

We'll now proceed with questioning of the witnesses under the 5-minute rule, and I'll begin by recognizing myself.

Mr. Sewell, Director Comey created a dichotomy between this being a technology problem or a business model problem, and said that Apple was addressing this as a business model problem. Is that a fair contrast, or is this something else?

Mr. SEWELL. It's by no means a fair contrast, Mr. Chairman. I've heard this raised before. It was raised in New York. It's been raised in San Bernardino, and every time I hear this, my blood boils.

This is not a marketing issue. That's a way of demeaning the other side of the argument. We don't put up billboards that talk about our security. We don't take out ads that market our encryption.

We're doing this because we think that protecting the security and the privacy of hundreds of millions of iPhone users is the right thing to do. That's the reason that we're doing this. And to say that it's a marketing ploy or that it's somehow about PR really, really diminishes what should be a very serious conversation involving this Congress, the stakeholders, the American people.

Just with respect to the New York case, Judge Orenstein last night took on this issue head-on, and he said, in footnote 14 on page 40, he said: I reject the government's claim. I find Apple's activities and the position that they are taking conscientious and not with respect to PR or marketing.

Mr. GOODLATTE. Director Comey and Mr. Vance seem to suggest that the security provided by encryption on prior devices is fine, but advancing encryption technology is a problem. What do you think about that?

Mr. SEWELL. So it's important to understand that we haven't started on a path of changing our technology. We haven't suddenly come to the notion that encryption security and privacy are important.

At Apple, this began back in 2009 with our encryption of FaceTime and iMessage. We've been on a path from generation to generation as the software and the hardware allow us to provide greater security and greater safety and privacy to our customers.

What happened between iOS 7 and iOS 8 was that we were able to transform the encryption algorithm that is used within the software and the hardware of the phone to provide a more secure solution.

Mr. GOODLATTE. We are moving to end-to-end encryption on many devices and apps, not just Apple iPhones. Why is that happening?

Mr. SEWELL. I think it's a combination of things. From our perspective at Apple, it's because we see ourselves as being in an arms race, in an arms race with criminals, cyberterrorists, hackers. We're trying to provide a safe and secure place for the users of our devices to be assured that their information cannot be accessed, cannot be hacked or stolen. So, from our perspective, end-to-end encryption move is an effort to improve the safety and security of our phones. From the terrorist's perspective, I think it's an effort to communicate in ways that cannot be detected, but the terrorists

are doing this independently of the issues that we're discussing here today.

Mr. GOODLATTE. Now, if the FBI succeeds in getting the order that is in dispute that Apple has appealed to a final resolution, however long that takes, and they then get Apple to develop this device that will allow the 10 times and your—by the way, all of us here, we can't turn that off, so——

Mr. SEWELL. Well, we could show you how to do that.

Mr. GOODLATTE. Well, but inside our firewall here, we can't do that. So we understand the reason, but that creates a separate vulnerability, does it not, for people whose device falls in someone else's hands, they could willfully try 10 times and erase what hasn't been backed up on the device.

But be that as it may, if they were to get you to develop that code and to apply it and then to crack the four-digit code to get into the device, once they get in there, they could find all kinds of other restrictions that Apple has no control over, right, with regard to apps that are on the phone, with regard to various other communications features that the consumer may have chosen to put on there? Is that correct?

Mr. SEWELL. That's absolutely right, Mr. Chairman. One of the most pernicious apps that we see in the terrorist space is something called Telegraph. Telegraph is an app that can reside on any phone. It has nothing to do with Apple. It can be loaded either over the Internet or it could be loaded outside of the country. And this is a method of providing absolutely uncrackable communications.

If what happens here is that Apple is forced to write a new operating system, to degrade the safety and security in phones belonging to tens or hundreds of millions of innocent people, it will weaken our safety and security, but it will not affect the terrorists in the least.

Mr. GOODLATTE. Thank you very much.

My time has expired.

The gentleman from Michigan, Mr. Conyers, is recognized for 5 minutes.

Mr. CONYERS. Thank you, Mr. Chairman.

And welcome to the witnesses.

Let me start off with Professor Landau. Director Comey has just testified that until the invention of the smartphone, there was no closet, no room, or basement in America that the FBI couldn't enter. Did encryption exist before the invention of the iPhone?

Ms. LANDAU. Encryption has existed—for centuries. And, in particular, there have been fights over encryption and the use of encryption in the 1970's about publication; in the 1980's about whether NIST or the NSA would control the development of encryption for nonnational security agencies; in the 1990's about whether there would be export controls on devices with strong encryption. The White House changed those rules in 2000.

We expected to see widespread use of strong encryption on devices and on applications, and the technologists' response to Apple is: What took you guys so long? How, in the face of all the cybersecurity problems that we've had, did it take industry so very long to do this?

Well, as our technical expert, let me ask you this: Is there any functional difference between asking Apple to break its own encryption, and what the FBI has demanded in California?

Ms. LANDAU. I'm sorry. Asking Apple to break—I don't quite understand the question.

Mr. CONYERS. All right.

Ms. LANDAU. What Apple is being asked to do is to subvert the security controls and go around. So it's not breaking the encryption, but it's subverting its own security controls.

Mr. CONYERS. Right.

Ms. LANDAU. And is there any functional difference between that and——

Mr. CONYERS. And what the FBI has demanded in California.

Ms. LANDAU. What it's demanded in California is that Apple subvert its own security controls.

Mr. CONYERS. Uh-huh. Let me ask Mr. Bruce Sewell the same question: What is the functional difference between ordering Apple to break its encryption, and ordering Apple to bypass its security so the FBI can break the encryption?

Mr. SEWELL. Thank you, Ranking Member.

Functionally, there is no difference. What we're talking about is an operating system in which the passcode is an inherent and integrated part of the encryption algorithm. If you can get access to the passcode, it will affect the decryption process itself.

What we're being asked to do in California is to develop a tool, a tool which does not exist at this time, that would facilitate and enable the FBI, in a very simple process, to obtain access to the passcode. That passcode is the cryptographic key. So essentially, we are throwing open the doors, and we are allowing the very act of decryption to take place.

Mr. CONYERS. I was hoping you'd go in that direction. Let me ask you this: There has been a suggestion that Apple is working against law enforcement, and that you no longer respond to legal process when investigators need your assistance. Is that accurate?

Mr. SEWELL. It's absolutely false. As I said in my opening statement, we care deeply about the same motivations that motivate law enforcement. The relationship with law enforcement falls within my shop at Apple. The people that we have who assist law enforcement every day are part of my team, and I'm incredibly proud of the work they do.

We have dedicated individuals who are available around the clock to participate instantly when we get a call. As we've discussed a little bit earlier in Director Comey's testimony——

Mr. CONYERS. I want to squeeze in one more question before my time runs out.

Mr. SEWELL. All right. I'll try to be very quick. We do everything we can to assist law enforcement, and we have a dedicated team of people who are available 24/7 to do that.

Mr. CONYERS. Why is Apple taking this stand? What exactly is at stake in the San Bernardino case?

Mr. SEWELL. This is not about the San Bernardino case. This is about the safety and security of every iPhone that is in use today.

And I'd like to address one thing that Director Comey raised. This is—there's no distinction between a 5C and a 6 in this con-

text. The tool that we're being asked to create will work on any iPhone that is in use today. It is extensible; it is common; the principles are the same. So the notion that this is somehow only about opening one lock or that there's some category of locks that can't be opened with the tool that they are asking us to create is a misnomer. It's something that we needed to clarify.

Mr. CONYERS. Thank you for your responses.

Mr. GOODLATTE. The Chair recognizes the gentleman from Wisconsin, Mr. Sensenbrenner, for 5 minutes.

Mr. SENSENBRENNER. Thank you very much.

Mr. Sewell, I think you know that I have been one of the privacy hawks on this Committee. And the whole debate over the USA FREEDOM Act was whether the NSA should go to court and get some type of an order or a warrant specifically naming the person or persons whose data is requested. And here, the FBI, you know, has done that.

Now, in your prepared testimony, you said the questions about encryption should be decided by Congress rather than through a warrant based on a 220-year-old statute. I point out that the Bill of Rights is about the same age. Now, the FBI's attempting to enforce a lawful court order. Apple has every right to challenge that order, as you have done. But why is Congress and not the courts the best venue to decide this issue?

Mr. SEWELL. Congressman, I think that, ultimately, Congress must decide this issue. So I'm completely in support of the position that you're articulating.

I think we find ourselves in an odd situation in a court in California, because the FBI chose to pursue, in an ex parte fashion, a warrant that would compel Apple to do something. We view that not as an extension of the debate, not as a way to resolve this issue; we view that as a way to cut off the debate. If the court were to grant the relief that the FBI is seeking, we would be forced to do the very thing which we think is at issue and should be decided by the American people. We'd be forced to create the tool.

Mr. SENSENBRENNER. Okay. Now, what's your proposed legislative response? Do you have a bill for us to consider?

Mr. SEWELL. I do not have a bill for you to consider.

Mr. SENSENBRENNER. Okay. Thank you. That answers that.

Now, the FBI has provided some fairly specific policy proposals to ensure that law enforcement can access encrypted data with a warrant. What policy proposal would Apple support? You don't like what the FBI said. What's your specific response?

Mr. SEWELL. What we're asking for, Congressman, is a debate on this. I don't have a proposal. I don't have a solution for it. But what I think we need to do is to give this an appropriate and fair hearing at this body, which exists to convene and deliberate and decide issues of legislative importance.

We think that the problem here is we need to get the right stakeholders in the room. This is not a security-versus-privacy issue. This is a security-versus-security issue, and that balance should be struck, we think, by the Congress.

Mr. SENSENBRENNER. Well, you know, let me make this observation, you know, having dealt with the fallout of the Snowden revelations and the drafting and garnering support of USA FREEDOM

Act. I can tell you, I don't think you're going to like what comes out of Congress.

Mr. SEWELL. Congress, we will follow the law that comes out of this process. We certainly understand.

Mr. SENSENBRENNER. Okay. Well, the thing is, I don't understand. You don't like what's being done with the lawfully-issued warrant. And most warrants are issued on an ex parte basis, where law enforcement submits an affidavit before a magistrate or a judge, and the judge determines whether the allegations of the affidavit are sufficient for the warrant to issue.

Now, you're operating in a vacuum. You've told us what you don't like. You said that Congress ought to debate and pass legislation. You haven't told us one thing about what you do like. What are we going to hear what you do like so that Apple has a positive solution to what you are complaining about? You said it's Congress' job to do it. Now, we won't shirk from that. This hearing, you know, is a part of this debate. The FBI has provided some policy suggestions on that. You haven't said what Apple will support. So all you've been doing is saying, no, no, no, no.

Now, our job in Congress, honestly, you know, as we did with the FREEDOM Act, and as we are doing with the Electronic Communications Privacy Act update, is to balance our belief that there should be privacy for people who are not guilty or suspected of terrorist activity, and that there should be judicial process, which there has been, in this case.

And, you know, I guess that while your position is because you don't have anything positive, you know, is to simply leave us to our own devices. Well, we'll be very happy to do that, but I can guarantee you, you aren't going to like the result.

I yield back.

Mr. SEWELL. Congressman, I do think we have said what we stand for and what we believe is the positive place.

Mr. SENSENBRENNER. No. You know, the thing is you've asked Congress to do something, and I asked you what Congress should do. You said we have nothing. Then I said the FBI has provided specific policy proposals to ensure law enforcement is able to get this information.

Now, here we're talking about the iPhone of a dead terrorist that was not owned by the terrorist, but was owned by San Bernardino County. Now, you know, the thing is is that I don't have a government iPhone. I have my own iPhone, which I use extensively. But the terrorist had, you know, a government iPhone which belonged to the government. I think the government, San Bernardino County specifically, would like to get to the bottom of this, and you're resisting it.

I said my peace.

Mr. GOODLATTE. Time of the gentleman has expired.

The gentleman from New York, Mr. Nadler, is recognized for 5 minutes.

Mr. NADLER. Thank you, Mr. Chairman.

Let me begin by welcoming my constituent and the great district attorney of New York County, Cy Vance, by saying that I appreciate his enlightenment of the district attorney's views of this dilemma that we all face.

Let me also suggest, in answer to Mr. Sensenbrenner's questions, that I assume that Apple may have legislative suggestions for us after the courts come out with their determinations, and Apple decides they like the determinations or they don't like the determinations, at which point Apple, and a lot of other people in institutions, I assume, will decide on specific legislative proposals. And it may very well be that this Congress will wait to see what the courts do, but we will see.

Let me begin my questions. District Attorney Vance, Director Comey suggested earlier today that the relief sought by the FBI is limited to this one device, running this particular operating software in this one case. Now, I gather that you've mentioned you have over 200 phones faced with a similar problem——

Mr. VANCE. Yes.

Mr. NADLER [continuing]. That you don't really think that this case will be limited to the one device; that, obviously, it's going to set a precedent, maybe not the only precedent, for a large class of devices, including the ones that you're interested in.

Mr. VANCE. There may well be an overlap between action in Federal court where the FBI is in litigation and in State court. I do believe that what we should be seeking, collectively, is not a phone-by-phone-by-phone solution to accessing devices and the contents when there's probable cause; we should be creating a framework in which there are standards that are required to—for a court to authorize access to a device and that it's not based upon litigation as to whether you can get into a West Coast phone or an East Coast phone.

Mr. NADLER. Well, I assume that, eventually, either the courts will set one standard, or Congress will have to consider it.

Mr. VANCE. Right. Yes.

Mr. NADLER. Professor Landau, several of your colleagues recently published the results of a survey of over—and this is similar to a question I asked Director Comey. Several of your colleagues recently published results of a survey of over 600 encryption products that are available online. More than 400 of these products are open sourced and made or owned by foreign entities.

If Congress would have passed a law, or for that matter, if the courts were to impose a requirement, that forcing U.S. companies to provide—forcing U.S. companies to provide law enforcement with access to encrypted systems, would that law stop bad actors from using encryption from open sources or foreign sources?

Ms. LANDAU. Absolutely not. Absolutely not. And what Apple's product does is it makes encryption easy by default. And so it means, as I said, the secretary to the Chair of the Federal Reserve, the HVAC employee, the chief of staff in your office—of course, your office should be protected anyway, but the regular person using a phone has the phone secured.

If Congress were to pass a law prohibiting use of encryption on Apple phones or however—you know, you wouldn't say it just for Apple, what it would do is it would weaken us, but not change it for the bad guys.

Mr. NADLER. And if someone purchased a phone from a foreign company, it could have the encryption that we prohibited an American company from creating?

Ms. LANDAU. That's—if someone purchased a foreign phone, somebody can just download the app from abroad. They don't have to buy a foreign phone. They can just download the app from anywhere.

Mr. NADLER. And let's assume that Congress decided to prohibit purchase of foreign encryption systems. Is there any practical way we can enforce that?

Ms. LANDAU. No. I mean, you would have to start inspecting so much as it comes over the Internet that it becomes an intrusive——

Mr. NADLER. So what you're saying is that we are really debating something that's undoable?

Ms. LANDAU. That's right. And we were there 20 years ago, which the open-source issue was part of the reason for the U.S. Government's change in export controls, which is part of what enabled——

Mr. NADLER. Okay. Let me ask two very quick questions before my time runs outs.

Mr. Sewell, the Eastern District Court yesterday, in its ruling that has been referred to, cited no limiting principle to the legal theory behind the FBI's request as a reason to deny the order. Is there a limiting principle in the San Bernardino case?

Mr. SEWELL. Absolutely none, Congressman.

Mr. NADLER. None. So it can be expanded indefinitely.

And finally, Mr. Sewell, your brief, Apple's brief to the court lays out several constitutional concerns. There's computer code speech as protected under the First Amendment. What are the First and Fifth Amendment—well, let me just ask, what are the First and Fifth Amendment questions does this case raise? We've been talking about statute, but let's ask about First and Fifth Amendment questions.

Mr. SEWELL. Right. Good question, Congressman. And bear in mind that what we're being asked to do is write a brand new computer code, write a new operating system. The law, with respect to the applicability of computer code to speech, I think, is well established. So this is a compelled speech by the government for the purpose of the government.

Mr. NADLER. Which is a First Amendment problem.

Mr. SEWELL. Which is absolutely a First Amendment problem. And bear in mind, this is a speech which Apple does not want to make. This is our position.

On the Fifth Amendment, the issue is conscription. The issue is forced activity, forced labor.

Mr. NADLER. Does anybody else on the panel want to comment on that question?

If not, thank you. My time is expired, Mr. Chairman.

Mr. GOODLATTE. The gentleman from California, Mr. Issa, is recognized for 5 minutes.

Mr. ISSA. Thank you, Mr. Chairman.

And I'll pick up where you left off on forced labor. Do you know of any place in our history in which, except in time of war, when things are commandeered and people are told to do that, or when police are in hot pursuit, do you know a time in which people were forced to apply their inventive genius against their will?

Mr. SEWELL. Congressman, I'm not aware of it. The steel cases during the war were the ones that were most applicable.

Mr. ISSA. Sure. And I certainly understand a different time and a different set of circumstances.

Now, I want to do two things: So Ms. Landau, I'm going to come to you first. Your expertise is encryption. You were probably very young, but you remember 20 years ago the argument. Wasn't it the FBI and then the late Mike Oxley and others that were championing that if we allowed more than 256-bit encryption, then the FBI couldn't easily decode it, and that would be the ruin of their investigations?

Ms. LANDAU. Right. And what you get instead is over the last 20 years, the NSA has increasingly supported the secure technologies for private sector communications infrastructure, including the 256-bit algorithm.

Mr. ISSA. Okay. I'm going to ask a quick question, and it's old technology, because I'm very good with analog world. But this happens to be a January 29, 2015, patent that's already in the record, and it's a patent on basically self-destructing the contents inside if someone tries to forcibly open it.

Now, the funny thing is, I was looking for the old patents going back decades and decades, because the military and others have used these. They've had acids and even more punitive, if you will, responses inside when we wanted to secure it. It's not a new technology, but there's a new twist on it.

Aren't we, in a sense, the equivalent of saying, well, you can make something that destroys the documents but then you have to tell us how to defeat it?

Ms. LANDAU. That's exactly right.

Mr. ISSA. Okay. And I'm looking and saying, there's no history in that, but we've had plain safes for a very, very long time. This isn't new. Do you know of any shredder company that has been told that they have to show you how to reassemble what they've shredded?

Ms. LANDAU. I don't study shredding companies, but I'd be very surprised if there were.

Mr. ISSA. Mr. Vance, have you ever ordered a shredding company to put the paper back together, use their inventive genius——

Mr. VANCE. Of course I haven't, Congressman, but—but——

Mr. ISSA. So you're asking, in this case, for somebody to create a product for your service. And I want to focus on that and I'll get to you, I promise.

But Mr. Sewell, I'm going to look at you as the representative of the one of the great technology companies in our country. Apple gets its great technology people, I assume, from Stanford and MIT and other great universities, right?

Mr. SEWELL. We do, yes, indeed.

Mr. ISSA. And you don't get all the graduates, right?

Mr. SEWELL. No, we don't. We wish we did.

Mr. ISSA. So when I was talking to the Director, and saying, well, if you take—and it's a hypothetical. My level of knowledge is way less than any of your folks, and probably any of the FBI's. But if you take this hard drive, solid-state hard drive, you pull it apart—and he even used the word "mirroring." Obviously, he had some

discussion at some point—and you make as many images as you want, then you have a true original; but even if the self-destruct occurs, that original, you throw it away you take another one.

So that part of what he's asking you to do, they can do themselves by pulling the chip out and having it imaged, if you will, in all likelihood. We're not saying for sure. But he hadn't checked it. So that's a possibility. Is that right?

Mr. SEWELL. I believe so. We don't know what the condition of the phone is and we don't know what the condition of the RAM is, but yes.

Mr. ISSA. Sure. And of course, we're not really talking about one phone. We know that. We're talking about thousands of phones.

And as I understand the technology used in your chip is you have burnable traces in your chip. So randomly, or in some way, when you're producing each chip, you burn traces which create the encryption algorithm, and it's internal. So the chip has its algorithm separate from the software.

But that chip, when interfacing with an image, if you keep giving it new images, that's the part that changes. So isn't it at least conceivable that as to that phone, and perhaps the 175 in New York and others, that the FBI, or the NSA could, in fact, come up with an elegant brute force attack that would work on your phones and also would work on hundreds of other types of phones around the world; and that that technology with, if you will, those brilliant young minds from Stanford, MIT, and Kent State, my alma mater, you know, could, in fact, produce something that would not be available to the public; they would have control over, and they would be able to make it more universal than just trying to go through your source code, which, I understand—is it correct—they've never asked for. Is that right?

Mr. SEWELL. We've never been asked for our source code.

Mr. ISSA. Okay. Mr. Chairman, if anyone else wants to opine on it, I would appreciate they be able to.

Mr. GOODLATTE. Chair thanks the gentleman and recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Well, thank you very much. I think this hearing is very helpful.

And just to get it on the record, Mr. Sewell, I mean, you're not objecting—let me step back. If you have something, and you are served with a warrant, you give that something up. Is that correct?

Mr. SEWELL. That's absolutely correct, yes, Congresswoman.

Ms. LOFGREN. So the issue here is you don't have it, you've got no way to get it, and, therefore, you can't give it, right?

Mr. SEWELL. That's correct.

Ms. LOFGREN. Now, if it were possible to do something that would get just this one thing without opening the door to everybody else's stuff, would you have a problem with that?

Mr. SEWELL. Let me——

Ms. LOFGREN. Let me rephrase that, because you're in court.

Mr. SEWELL. Sure.

Ms. LOFGREN. That would be a different issue than breaking encryption generally, wouldn't it be?

Mr. SEWELL. The best analogy that I can come up with, and I've been struggling with how do we create the right kind of analogy

for this situation. If Apple had a box somewhere that we could guarantee, we could assure 100 percent certainty, that anything that was put in that box was not susceptible to thievery, to attack, to corruption; if we had such a place in the world, we wouldn't be here today——

Ms. LOFGREN. Right.

Mr. SEWELL [continuing]. Because what we would have done is gone to our customers and we would have said, give us your passwords. We can absolutely 100 percent protect them. And then if you lose your phone, if you need our help, we can just give you the passcode.

Ms. LOFGREN. But you didn't do that because you can't guarantee that, which is why you encrypted this phone.

Mr. SEWELL. Exactly right. And now the bizarre situation is that essentially, the FBI is saying, We all realize it's silly that everybody would give you your password, but instead, we want you to build a tool that will get those passwords, and we're telling you, you can put that tool in this box that doesn't exist.

Ms. LOFGREN. So let me ask you this: Is it possible, theoretically, to create code that would preclude you from creating a system that would allow you to defeat the 10-try erase function?

Mr. SEWELL. We could write a program that would suppress that protective measure.

Ms. LOFGREN. So that you couldn't do what it is you're being asked to do?

Mr. SEWELL. Right. We're being asked to do three things, but it is capable—we are capable of doing those three things. The issue is what's the consequence of doing those?

Ms. LOFGREN. Right. But the question is also, I mean, this hearing caused me to go in and turn on the 10-erase function which I neglected to do before the hearing, thank you very much. But, you know, as you go forward, people are insecure about what's safe.

Mr. SEWELL. Absolutely.

Ms. LOFGREN. And, you know, for example, you don't have—and I think for good reason—what's in iCloud is not encrypted. Is it possible to encrypt the data in iCloud?

Mr. SEWELL. Yes, actually, in the iOS 8 and 9 generation, we have encrypted the iCloud data. It's encrypted in a different way than it was before and we think in a more secure way.

Ms. LOFGREN. Right. But you can still provide access to that?

Mr. SEWELL. It is encrypted in a different way——

Ms. LOFGREN. But you could change that if you wished?

Mr. SEWELL. Yes.

Ms. LOFGREN. Now, let me ask you this, Dr. Landau: Now, you were involved with that paper that was published, I think, last year.

Ms. LANDAU. Keys under Doormats.

Ms. LOFGREN. Thank you. That was an excellent paper. And I think for anybody who has—it's dense. I had to read some pages two and three times to understand it. But for anybody—and actu-

ally, I've asked unanimous consent, Mr. Chairman, to put that paper in the record from the cryptographers.**

Mr. GOODLATTE. Without objection, it will be made a part of the record.

Ms. LOFGREN. If you just go to the questions at the end, you see that this is a fool's errand. We'll never be able to do what is being asked of us by the FBI. It's a practical matter; it's just not achievable.

But I'm interested in your take on, you know, Director Comey said, you know, they don't want the master key. They just want this one bypass on security. Isn't that exactly the same?

Ms. LANDAU. It's wrong, and it's just, as Mr. Sewell said, once they've built that software, that software works for other phones. Of course, it has to have the serial number of the particular phone, so Apple has to sign—you know, has to take the software, put in a new serial number, sign it so the new phone accepts it. And that's where all the security risks comes in, because it becomes a routine process, and as I mentioned during my remarks, routine processes get subverted.

Ms. LOFGREN. I'll ask the final question. Mr. Sewell, it was asked earlier by my colleague, Mr. Richmond, about whether these other countries have better security than we do. If I take my phone, my iPhone with the current operating system to Russia or China, can they break into it?

Mr. SEWELL. With respect to the phone itself, we believe the encryption we provided in iOS 8 makes that effectively impossible. With respect to the things that are going on at the Internet level, there are very sophisticated techniques that can be used by malicious actors who have access to the Internet itself. There are ways to fool the Internet into thinking that something is what it isn't. And so I think there is a vulnerability still in that regard. But on the phone, what we've tried to do is to remove that possibility with iOS 8 and 9.

Ms. LOFGREN. Thank you very much, all of you, for your testimony.

Mr. GOODLATTE. The Chair thanks the gentlewoman and recognizes the gentleman from Texas, Mr. Poe, for 5 minutes.

Mr. POE. Thank the Chairman.

Thank you all for being here. Fascinating, important discussion on this issue of, as you say, security/insecurity.

As you know, I'm a former prosecutor and former judge, and dealt with warrants for 30 years, either requesting them or signing them. And this particular case, I think we're really talking about two cases now. We're talking not just about the San Bernardino case, but the New York case as well. Different facts, different issues.

Fourth Amendment, we have discussed—Fourth Amendment doesn't really apply too much to this situation, because the possession of the item is lawful in the possession of government. I do think it's ironic, however, we're talking about privacy, United States is supposed to lead on the issue, I think, on the issue of pri-

**Note: The material referred to is not printed in this hearing record but is on file with the Committee. Also, see Lofgren Submission at:

http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104573

vacy. We're the only one that has a Fourth Amendment. But we see that other countries seem to have more concern about privacy in their technology than maybe we do. I find that somewhat ironic.

Let me ask you a couple questions. You discuss the idea of constitutional right, right of privacy. But in one of your testimonies, and I think it was Mr. Nadler from New York, he and I have a language barrier problem, so I'm not sure I understood his question. You mentioned the First Amendment and the Fifth Amendment. Is that correct?

Mr. SEWELL. I did, that's correct.

Mr. POE. Briefly explain how you see this as a First Amendment issue as well as a Fifth Amendment issue. We don't need to talk about the Fourth Amendment. We've discussed that.

Mr. SEWELL. The Fifth Amendment issue derives from the fact that we're being asked to write code, and code is speech, and Supreme Court has held that that speech is protectable. So we're being asked to speak by the government. That speech is not speech that we want to make. And the First Amendment provides us with protections against being compelled to speak by the government. So that would be the First Amendment argument in a nutshell.

The Fifth Amendment provides us with protection from conscription, protection from being forced into labor at the government's will, except under the most extraordinary of circumstances, which I discussed with Congressman Issa. But that's the Fifth Amendment issue.

Mr. POE. All right. Thank you.

What this request, the results of the request, how would that affect Apple worldwide in other countries?

Mr. SEWELL. Well, there are a number of parts of that question, Congressman, so thank you. The way that this would affect Apple is that it would affect our customers. It would affect everyone who owns an iPhone, and it would create a risk for everyone who owns a phone that their data could be compromised, that their security could be compromised.

With respect to the international question, I agree with you. I think America should be leading on this issue. And I think that the world is watching what happens right now in our government and what happens, even today, with respect to this particular debate.

Our ability to maintain a consistent position around the world, our ability to say that we will not compromise the safety and security of any of our users anywhere in the world is substantially weakened if we are forced to make that compromise here in our own country. So I urge this Congress, and I urge the government generally to understand that to take a leadership role, give us the strong support that we need to resist any effort by other governments to weaken security and privacy.

Mr. POE. One of the questions that was asked was talking about what is your solution, and I actually agree with Mr. Nadler. I know this is going to bother him a little bit, that there may be, after all this litigation, and there may be a solution that we haven't thought of yet, but would not one option be Congress taking the position that prohibits the backdoor key security system, the Viper system, as I call it, from——

Mr. ISSA. Thank you, Mr. Poe.

Mr. POE. I said that earlier but you stepped out. The Viper system from being imposed, required, prohibit that from government requiring that type of system in specific technology like an iPhone?

Mr. SEWELL. I think that is certainly one possibility, yes, sir.

Mr. POE. Prohibit the key.

Let me ask you something else. If courts rule that you're required to develop the technology, develop the software, would that software be able to be used on all those other hundreds of phones that are out there that the government lawfully has in their possession but they can't get into?

Mr. SEWELL. Absolutely. There's nothing that would preclude it from being used on any iPhone that is in use today.

Mr. POE. And my last question, would other countries then, if U.S. takes the position thou shalt give government the key, what will other countries, like China, require or request or demand of Apple?

Mr. SEWELL. So to date, we have not had demands like that from any other country. The only place that we're having this debate is in our own country. But as I said before, I think if we are ordered to do this, it will be a hot minute before we get those requests from other places.

Mr. POE. All right. Thank you, Mr. Chairman. I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentleman from Georgia, Mr. Johnson, for 5 minutes.

Mr. JOHNSON. Thank you, and thank the witnesses for being here.

Mr. Vance, what's the difference between a company being ordered to use its best efforts—I think the language is—let's see—reasonable—an order—a court order requiring reasonable technical assistance. What's the difference between a court order requiring reasonable technical assistance to accomplish the bypassing or disabling of the auto-erase function versus a civil subpoena, or a court order pursuant to a subpoena, a motion to compel the delivery of information under that person's custody and control? Is there a difference?

Mr. VANCE. I'm not sure, Congressman, there is a difference. They're both court orders that are directing an end result. One may be in a civil context; one in a criminal context.

But I would say that in this discussion, it's very much a part of our history in America that when companies produce items or objects, or commerce becomes ubiquitous in a particular area, that the company has to have the realization that part of a group of people who are using its products are using it to commit criminal purposes.

Take a look at the banking system, currency transaction reports. So once it became obvious that criminals were moving cash through the banks, the response was you have to create and file transaction reports when cash is moved.

When two companies like these two hugely successful and important companies own 96.7 percent of the world's smartphone market, and we know that criminals—we know that criminals are using the devices to commit crimes—we've heard some of those stories—I don't think that it is new in American history, or in the con-

text of business ethics or oversight for companies to have to adapt to the realities of the product they've created.

Mr. JOHNSON. Because they are the only ones that can—a bank that received the cash would be the only entity in a position to submit a currency transaction with the court?

Mr. VANCE. It would be the only one required to. If someone else had information about it, they could submit it, but it would be the only one who had firsthand knowledge.

Mr. JOHNSON. Okay. Now, Ms. Landau, is it your opinion that the government should not have the ability to compel Apple to use its best efforts to accomplish a technical feat? Is that your opinion?

Ms. LANDAU. So there are two answers to that. If you're asking me a lawyer question, then I'm not a lawyer and I'll dodge; but if you're asking me as a technologist, then I would say that it is a security mistake. It's a security mistake because that code——

Mr. JOHNSON. Because what Apple would do would inherently cause an insecurity in their system?

Ms. LANDAU. That's right. And it will be the target of organized crime and nation states, because it will be very valuable for somebody who puts a phone down as they go through Customs, for somebody who goes to a business meeting, and they're not allowed to bring their phone in because it's a meeting under nondisclosure, and the phone is sitting outside for a few hours. All sorts of situations. The phone will become very interesting. And if there's code that can actually get into the phone and get the data, that code is going to be the target of nation states——

Mr. JOHNSON. So once Apple creates the code, then it makes it susceptible to being stolen and misused?

Ms. LANDAU. That's right.

Mr. JOHNSON. So, therefore, Apple should not be required to comply with the court order?

Ms. LANDAU. I'm not answering the legal question. I'm answering the security question. The security question, it makes a real mistake.

Mr. JOHNSON. Yeah. Okay. And, Mr. Sewell, you would agree with that?

Mr. SEWELL. I would agree that if we're forced to create this tool, that it reduces the safety and security not within our systems, Congressman, but with our users.

Mr. JOHNSON. Let me ask you a question. What about the security and the safety of those whose liberty can be taken and lives can be taken due to an ongoing security situation which the FBI is seeking to get access to information about? Is there an interest in the public security that we're talking about here?

Mr. SEWELL. Congressman, that's what——

Mr. GOODLATTE. The time of the gentleman has expired, but Mr. Sewell may answer the question.

Mr. SEWELL. That's what makes this such a hard issue, because we're balancing two different but very similar issues: private security, the security of people who use iPhones, the location of your children, the ability to prevent your children from being kidnapped or harmed, versus the security that's inherent in being able to solve crimes.

So it's about how do we balance these security needs, how do we develop the best security for the United States. If you read the statements by General—any of the encryption specialists today, we'll say that de-featuring or debilitating encryption makes our society less safe overall. And so that's what we're balancing. Is it the right thing to make our society overall less safe in order to solve crime? That's the issue that we're wrestling with.

Mr. JOHNSON. Thank you.

I yield back.

Mr. GOODLATTE. The Chair recognizes the gentleman from South Carolina, Mr. Gowdy, for 5 minutes.

Mr. GOWDY. Thank you, Mr. Chairman.

Now, Mr. Sewell, you just mentioned a balancing. Can you give me a fact pattern where Apple would consent to the magistrate judge's order in California?

Mr. SEWELL. Congressman, we will follow the law. If we're ordered to do this——

Mr. GOWDY. No, I'm asking for a fact pattern. You mentioned balancing. I want you to imagine a fact pattern where you balance the interest in favor of what the Bureau is asking you to do as opposed to your current position. Give me a fact pattern.

Mr. SEWELL. Congressman, what I said was we have to balance what is the best security for the country. Not balance when we should give law enforcement what they're asking, but balance what's the best security for the country.

Mr. GOWDY. I thought that's what we were balancing is public safety versus privacy. You also mentioned the First and Fifth Amendment. Can you give me a fact pattern where Apple would consent to the order of the magistrate judge?

Mr. SEWELL. Congressman, what I said was privacy, security, personal safety.

Mr. GOWDY. Perhaps I'm being ambiguous in my asking of the question. Can you give me a fact pattern where you would agree to do what the Bureau is asking you to do in California, whether it be nuclear weaponry, whether it be a terrorist plot? Can you imagine a fact pattern where you would do what the Bureau is asking?

Mr. SEWELL. Where we would create a tool that doesn't exist——

Mr. GOWDY. Yes.

Mr. SEWELL [continuing]. In order to reduce the security and safety of our users?

Mr. GOWDY. Yes.

Mr. SEWELL. I'm not aware of such a fact pattern.

Mr. GOWDY. So there is no balancing to be done. You have already concluded that you're not going to do it.

Mr. SEWELL. No, I've said that we will follow the law. If a balance that is struck, if there is an order for us to comply with, we——

Mr. GOWDY. There is an order.

Mr. SEWELL. That order is being challenged at the moment as we speak. There's an order in New York that says——

Mr. GOWDY. I'm glad you mentioned the order in New York. That's a drug case. You would agree with me the analysis in drug cases is very different from the analysis in national security cases.

And even if you didn't agree with that, you would agree that in footnote 41, the magistrate judge in New York invited this conversation about a legislative remedy, which brings me back to Chairman Sensenbrenner's question: Where is your proposed legislative remedy?

Mr. SEWELL. We don't have legislation to propose today, Congressman. What we've suggested——

Mr. GOWDY. Well, then how will we know whether or not you think it strikes the right balance if you don't tell us what you think?

Mr. SEWELL. Congressman, where we get to the point where it's appropriate for us to propose legislation, not just Apple, but the other stakeholders that are engaged in this process, I'm sure there will be legislation for Congress to consider.

Mr. GOWDY. Well, let the record reflect I'm asking you for it now. I would like you to tell us what legislative remedy you could agree with?

Mr. SEWELL. I don't have an answer for you today. No one's had an answer for you today.

Mr. GOWDY. Can you give me one? I don't know whether Apple has a lobbyist. I suspect that you may have a government relations department, possibly. Can you submit legislation to Chairman Sensenbrenner's question that you could wholeheartedly support and lobby for that resolves this conundrum between you and the Bureau?

Mr. SEWELL. It is my firm belief that such legislation can be drafted. I do not have language for you today.

Mr. GOWDY. Well, but, see, Mr. Sewell, we draft it and then your army of government relations folks opposes it. So I'm just trying to save us time. The judge in New York talked about a lengthy conversation. Sometimes circumstances are exigent where we don't have time for a lengthy conversation. So why don't we just save the lobbying and the opposing of whatever, Cedric Richmond or Hakeem or Luis and I come up with. Why don't you propose it? Tell us what you could agree to?

Mr. SEWELL. Congressman, we're willing to and we've offered to engage in that process.

Mr. GOWDY. The legislative process or the debate process?

Mr. SEWELL. Both, of course.

Mr. GOWDY. Will you submit legislation to us that you could live with and agree with?

Mr. SEWELL. If, after we have the debate to determine what the right balance is, then I think that's a natural outcome.

Mr. GOWDY. Well, how long is the debate going to last?

Mr. SEWELL. I can't anticipate that, Congressman.

Mr. GOWDY. Well, let me ask you this: You mentioned the First Amendment, which I found interesting. Are you familiar with voice exemplars?

Mr. SEWELL. I'm sorry. Is that a case, Congressman?

Mr. GOWDY. No. Voice exemplars are ordered by courts and judges for witnesses or defendants to actually have to speak, So a witness can see whether or not that was the voice that they heard during a robbery, for instance. Because you mentioned you have a First Amendment right to not speak. What about those who have

been immunized and still refuse to cooperate with a grand jury, and they are held in contempt and imprisoned? So there are lines of cases where you can be forced to speak.

Mr. SEWELL. Congressman, we've made an argument, a constitutional argument. If the courts determine that that argument isn't firm, then we will lose the argument.

Mr. GOWDY. I'm just asking you whether or not you agree that there are exceptions?

Mr. SEWELL. You've given me two examples that I've not heard of before.

Mr. GOWDY. All right. How about back to the Fifth Amendment, because I'm out of time. Really quickly, the Fifth Amendment, you say you're being conscripted to do something. But there's also a line of cases where folks are conscripted to perform surgical procedures, or cavity searches or other things I won't go into in mixed company, where they are looking for contraband. So that's a nurse or a doctor or an anesthesiologist that is conscripted by the government, you would agree?

Mr. SEWELL. I'm not familiar with these cases. But this is what the court will decide.

Mr. GOWDY. Here's what I'll do. I'm out of time. I'll get you the cases I'm relying on, if you'll help me with the legislative remedy. Deal?

Mr. SEWELL. I look forward to the cases.

Mr. GOWDY. Deal. Thank you.

Mr. GOODLATTE. Time of the gentleman has expired.

The Chair recognizes the gentleman from Florida, Mr. Deutch, for 5 minutes.

Mr. DEUTCH. Thank you, Mr. Chairman.

I would start by saying this is really hard. I'm not looking to Apple to write the legislation to balance these very difficult issues between privacy and public safety. I don't expect you to do it. I expect us to grapple with it. And that's what we're trying to do here today.

And I had raised the point earlier, but it's a perfect lead-in to the questions I want to ask, that this focus on surgical procedures that we can force—that the government can force a surgical procedure to be done, sounds like it's somehow equivalent. Certainly if we can do that, then we can require that a company create a way into its phone.

Except, as I said earlier with Director Comey, that surgical procedure is going to be done by the person that the government says should do it. And there is no one from around the world who, from their remote location, is going to be able to figure out how to conduct surgery on that individual.

Yet, in this case, and this is why this is so hard for me, in this case, there are people all over America and around the world who would be trying to figure out how to utilize whatever it is that's created here, if this is where this goes, to access the phone.

And Director Comey earlier—Mr. Sewell, Director Comey said it's a three step—he believes it's a three-step process that they're asking. Can you just speak to that process?

Mr. SEWELL. I absolutely can. Thank you, Congressman.

First, I agree with you that this is not a problem which—there are people that are trying to break into these systems. There are people who are trying to steal this information, if it existed. And their capabilities are increasing every day. So this is not a threat which is static. This is a threat which is increasing.

The three parts that we're being asked to develop are, first, a method to suppress the data deletion after 10 failed attempts. The second thing that we're being asked to suppress is the time delay between successive attempts. Both of these are specifically tailored to deal with the situation where your phone is stolen, or some bad person is trying to break into it, and it's specifically designed to defeat the brute force attack.

The third piece is interesting, because the third piece is the government asking for us to rewrite the code that controls the touch screen, and allow them to put a probe into the phone and to bypass the need to enter numeric digits through the touch screen. The only reason that that makes sense, Congressman, is if you anticipate that this is going to be technology used on other phones, and other phones that likely have more complicated passcodes.

Mr. DEUTCH. Right. So that's the question, and Mr. Sewell, it's a question for you, and Mr. Vance, it's a question for you. This is one where if I believed—if I understand that what's being asked of you is to create this weigh-in to this one phone, then I want you to do it. I do. And I can get past a lot of these privacy issues, if I believe that it's, once in, and then this can then be disposed of, destroyed, and that will be the end of it.

The question is, is that the case? And when you create it for this one, is it something that can be used on other phones? Director Comey, I don't think, was clear about that, so I'd ask you that question, and Mr. Vance, I'd ask you the same question.

Mr. VANCE. If I can refer to actually the Doctor's own paper. You need the phone physically at Cupertino to open it. And I refer you to her——

Mr. DEUTCH. I don't have much time. I'm not sure that I understand what that means. I just want to know—cutting to the chase, I just want to understand, if this is created, is it something that not just could be used by you in the pursuit of justice, but by the criminal cyber terrorist, hackers, and really dangerous people who are looking to do bad things every day of the year going forward?

Mr. VANCE. Congressman, my point is simply that if this code is created, and you are looking at the risk to other devices, other Apple phones in the world, those phones are going to have to come to Cupertino to be opened. This is——

Mr. DEUTCH. Well, let me ask Mr. Sewell, then. I only have a couple seconds left.

Mr. SEWELL. That is incorrect.

Mr. DEUTCH. Well, the question is, even if that's correct, I'd like you to speak to it. Is it true that the hackers of the world, that there will be those who try to find a way to get around having to take the phone to Cupertino in order to conduct whatever operation is necessary to break in?

Mr. SEWELL. Unquestionably, Congressman, and that's exactly the risk and the danger that we foresee.

With respect to the comment that Mr. Vance just made, in fact, the request that we got from the government in this case was that we should take this tool and piece—put it on a hard drive, and send the hard drive to the FBI. The FBI would then load that hard drive into a computer, hook the phone up to the computer, and they would perform the entire operation. So that this whole tool is transportable on a hard drive. So this is a very real possibility.

Mr. DEUTCH. So should we be concerned, Mr. Vance? I mean, look, I want to get into this phone, but shouldn't we be concerned, if that's accurate, that there's something that's being created that's transported on a hard drive that winds up on another computer, that there is at least the risk that that gets stolen and then—and suddenly, there is—that not just a bad person and these terrorists that we desperately want to get and get this information, but suddenly, all the rest of us who are trying to protect ourselves from the bad people and are trying to protect our kids from these bad people are potentially at risk, too?

Mr. VANCE. Congressman, I respectfully disagree with the colleague from Apple, but I will confess that his knowledge of the company is great. Apple has created a technology which is default disk encryption. It didn't exist before. It exists now. Apple is now claiming a right of privacy about a technology that it just created. That right of privacy didn't exist before Apple created the technology, number one.

Number two, I can't answer how likely it is that if the Federal Government is given a source code to get through the front door of the phone, that is at risk of going viral. I think it may be overstated to suggest that.

But I can tell you this: If there's an incremental risk that providing the source code creates a vulnerability, what is that risk? Don't tell us just millions of phones might be affected; tell us—I think they can do better than just giving us broad generalizations without specifics.

But I can tell you this: The consequence, the other side of the weight, the consequence is in cases all over the country right now, in my jurisdiction, your jurisdiction, everywhere, families like the Mills family are not getting justice.

And the direct consequence of this disk encryption is that innocent victims all over the country are not getting their cases solved, prosecutors are not doing the job that they have been elected and sworn to do, and there is a significant consequence to default disk encryption that I think needs to be balanced against a speculative claim of increased insecurity.

Ms. LANDAU. I'd like to just add a couple of comments. This is not about a new right of privacy; it's about a new form of security. And if we think about how the phones are used and increasingly how the phones are used, I certainly have two-factor authentication I use through my phone, but there are ways of using the phones as the original authentication device.

And if you make the phone itself insecure, which is what is being asked for by law enforcement, you preclude that, and that is the best way to prevent stealing of log-in credentials, the use of the phone as authenticator.

In terms of the risk of the disk and so on, it's not the risk of the disk going out because the disk is tied to a particular phone. The risk is that somebody will come into Apple and provide a rogue certificate that, you know, they're from law enforcement or wherever and will get the ability to decrypt a phone that should not be decrypted, whether it's the Chinese Government, or an organized crime group or whatever. That's the risk we're facing.

Mr. VANCE. May I, Congressman, with the Chairman's permission?

Mr. DEUTCH. My time is up. The Chairman has been very generous.

Mr. GOODLATTE. Well beyond the time, but briefly.

Mr. VANCE. The professor has not answered what about the people, the residents, the citizens, the victims whose cases are being put on the side, and not addressed why we have an academic discussion, an important one——

Mr. GOODLATTE. Well, it's an important academic discussion because before these phones existed, the evidence that you're talking about didn't exist in the form that you have had access to. Now the technology is moving to a new generation, and we're going to have to figure out a different way to help law enforcement. But I don't think we say we're not going to ignore these vulnerabilities that exist in order to not change the fact that law enforcement is going to have to change the way it investigates and gathers evidence.

The time of the gentleman has expired.

The Chair recognizes the gentleman from Illinois, Mr. Gutierrez.

Mr. GUTIERREZ. Thank you, Mr. Chairman.

First of all, I'd like to ask through the Chair if Congressman Lofgren has a need for any time, I'd like to yield to her first.

Ms. LOFGREN. Well, I thank you very much.

You know, I don't know you, Mr. Vance. I'm sure you're a great prosecutor. I do know Mr. Sewell. He's a great general counsel.

But the person who really knows technology on the panel is Dr. Landau. And I'm interested in your comments about the vulnerabilities that would be created by complying with the magistrate's order. And some have suggested that it's speculative and, you know, academic and the like, but is that what your take on this is?

Ms. LANDAU. Absolutely not.

Ms. LOFGREN. The theory—I mean, we're moving to a world where everything is going to be digital, and you could keep track of, you know, my—when I'm walking around the house I'm in, my temperature, opening the refrigerator, driving my car. And if that all is open to a legitimate warrant—I'm not downplaying the problem the prosecutors have, but this is evidence you currently don't have access to—how vulnerable is our country going to be? That's the question for you.

Ms. LANDAU. Extremely vulnerable. David Sanger's article in today's New York Times about the Ukraine power grid says that they got in, as I mentioned earlier, through the log-in credentials. It's based on a DHS memorandum that talks about locking down various systems.

I served for a number of years on NIST Information Security and Advisory—Security and Privacy Advisory Board, and we used to

talk to people from the power grid and they would say, oh, it's okay. We're not—our systems aren't connected to the Internet. Well, they were fully connected.

We are—whether you're talking about the power grid, the water supply, whatever—we're connected in all sorts of the disastrously unsafe ways. And as I mentioned earlier, the best way to get at those systems is through log-in credentials.

Phones are going to provide the best way to secure ourselves. And so this is not just about personal safety of the data that all of you have on your phone, and it's not just about the location of where your family is, and it's not just about the business credentials, but it's really about the, as you say, Congressman Lofgren, it's really about the way we are going to secure ourselves in the future.

And what law enforcement is asking for is going to preclude those strong security solutions. It also is very much a 20th century way of looking at a 21st century problem. And I didn't get a chance to answer Congressman Gowdy, but the FBI, although it has excellent people, it hasn't put in the investment.

So Director Comey said—we talked to everyone who will talk to us, but I was at a meeting—I briefed at FCC a couple of years ago, and some senior people from DOJ were there. And I said, well, you know, NSA has scale X and scale Y, and DOJ said they won't share it with the FBI, except in exceptional circumstances, they keep it for themselves.

We're in this situation where I think law enforcement needs to really develop those skills up by themselves. And you ask about what it is this Committee can do, it's thinking about the right way for law enforcement to develop those capabilities, the right level of funding. The funding is well below what it should be, but they also don't have the skills.

Mr. GUTIERREZ. Thank you.

So, I'm happy I yielded the time to you. I always know it's one of the smartest things I do is work with Congressman Lofgren in this Committee.

But I just want to share with you, look, I understand the competing interests here. But I think, Mr. Sewell, you should understand that I love your products. You know, I used to think, you know, house, then a car, now I think technology. Between what they charge me for the Internet, all the stuff I buy just to get information every day, it's—but don't worry, I can afford it. I'm not going into the poorhouse because of it.

So I'm excited about all of the new things that I get to and how it improves my life. And so I'm thankful to men and women in technology for doing that. But a lot of times in this place, there's adversarial positions taken, and I would hope, simply, that we would look for a way in which we put the safety interests of the American people.

I understand that you think that if we find a back door, that that causes all kinds of insecurity. But in this Committee, I'm going to work with Congressman Lofgren, but I'm also going to work with Trey Gowdy. We're going to work—a lot of times bipartisanship in this place is many times promoted, but very rarely rewarded in

this place, because everybody says, oh, you should take one position or another.

I'm going to take a position for the American people. While you might dispute, I kind of look at apple as an American company. I look at Toyota as a Japanese company, BMW as a German. I look at you as an American company, and so that's the way I see you. You can dispute that, you may look at yourself as an international entity, but I always looked at you as the pride. When I take this phone as a member of the Intelligence Committee, and I take this phone to China, the Intelligence Community of the United States of America, the first thing before I get off that plane, they take it away from me. So there are bad actors out there already intervening with your products, or I don't think the fine people of the Intelligence Community would take away one of the things that I need the most in my life.

So having said that, I hope we might find a way so that we could balance the security needs and the safety needs of the people of the United States and their rights to privacy. I think it's essential and important. And I want to thank you guys for coming and talking to us, and let's try to figure it out all together. Thanks.

Mr. SEWELL. Thank you, Congressman. And I absolutely—I agree with what you said. And I think that—I am proud to work for Apple. And I think Apple embodies so many of the most valuable characteristics that make up America, make America a great place. We stand for innovation, we stand for entrepreneurship, we stand for empathy, we stand for all boats rise. And so I am very proud. And we are an American company, and we're very, very proud of that.

The point about security outside the United States is exactly the point that drives us. We are on the path to try to create the very best, most secure, and most private phones that we can. That's a path that will probably never end, because the people that we're competing with, the bad guys, not just in the United States, but all over the world, are on an equally aggressive path to defeat everything that we've put into the phone. So we will continue from generation to generation to improve the technology, to provide our users with a safer experience.

Mr. GUTIERREZ. Thank you, Mr. Sewell.

Thank you, Mr. Chairman.

Mr. GOODLATTE. The gentleman from Louisiana, Mr. Richmond, is recognized for 5 minutes.

Mr. RICHMOND. And I'm happy to follow Luis, because I guess we're going to start—I'll start where he left off. And I think about a 9-year-old girl who asked, you know, why can't they open the phone so we can see who killed my mother, because I was there and heard it happen.

So let me start with this: If the FBI developed the ability to brute force open a phone, would you have a position on that?

Mr. SEWELL. Without involving Apple, without having Apple——

Mr. RICHMOND. Yes.

Mr. SEWELL. - complicit in that. I don't think we have a position to object or not object to that. I think if the FBI has a method to brute force a phone, we have no ability to stop them.

Mr. RICHMOND. But are you okay with it?

Mr. SEWELL. Well, I think that privacy and security are vitally important national interests. I think that if you weaken the encryption on the phone, then you compromise those vitally important interests.

Mr. RICHMOND. Well, I'm not asking you about the encryption. If they could brute force open a phone, do you have a problem with that? I think that's just an easy question.

Mr. SEWELL. Then I'm sorry. Perhaps I'm misunderstanding. If the FBI had the ability to brute force a phone, I would suggest that that's a security vulnerability in the phone. So I would have a problem with it, yes.

Mr. RICHMOND. Let me ask you another question, because I see you're a lawyer, I'm a lawyer, and I would feel awful if I didn't ask this. Brittney Mills——

Ms. LANDAU. I—can I just say something for a second?

Mr. RICHMOND. In a second. Let me get through this question. Brittney Mills had a 5S phone operating on an 8.2 iOS. Does Apple, any employee, subcontractor, subsidiary, or anyone that you know of possess the knowledge or the ability to open that phone? Or unlock that phone?

Mr. SEWELL. We don't. And I'm glad that you asked about the Mills case, because I think it's instructive about the way that we do work together cooperatively. I know that we met with members of your staff——

Mr. RICHMOND. Look, and I'm not suggesting that you all don't, but I just want to—I want to know, does anybody have the ability to unlock the phone first? And if you tell me no, then I get a no in public on the record and I feel a lot better about what I'm doing.

Mr. SEWELL. Congressman, let me be clear. We have not said that we cannot create the tool that the FBI has asked us to create.

Mr. RICHMOND. Right. And I'm not asking about creating anything. I'm saying does it exist now? Do you know anybody—or does anyone have the ability to do it right now?

Mr. SEWELL. Short of creating something new, no.

Mr. RICHMOND. Now—and I—oh, I'm sorry. Ms. Landau. I promised to let you answer.

Ms. LANDAU. I just wanted to add that in security, we have an arms race. People build good products, somebody finds a vulnerability. It could be the FBI, it could be—now, the FBI may not tell anybody about the vulnerability, but we have this arms race where as soon as somebody finds a problem, the next role of technology comes out, and that's the way we do things.

Mr. RICHMOND. So what would be your feeling if the FBI developed a technology that they can plug something into the iPhone——

Ms. LANDAU. I think that the FBI should be developing the skills and capabilities to do those kinds of investigations. I think it's absolutely crucial. And I think that they have some expertise, but it's not at the level that they ought to have. And I think we're having this conversation exactly because they are—they are really using techniques from—they're using a mind-set from long ago, from 20 years ago, rather than the present.

Mr. RICHMOND. So they're antiquated?

Mr. GOODLATTE. Would the gentleman yield?

Mr. RICHMOND. Sure.

Mr. GOODLATTE. I just want to clarify. Both Mr. Sewell and Ms. Landau did not say subject to an authorized court-ordered warrant.

Ms. LANDAU. Well, I certainly——

Mr. GOODLATTE. And you're not suggesting they develop this technology and then do what they think is best. They've got to do it subject to a warrant.

Ms. LANDAU. Of course. Thank you.

Mr. RICHMOND. And I'm glad you cleared that up, because I want to make sure that everybody understands what I'm saying. I don't think any of this should happen without a court order.

Now, you know, maybe I watch too many movies, and maybe I listen to Trey Gowdy too much. Some people would suggest if I listen to him at all, that's too much. But in the instance that there's a terrorist that has put the location of a nuclear bomb on the phone, and he dies, how long would it take Apple to develop the technology to tell us where that nuclear bomb was, or would Apple not be able to develop that technology to tell us in a short period of time?

Mr. SEWELL. The first thing we would do is to try to look at all of the data that surrounds that phone. There is an enormous change in the landscape over the last 25 years with respect to what law enforcement has access to. So when we have an emergency situation like that, whether it be a lost child or the airplane—when the Malaysia airline went down, within 1 hour of that plane being declared missing, we had Apple operators cooperating with telephone providers all over the world, with the airlines, and with local law—well, the FBI, to try to find a ping, to try to find some way that we could locate where that plane was. So the very first thing that we would do in the situation is to bring to bear all of the emergency procedures that we have available at Apple to try to find them.

Mr. RICHMOND. Thank you.

Mr. Chairman, can I just clarify, because I don't want anyone to leave out of here thinking that Apple has not been cooperative with our district attorney in the effort to access the data, and, in fact, they came up with new suggestions, but my questions are just about the government's ability to just brute open a phone at any point with a court order. So I don't want to suggest that Apple has not been working diligently with my DA, who's also been working diligently. So thank you, Mr. Chairman. I yield back.

Mr. SEWELL. I appreciate that, Mr. Congressman.

Mr. GOODLATTE. The Chair thanks the gentleman and recognizes the gentlewoman from Washington State, Ms. DelBene.

Ms. DELBENE. Thank you for being here and enduring this for a while. It's very, very important.

In the earlier part of the hearing, Director Comey said that it is not a company's job to worry about public safety, and I think that that is—would be very concerning for a company to send that message, given that we have technologies that impact people's everyday lives in so many ways. And I assume you agree with that, Mr. Sewell.

Mr. SEWELL. I absolutely do. I do not subscribe to the position articulated by Director Comey.

Ms. LANDAU. I've worked for two Silicon Valley companies, Sun Microsystems and Google, and that's certainly not what I saw at either one of them.

Ms. DELBENE. In the Brooklyn case decided yesterday, Judge Orenstein stated, in his opinion, that the world of the Internet of things, all of the connected devices and sensors that we see coming forward, the government's arguments would lead quickly to a world of virtually limitless surveillance and intrusions on personal privacy.

So I'd like to explore the issue of encryption and securing the Internet of things a little bit. We often talk about security by design when it comes to the Internet of things. And I'm sure we can all imagine the horror stories of insecure Internet of things, types of devices, like appliances being hacked that could cause a fire, or spying through baby monitors, hacking into a car, or tampering with a home security system.

So I'm wondering—Dr. Landau, I'm wondering if you could comment on what this means in the encryption context and whether directives we've heard from the FTC, for example, to adopt security by design in the interests of protecting consumers from malicious actors is inherently incompatible with what you might call insecurity by design should that be mandated by the courts.

Ms. LANDAU. Well, here you're in a situation where the companies often want to collect the data. So, for example, if you're using smart meters, the company wants the data, the electric company wants the data to be able to tell your dishwasher, no, don't turn on at 4 in the afternoon when air conditioning requirements are high in Silicon Valley right now, turn it on at 8 at night or 2 a.m. And so, in fact, it actually wants the individualized data. And if it has the individualized data, then it can certainly share it with law enforcement under court order.

The security by design is often in the Internet of things securing data on the device and securing the transmission of the data elsewhere.

The issue in the Apple phone is that the data stays on the device, and that's the conflict that we're having. For the Internet of things, it's most useful if the data goes off the device to somewhere else where it can be used in a certain way.

Ms. DELBENE. And, Mr. Sewell, could companies open themselves up to liability if vulnerabilities through law enforcement end up being exploited by a bad actor?

Mr. SEWELL. I think that's absolutely true. Somewhat ironically, I suppose, we have the FTC at this point actively policing the way in which technology companies deal with these issues, and we can be liable under the—Section 5 or under the authority of the FTC if we fail to close a known vulnerability.

Ms. DELBENE. And, Ms. Landau, you talked about the issue of security versus security, and that this really is a debate about security versus security. Could you explain a little bit more why? And are national security and cybersecurity incompatible, in your opinion?

Ms. LANDAU. So what we really have here over the last 20 years, as I mentioned earlier, is you see the NSA, and Snowden revelations aside, we don't have time for me to describe all of the subtle

points there, but you really see the NSA working to secure private sector telecommunications infrastructure, many, many examples.

We have moved to a world of electronic devices, you talk about the Internet of things, that leak all sorts of data. And in order to protect ourselves, whether ourselves, our health data, our bank data, the locations of our children and so on, we need encryption and so on. But if you think more broadly about the risks that our nation faces and the risks of people coming in and attacking the power grid, people coming in and stealing data from whatever company, and stealing patented information and so on, you see a massive national security risk. And you've been hearing it from General Keith Alexander, we've been hearing it from Hayden, we've been hearing it from Mike McConnell, we've been hearing it from Chertoff, all the people who have been involved on the DHS and NSA side.

The only thing that can secure that is security everywhere, and the move that Apple makes to secure the phones is one of the many steps we need in that direction.

Ms. DELBENE. Thank you. My time's expired. I yield back, Mr. Chair.

Mr. MARINO [presiding]. Thank you. I now am going to recognize myself for some questions. So welcome to everyone. We'd like to start with Mr. Sewell.

I'm sorry. Mr. Sewell, pronouncing that name correctly?

Mr. SEWELL. You are.

Mr. MARINO. All right. I have some questions for you concerning China. In 2014, you moved your—what's referred to as your Chinese cloud to China. Is that correct?

Mr. SEWELL. That is correct.

Mr. MARINO. Okay. And can you tell me whose data is stored in that Chinese cloud? Is it just people in China? Is my data stored in that cloud as well?

Mr. SEWELL. Your data is not stored in that cloud.

Mr. MARINO. Is it strictly limited to Chinese people?

Mr. SEWELL. There are a number of things that are in the cloud, so I should probably be clear about what's there.

Mr. MARINO. Okay.

Mr. SEWELL. With respect to personal data, no personal data is there unless the individual's data—the individual himself has registered as having a Chinese address and having a Chinese access point. In addition, we have other data, which has to do with film content, movies, books, iTunes music. The reason we do that is because of something called latency. If you're streaming across the Internet, and you have to bring the data from the United States to China, there's a lag time, there's a latency piece, whereas if we move that data closer to China, either Hong Kong or mainland China, then we can provide a much better service to our customers.

Mr. MARINO. Okay. Can you tell me, what was the cost, in a ballpark figure, in the time to make the move to—for the United States to move Chinese information over to China in their cloud?

Mr. SEWELL. Sorry. Did you say in time?

Mr. MARINO. Yeah. Cost and time.

Mr. SEWELL. So the time—the cost is building the facilities. I don't have a number for that. It's certainly not something that I

am aware of, although, of course, the company has that information. In terms of the time, once—once the server exists, once there is a receptacle for the data, in theory, it's instantaneous.

Mr. MARINO. Okay. You may or may not know, but I was a prosecutor for a while, both at the State and Federal level. And we prosecutors are focused on a case and the crime concerned, and we want going to get our hands on anything we can to see that justice is served, but on the other side of this too, we're talking about privacy issues. And I'm very concerned about to what extent, if, for some reason, you were to change your mind about working with the FBI, or the court ordered that, what does that mean to our privacy?

Mr. SEWELL. I think it means that we have put our privacy at risk. The tool that we're being asked to prepare is something which could be used to defeat both the safety and the privacy aspects of——

Mr. MARINO. Let me get this clear, because there are many rumors flying around. And you've probably answered this a couple times, and I apologize. I've had to run and do something else.

Are you saying that there is no method that exists now that you could unlock that phone and let the FBI know what is in there?

Mr. SEWELL. Short of creating the tool that they have asked us——

Mr. Marino. Right.

Mr. SEWELL [continuing]. We are not aware of such a method, no.

Mr. MARINO. Now, you talk about the cost is an unreasonable burden and the time involved. That's why I asked you what did it cost to move the cloud, what was the time. And you're the expert, I'm not.

Mr. SEWELL. Congressman, to be fair, we haven't claimed that the time that it would take to create the tool is the undue burden. Our claim is that the undue burden is to compromise the safety and security of all of our customers.

Mr. MARINO. So it's your position that if you do what the FBI wants to one phone, could you elaborate on that in the 33 seconds I have left as to why that would be an undue burden, keeping in mind that I'm very critical about our privacy?

Mr. SEWELL. Congressman, the answer is very simple. We don't believe this is a one-phone issue. We don't believe that it can be contained to one phone or that it would be contained to one phone.

Mr. MARINO. Okay. I see that my time has just about run out, so I'm going to yield back.

And who's next? Mr. Jeffries, Congressman Jeffries is next.

Mr. JEFFRIES. I thank my good friend from Pennsylvania for yielding. I want to thank all of the witnesses for your presence here today. It's been a very informative discussion. In particular, I want to thank DA Vance for your presence, and certainly for the many progressive and innovative programs that you have in Manhattan, proving that you can be both tough and fair as a prosecutor, and that has not gone unnoticed.

Let me start with Mr. Sewell. There's an extensive record of cooperation that Apple has with law enforcement in the San Bernardino case. Isn't that fair to say?

Mr. SEWELL. That's correct. For over 75 days, we've been working with the FBI to try to get to more information to try to help solve this crime.

Mr. JEFFRIES. I think it's useful to put some of this on the record. On December 5, the Apple emergency 24/7 call center received a call concerning the San Bernardino shooting. Is that right?

Mr. SEWELL. That's right. In fact, the call came in to us at 2:47 a.m. On a Saturday morning. We have a hotline that exists; we have people who are manning that hotline.

Mr. JEFFRIES. And you responded with two document productions that day, correct?

Mr. SEWELL. By 2:48 that morning, we were working on the case, and we responded by giving the FBI all of the information that we could immediately pull from our sources, and then we continued to respond to subpoenas and to work directly with the FBI on a daily basis.

Mr. JEFFRIES. Right. In fact, the next day, I think, Apple received a search warrant for information relating to at least three email accounts. Is that right?

Mr. SEWELL. That's correct.

Mr. JEFFRIES. You complied with that request?

Mr. SEWELL. We did comply with that and subsequent requests.

Mr. JEFFRIES. And so I think also on January 22, you received another search warrant for iCloud information related to the iPhone that was in possession of the male terrorist. Is that right?

Mr. SEWELL. That's right. And it's important that in the intervening stage, we had actually sent engineers to work directly with FBI technicians in Washington, D.C., and in Cupertino, and we provided a set of alternatives, or options that we thought should be tried by the FBI to see if there might be some possibility that we could get into this phone without having to do the tool that we're now being asked to create.

Mr. JEFFRIES. So the issue here is not really about cooperation, as I understand it. Apple has clearly cooperated in an extensive fashion as it relates to all of the information that you possess.

The question, I think, that we all, on the Judiciary Committee and beyond, have to consider is the notion of you being asked, as a private company, to create anti-encryption technology that currently does not exist and could jeopardize the privacy and security of presumably hundreds of millions of iPhone users throughout the country and the world. Is that right?

Mr. SEWELL. We're being asked to create a method to hack our own phones.

Mr. JEFFRIES. Now, Mr. Vance, are you familiar with the *Arizona v. Hicks* Supreme Court case from the late 1980's?

Mr. VANCE. If you give me the facts, I'm sure I have read it.

Mr. JEFFRIES. Okay. The Supreme Court held that police conducted an unconstitutional search of evidence that was not in plain view. It was a decision that was written by Justice Antonin Scalia. And the most important point that I want you to reflect upon is, he stated, in authoring the majority opinion, that "There is nothing new about the realization that the Constitution sometimes insulates the criminality of the few in order to protect the privacy of us all."

Do you agree that embedded in the fabric of our Constitution, the Fourth Amendment, and beyond, is the notion that we value the privacy rights of Americans so deeply, that, at times, it is something that will trump law enforcement convenience?

Mr. VANCE. Congressman, I do sincerely believe that. What concerns me about the picture we are seeing from the

State perspective is that Apple has decided that it's going to strike that balance now with no access by law enforcement for full disk-encrypted devices even with a warrant. So they have created their own balance. They now have decided what the rules are, and that changes radically the balance that existed previously, and it was done unilaterally. So this Committee——

Mr. JEFFRIES. Well, I think—if I can——

Mr. VANCE. Yeah.

Mr. JEFFRIES [continuing]. Just interject. I mean, I think that that is a balance that ultimately the Congress is going to have to work out, and also the Article III court systems, certainly beyond an individual magistrate, who is not even appointed for lifetime tenure, is going to have to work itself through the court system, a district court judge, maybe the Ninth Circuit, ultimately the Supreme Court, and so the company exercising its right in an adversarial system to have all facts being aired on both sides of the debate is very consistent, in my view, with American democracy and jurisprudence.

There is just one last question that I wanted to ask as my time is expiring, because you raised an interesting point earlier in your testimony about an individual who is a suspected criminal who claimed that the encryption technology was a gift from God. But I also noted, I think, in your testimony that this individual communicated that in an intercepted phone conversation that presumably your office or others were wiretapping. Is that right?

Mr. VANCE. No, it's not right. All phone calls from prison, out of Rikers——

Mr. JEFFRIES. Right.

Mr. VANCE [continuing]. Are recorded.

Mr. JEFFRIES. Right.

Mr. VANCE. There's a sign, when you pick up the phone, if you are in Rikers Island, that this is happening. So there's a tape, and ultimately that tape was subpoenaed, and it's from that tape that that conversation was transcribed.

Mr. JEFFRIES. And if I could just, in conclusion, I appreciate the Chair's indulgence. I think that illustrates the point, presumably, that it's fair to say that, in most instances, bad actors will make a mistake, and at the same time that he is heralding the availability of encryption technology to shield his activity from law enforcement surveillance and engagement, he is ignoring a plain-view sign that these conversations are being recorded and subjecting himself to unfettered government surveillance. And I think that I have faith in your ability, in the FBI's ability ultimately to outsmart the criminals and the bad actors without jeopardizing the privacy and the security of the American people.

Mr. VANCE. And in that case, our challenge is, because of our inability to access the phone, our inability to investigate further, any evidence of sex trafficking is not made available to us.

So, yes, he did something that was not smart, but the greater harm is the inability, in my opinion, of being able to get to the true facts, which, in fact, are extremely important as a matter of public safety to get access to.

Mr. JEFFRIES. My time is expired. I thank you.

Mr. MARINO. I thank the gentleman from New York.

And the Chair recognizes now the gentleman from Rhode Island, Congressman Cicilline.

Mr. CICILLINE. Thank you, Mr. Chairman.

And thank you to our witnesses for your testimony and for this very important discussion.

I think we all recognize there are few absolutes in the law, and so balancing occurs all the time. There are risks in developing this software that have been articulated very well during this hearing, and indeed, there are risks associated with an inability to access critical information. So I think we are living in a world there are risks in both ways forward, and I guess my first question is: Many people who agree that Apple or any other company should not be required and there's no authorization to require them to produce a product that doesn't exist or to develop an intellectual property that doesn't exist, many people who think that that's correct wonder whether Apple has considered, in limited circumstances and maybe a standard you would set internally, if it in fact is a situation that would prevent immediate death or serious bodily injury, coupled with a consent of the person or lack of objection—in this case, the person is deceased—where there is no privacy claim asserted, in some very narrow category, whether there is a set of protocols you might voluntarily adopt to provide that information or that software with then instruction that it be immediately destroyed; it be done in a SCIF, in a secure safe. I mean, is that practical, something like that? Should that be part of this discussion that we keep hoping that the industry and the Justice Department will have in trying to develop something, or is that fraught with so many problems that it's——

Mr. SEWELL. Thank you for the question, Congressman. We have and spend a lot of time thinking about how we can assist our customers in the event that they have a problem, if they have lost a phone, if they have—they're in a situation where they're trying to recover data. We have a number of mechanisms to do that, and we will continue to improve those mechanisms as we move forward.

It's very important to us that we try to think about the consequences of the devices that we create. In this particular case, the passcode unlock is not something that we think lends itself to a small usage. The problem with this particular issue is that once you take that step, once you create the mechanism to unlock the phone, then you have created a back door, and we cannot think of a way to create a back door that can only be used beneficially and not be used by bad people.

Mr. CICILLINE. So you have, in fact, sort of already contemplated other ways in which you could make this information available in this case that would not have those sorts of broader implications?

Mr. SEWELL. And we have provided information in this case. We have provided logs. We have provided iCloud backup. We've provided all the things that we have that are available at our disposal.

Mr. CICILLINE. Thank you.

Ms. Landau, you say in your written testimony, the—in your written testimony, the point is that solutions to accessing the data already exist with the forensic analysis community. We did ask Director Comey, and we probably limited our question too narrowly because we asked about the intelligence communities of the United States. It sounds like you're suggesting that there may be capabilities outside the United States Government that the Justice Department or the FBI could contract with that are capable of doing what it is they're asking a court to order Apple to do.

Ms. LANDAU. That's right. So I noticed that when Director Comey answered the question, he said: We talked to everyone who will talk with us.

And I, as I mentioned earlier, I don't know if you were here at that point, I had a conversation with some senior DOJ people a few years ago about using NSA tools in law enforcement cases, and they said: NSA is very loathe to share, because of course, when you share a tool, it can get into a court case, and then the tool is exposed.

And so I don't know in the "we talked with everyone who will talk with us" how much NSA revealed about what they know and what they can do, so that's the first place I would ask. Now, I phrased that incorrectly. That's the first place that I suspect has some tools for exactly this problem. But, yes, there were discussions last week in Silicon Valley. There have been discussions I've had with colleagues where people believe, as Congressman Issa portrayed various potential solutions, that there are ways to break into the phone.

There is, of course, a risk that the data might be destroyed, but I have described both in my testimony—written and verbal testimony, the FBI has not tried to develop this level of expertise and they should.

Mr. CICILLINE. So it seems as if, you know, we are contemplating whether or not Congress should take some action to either grant this authority and then figure out what is the appropriate standard and test, et cetera. It sounds as if you think that is problematic and that, in fact, the real answer is a substantial increased investment in the intelligence capability, the law enforcement capability to sort of keep pace with the advances that companies like Apple are making, that that's really the best protection in terms of both law enforcement and the long-term security of the United States.

Ms. LANDAU. That's right. I don't think actually there needs to be more authority, but there needs to be a completely different view of how it's done. There probably needs to be some authority in terms of how do you handle it for State and local, because State and local will not have the resources, and so there has to be some sort of sharing of tools. And that's a jurisdictional issue and also just a—you know what, an issue between bureaucracies that will have to be worked out, and that will have to be worked out through law and policy.

But in terms of creating new authority, the FBI already has that authority, but it uses it at a much lower level, and I'm sure it's funded at a much lower level. They need to move from the situa-

tion they're in to dealing with 21st century technologies in the appropriate way.

Mr. CICILLINE. Thank you.

I thank you, Mr. Chairman. I yield back.

Mr. MARINO. You bet.

The Chair recognizes Ms. Lofgren from California.

Ms. LOFGREN. Could I ask just one quick question, Mr. Sewell, because I forgot when it was my turn? And we had asked Mr. Comey, somebody asked Mr. Comey about the changing of the password, apparently the county did it at the request of the FBI. What did that do? Can you explain what happened?

Mr. SEWELL. Certainly. One of the methods that we might enable the phone in San Bernardino to do what's called an auto backup. That is, the issue that the FBI is struggling with is to find data between a certain timeframe, the time of the last backup and the time of the horrific incident in San Bernardino.

If the phone would backup, that evidence, that information would become available to the FBI. The way that we can back these phones up in an automatic way is we connect them to a known WiFi source, a source that the phone has already connected to before and recognizes. If you plug the phone in and you connect it to a known WiFi source, it will, in certain circumstances, auto backup, and so the very information that the FBI is seeking would have been available, and we could have pulled it down from the cloud.

By changing the password—this is different than passcode—but by changing the password, it was no longer possible for that phone to auto backup.

Ms. LOFGREN. Thank you, and thank you, Mr. Chairman, for letting me get that information out.

Mr. MARINO. Mr. Sewell, I have one more question for you. Does China—does the Chinese Government have access to the cloud, or is there any indication that they have tried to hack the cloud in China to get information on the Chinese people?

Mr. SEWELL. Let me be clear about the question. The Chinese, undoubtedly, have the ability to access their own cloud.

Mr. MARINO. Yes.

Mr. SEWELL. But with respect to the U.S. cloud, we believe that—again, I'm struggling because of the words. The cloud is a synonym for the Internet.

Mr. MARINO. Yes.

Mr. SEWELL. So, of course, Chinese people have access to the Internet. Are we aware of a Chinese hack through Apple? No. But beyond that, I can't say.

Mr. MARINO. You answered my question. Thank you.

This concludes today's hearing. I want to thank the panel very much for being here.

Without objection, all Members will have 5 legislative days to submit additional written questions for the witnesses or additional materials for the record. The hearing is adjourned.

[Whereupon, at 6 p.m., the Committee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Material submitted by the Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary

March 1, 2015

Congressman Bob Goodlatte
Chairman, House Judiciary Committee
2309 Rayburn House Office Building
Washington, DC 20515

Congressman John Conyers, Jr.
Ranking Member, House Judiciary Committee
2426 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman and Ranking Member:

As your committee takes up "The Encryption Tightrope: Balancing Americans' Security and Privacy," we, the undersigned, write to make the following suggestions:

- Legislation governing cases like Apple's is, as Apple argues, probably inevitable.
- Unfortunately, Congress is currently ill-prepared to draft such legislation, given the complex technical and legal issues involved and widespread confusion over both aspects.
- Only an expert commission of independent experts can help draft legislation that appropriately balances the competing equities.
- There simply is no middle ground on encryption: Congress has already recognized "the right to use encryption" (i.e., secure End-to-End Encryption (E2EE)). Any new legislation should reaffirm that right, whatever it says about cases like Apple's.

We also write to clarify two points of confusion in much of the media coverage of Apple case.

First, while the Apple case involves an "encrypted iPhone," the issue there is readily distinguishable from the central debate regarding encryption that began in the 1990s and that recently flared up again in Congressional hearings last summer over the following questions: May Americans, and American companies, use end-to-end encryption (E2EE)? Or will software makers and service providers have to build a backdoor into communications systems so that law enforcement agencies may intercept all communications?

By contrast, the Apple case turns on what duties tech companies have to facilitate law enforcement's access to an encrypted device – *but not to decrypt the data itself*. This is essentially parallel to the distinction drawn by the 1994 Communications Assistance to Law Enforcement Act, which requires telecommunications services to design their systems to be, essentially, wiretap-ready, subject to a carve-out for encryption. As summarized by the House Report on CALEA:

> Finally, telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court ordered wiretaps, unless the carrier provided the encryption and can decrypt it. This obligation is consistent with the obligation to furnish all necessary assistance under 18 U.S.C. Section 2518(4). *Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access.* The bill does not address the "Clipper Chip" or Key Escrow Encryption issue. *Nothing in the bill is intended to limit or otherwise prevent the use of any type of encryption within the United States.* Nor does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, [47 U.S.C. § 1002(d)(3)] *protects the right to use encryption.*[1]

[1] H.R. Rep. No. 103-827, pt. 1, at 25 (1994), *available at* https://goo.gl/tzqrJk.

CALEA, of course, covered only communications systems, not devices like iPhones. But the question raised by the Apple case is, essentially, about the duties that tech companies not covered by CALEA – including device makers – should have to facilitate law enforcement's access to their products pursuant to a valid court order; it is not about whether they may offer encryption in the first place.

This distinction is vital because the two issues differ fundamentally. Whether American companies may offer, and Americans may use, E2EE is, according to current technological/cryptographic consensus, a "binary" (yes/no) question: either the *user* holds the key necessary to decrypt communications (secure E2EE), or there is a master key that can open those communications (no E2EE). Whether that master key is held by a service provider, the government, or some other third party is immaterial: With the encryption key in another party's hands, the user simply no longer has access to a fully secure system.

But the Apple case presents no choice so stark. There has always been a *range of possible ways to configure device security*. Unlike encryption, other security design decisions work on a sliding scale, which means the needs of law enforcement, for example, can generally be accommodated, to *some* degree, without fundamentally undermining the purpose of a security mechanism. Determining the "right" approach to device security thus involves difficult tradeoffs among competing values: legitimate access by law enforcement, user security, convenience for users, costs of compliance, the courts' interest in "achiev[ing] the ends of justice,"[2] and so on.

We take no position here on how the precise question in the Apple case should be resolved, either under the All Writs Act (AWA) or in future legislation. We simply note that reasonable minds can differ on the Apple case and other cases involving facilitation of law enforcement access to data (if only still in its encrypted form), both on law and on policy, while still agreeing that the "the right to use encryption" should be reaffirmed in American law.

Second, contrary to its depiction in much media coverage, the AWA is not a reactionary throwback, but rather a core part of the American legal system that assures the rights of plaintiffs to obtain justice and due process. And, crucially, the AWA vindicates *the court's* right and ability to exercise its jurisdiction; it is not, in the first instance, about the government's (or other plaintiffs') power per se. For example, U.S. citizens detained without trial at Guantanamo asked Article III courts to use the Act in their attempts to obtain judicial review of their petitions for writs of *habeas corpus*.

While there is nothing inherently wrong with the AWA – and, indeed, much to celebrate about it – that does not mean the Act could not be misused here. Without further direction from Congress, courts applying the AWA's balancing of equities might well set too low a bar for the government to second-guess specific security features. This risk may present a good reason for legislation, but if Congress does decide to legislate, *it should create a statutory alternative to the* AWA, rather than tinkering with what is otherwise a fundamental protection of judicial powers embodied in the AWA – a key part of Judiciary Act of 1789.

Indeed, if there is a problem with the AWA's application in matters of security design, it is not the Act itself, which requires a weighing of equities, but that courts might not weigh the right equities, or weight them properly. Thus, even if one sides entirely with Apple, the Act, and the caselaw interpreting the Act, offer an excellent model for legislation. Specifically, such standards-based statutes can avoid the problem inherent in overly prescriptive, technologically specific legislation: because technological change will inevitably upset whatever balance Congress attempts to codify in statute. The Electronic

---

[2] *United States v. New York Telephone Co.*, 434 U.S. 159, 173 (1977).

Communications Privacy Act of 1986, for example, has failed to protect Americans' privacy simply because the plummeting cost of digital storage made it common to store documents in the "cloud" – which ECPA failed to foresee, and thus failed to protect.

We look forward to contributing to a measured consideration of these difficult questions. In the balance hang both our liberties and our security – both national and personal.

Respectfully,

- TechFreedom
- International Center for Law & Economics
- Niskanen Center

Material submitted by the Honorable Doug Collins, a Representative in Congress from the State of Georgia, and Member, Committee on the Judiciary

MotionMobs
3423 Piedmont NE
Atlanta, GA 30305

The Honorable Doug Collins
1504 Longworth House Office Building
Washington, DC 20515

February 29, 2016

Dear Congressman Collins,

I am writing to you today to urge you to take action on the growing legal dispute between Apple and the Department of Justice. I am the co-founder and president of MotionMobs, a custom app development company with developers in your district that builds apps for local schools and companies. America needs the right tools and intelligence to fight and stop the threat of terrorism, but I am concerned that the FBI's approach will weaken Americans' security in the future.

As an app developer on the Apple platform, I appreciate the built-in security and privacy that I can offer my customers who are building apps that work with private financial, health, and even student information. While it's tempting to believe that the FBI's request is simple and would only affect one phone used by a terrorist, that's simply not how digital security works. Once Apple makes the tools required to help the FBI hack that one phone, they will work on EVERY iPhone and it will be target for hackers around the world. And, it's clear that law enforcement around the country will also start lining up to use these tools regardless of whether it's a terrorism case or a case of unpaid taxes. Putting the genie back in the proverbial bottle is not a real option.

What is even more concerning as an app developer is that the DOJ seems to think this is no big deal, and the precedent is set for all software developers, not just Apple. The FBI argued in their motion to the court that it's not an "undue burden" to force a "software company" to write software to comply with a legal order. This may be true for Apple, but for small companies like ours, or the clients we work with, that kind of burden could lead to bankruptcy. Most startups and small companies don't have excess programmers sitting idly by.

Finally, there is a significant issue regarding the protection of my intellectual property. As I understand it, the government is asking the court to rule that software companies can be asked to modify their software to help apprehend a criminal. If the data from my modified software is used in court, I may be asked to defend my modifications, and explain how the data given is accurate. Moreover, defense attorneys may be able to demand a copy of my source code to be given to outside consultants ostensibly to validate my methodology. My source code is often

the crown jewel of my business – handing it over to "consultants" risks theft or loss, and certainly means any security features will also be exposed.

That is why I'm urging Congress to step in and look at real solutions that can work for law enforcement, the tech industry, and Americans.

From,

Taylor Peake Wyatt
Co-Founder and President
MotionMobs

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

March 1, 2016

The Honorable Bob Goodlatte
Chairman
House Judiciary Committee

The Honorable John Conyers
Ranking Member
House Judiciary Committee

Dear Chairman Goodlatte and Ranking Member Conyers,

TechNet, the bipartisan network of innovation economy CEOs and senior executives, thanks you for holding today's hearing: "The Encryption Tightrope: Balancing Americans' Privacy and Security."

Today's hearing has been driven in no small part by the U.S. government's decision to take the unprecedented step of trying to force a leading American technology company – Apple – to provide access to the encrypted contents of an iPhone. Expanding the 227-year-old All Writs Act, to date used exclusively to require administrative support to the government, into a tool to require a private technology company to create new software and in effect undermine its existing security systems sets a disturbing precedent for obtaining access to iPhones and other American devices. It would also open the door to governments from around the world seeking the very same type of access. This would be a major step in the wrong direction, and given the ubiquity of available encrypted mobile applications, would provide limited useful data to government investigators.

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.

The challenge in this case is that creating a precedent that could force companies to eliminate security features from their products is 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.

However, the attention this particular case has drawn can have a positive outcome if we use it to begin a national dialogue to chart a way forward on the complicated set of legal and technical issues now before this esteemed committee. At TechNet, we hope that today's hearing will serve as a catalyst for such a dialogue.

Sincerely,

Linda Moore
President & CEO
TechNet

Questions for the Record submitted to the Honorable James B. Comey, Director, Federal Bureau of Investigation

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–3951
http://www.house.gov/judiciary

March 31, 2016

The Honorable James B. Comey
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Director Comey,

The Committee on the Judiciary held a hearing on "The Encryption Tightrope: Balancing Americans' Security and Privacy" on March 1, 2016 in room 2141 of the Rayburn House Office Building. Thank you for your testimony.

Questions for the record have been submitted to the Committee within five legislative days of the hearing. The questions addressed to you are attached. We will appreciate a full and complete response as they will be included in the official hearing record.

Please submit your written answers by **Thursday, May 19, 2016** to Kelsey Williams at kelsey.williams@mail.house.gov and Allen Jamerson at allen.jamerson@mail.house.gov or 2138 Rayburn House Office Building, Washington, DC, 20515. If you have any further questions or concerns, please contact the Committee at 202-225-3951.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte
Chairman

Enclosure

Note: The Committee did not receive a response to the questions submitted to this witness at the time this hearing record was finalized and submitted for printing on August 5, 2016.

Questions for the record from Chairman Bob Goodlatte (VA-06):

1. When seeking a solution to the San Bernardino terrorist's phone, did you consult with the NSA or any other agency to determine whether there was a way to override the auto-erase feature?
    a. What other entities did you seek assistance from in trying to find a work-around?
2. Now that you have reportedly found a solution, do you believe it represents an exploit that will soon be patched by Apple?
    a. Are you sharing the solution with state and locals?
    b. Are you using the solution on other iPhones in your possession? Will it work on phones other than just the iPhone 5c?
    c. How likely will it be that this solution will continue to work?
3. What entity helped the FBI develop a solution?
    a. It was reported that an Israeli company assisted? Why was it that a foreign company was able to find a solution but the FBI or other American-based companies couldn't?
    b. Are you concerned that an exploit was developed by a company from a nation which has historically been known to have a sophisticated intelligence apparatus?
    c. If a company in a foreign nation developed this exploit, do you believe other countries also have developed similar exploits? What is the risk that an adversary nation has developed a similar exploit?
    d. Are you going to share with Apple the solution you have found that enables FBI to access stored content that was previously blocked due to the auto-erase function and passcode key?
4. There has been quite a bit of debate about the government's reliance on the All Writs Act to compel Apple to bypass the auto-erase functions on the phone. It has been characterized as an antiquated statute, dating back to 1789, that was never intended to empower the courts to require a third party to develop new technology. Has the FBI relied on the Act in the past to gain access to iPhones or other similar devices? Is the Act limited to circumstances in which Congress has already imposed a statutory duty on a third party to provide assistance?
5. If the U.S. government is allowed to access encrypted devices, what's to stop other governments from making similar demands of American tech companies or prevent cyber hackers and criminals from getting their hands on this technology?

6. Some have argued that law enforcement does not need access to end-to-end encrypted technology since they can already access a wide variety of non-content metadata from providers and obtain content stored in the cloud. Why is it necessary that law enforcement, such as the FBI, also gain access to encrypted devices or apps?

7. Why can't the FBI simply compel a user to turn over their passcode to unlock an iPhone or other encrypted device?

8. Would you say that a phone that is unlocked with a fingerprint or other biometric feature could be unlocked without the assistance of the manufacturer or provider? If so, does that mean that only numeric passcodes are considered "testimonial" for purposes of the 5th Amendment privilege against self-incrimination, but biometric authentication is not similarly protected?

9. Do you have a sense from FBI engineers or cryptographers, or from your discussions with others in the intelligence community, whether there are any adequate, long-term solutions that will both respect consumer privacy and offer law enforcement access to communications when necessary to protect public safety?

10. Do you believe that there are any privacy considerations in the San Bernardino case considering the user of the phone is now dead and the owner of the phone (the former employer) has consented?

11. Considering we are analyzing the larger encryption issue, are you aware whether any of the information that was the subject of the OPM breach was encrypted?

**Response to Questions for the Record from Bruce Sewell,
Senior Vice President and General Counsel, Apple, Inc.**

**Responses to Questions for the Record
"The Encryption Tightrope: Balancing Americans' Security and Privacy"
Bruce Sewell, Senior Vice President and General Counsel
Apple, Inc.**

Questions for the record from Chairman Bob Goodlatte (VA-06)

1. Now that it has been reported that the FBI has been able to access the phone of one of the San Bernardino terrorists, is Apple doing anything to ensure that this vulnerability is patched?

Answer: The FBI has never presented evidence a vulnerability exists. To the extent one does exist, we are committed to finding it and fixing it.

2. Was Apple previously aware that there was a vulnerability in the auto-erase function that would enable a work-around?

Answer: No, and we have no information that there is a vulnerability in the auto-erase function.

3. Have you continued to work with the FBI to develop alternative solutions to access the material on the subject's iPhone?

Answer: No. The FBI states that it was able to access the device without Apple's assistance.

4. Do you believe that FBI's solution will work on newer iPhones or just the subject iPhone 5c?

Answer: The FBI has never presented evidence a vulnerability exists. I believe it has been reported that the FBI says the tool does not work on the 5s or the 6. If that is true, whatever vulnerability may have existed is now fixed. In any event, part of our software and product development processes is to always do our best to find and fix whatever vulnerabilities may exist.

5. If Apple receives a search warrant for contents stored in the iCloud, does it comply? Is the iCloud encrypted?

Answer: Yes, if Apple receives a search warrant for contents stored in iCloud and we have responsive data, Apple will provide it. Yes, with the exception of email, content stored in iCloud is encrypted.

5(a). If so, is it encrypted in such a way that Apple cannot access it? Does that mean it's unsafe?

Answer: Apple retains the key to decrypt iCloud content. Please see the response to Question 5(b), immediately below.

5(b). If the iCloud is safe, despite the fact that Apple can access it, why can't the same be true for iPhones?

Answer: Securing data that exists on servers in Apple's facilities is a very different challenge from securing data that exists on an iPhone or iPad in the possession of our customers. These devices are physically lost and stolen. In addition, customers use iCloud in different ways from how they use their devices, so in designing our products we take those differences into account. This is a question that we continually address as we strive to make our products both as secure and as usable as possible.

6. Why did Apple change its operating system with the iOS 8 version in such a way that the encryption keys on the device are safeguarded by the passcode designated by the user? Presumably, it was to ensure that the phones cannot be hacked?

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.

6(a). How many phones operating on the iOS 7 or an earlier operating system were hacked?

Answer: Apple does not have data tracking that type of information.

6(b). How did Apple decrypt iPhones operating on the iOS 7 or an earlier operating system? Was this done remotely or in-house?

Answer: In the past, using an in-house process, Apple was able to extract data that was not protected by passcode-protected encryption. This applies to iPhones running iOS 7 and earlier operating systems.

6(b)(1). Was the technology you possessed to decrypt these phones ever compromised?

Answer: The process Apple used to extract data from locked iPhones running iOS 7 or earlier operating systems was not, to our knowledge, compromised.

7. In one of its motions, Apple argues that "once the [unlocking] process is created, it provides an avenue for criminals and foreign agents to access millions of iPhones." How would this happen?

Answer: A special operating system created to weaken the security of one iPhone is applicable to all other iPhones. We continue to believe that creating and maintaining a persistent vulnerability would put all of our customers' data in harm's way.

8. Is it possible that there is content or other information on an iPhone, such as the one at issue in the San Bernardino investigation, that is only on the phone and nowhere else - it's not in the cloud, it doesn't reside with a telecommunications provider, it's only on the phone?

Answer: Yes.

8(a). Why should that information be walled off from the rule of law? Why should it be more protected than the papers or effects in someone's home?

Answer: We do not believe the information resides outside the rule of law. We believe US laws can and should be interpreted and applied in recognition of the fact that if an encryption system is undermined, then it is undermined for everyone who uses that system.

8(b). Doesn't the type of encryption employed on the iOS 8 and later operating systems render a search warrant useless to search the phone?

Answer: Apple shares law enforcement's goal of creating a safer world and therefore continues to provide law enforcement all the data we have. Apple does not have the technical ability to extract data from a locked iPhone running iOS 8 or later.

9. In its motion, Apple repeatedly argues that Congress - and not the courts - should resolve this issue. Is it Apple's position that were Congress to enact a new law requiring unlocking or decrypting assistance, that Apple would comply with it?

Answer: Apple does and will comply with the law.

10. If Congress enacts specific legislation to require device manufacturers and app designers to decrypt or unlock their technologies, isn't this incentive for foreign manufacturers to market products with stronger encryption than U.S. products? And couldn't this drive U.S. consumers to those foreign products, thus creating an even greater barrier for U.S. law enforcement?

Answer: Yes.

11. Historically, how many All Writs Act orders has Apple complied with for an Apple device?

Answer: Apple has complied with hundreds of All Writs Act orders to extract data.

11(a). Why is Apple now challenging an All Writs order in this case?

Answer: Please see the response to Question 11(b), immediately below.

11(b). Why is Apple also challenging an All Writs order in the Eastern District of New York for a phone that is using the iOS 7 operating system? Had Apple previously complied with All Writs orders for phones using the iOS 7 or earlier operating system? If so, what has changed that has caused Apple to reject this law as a legitimate means to for the government to obtain assistance with a search warrant?

Answer: Yes, Apple had previously complied with All Writs orders for phones using iOS 7 or earlier operating systems. In the case you reference, it was the Magistrate Judge, not Apple, who questioned whether the All Writs Act provides the government with sufficient legal authority to access data stored on a device. The judge sought briefing and subsequently ruled that the All Writs Act does not provide such authority.

12. The iPhone at issue in the San Bernardino case did not belong to Mr. Farook, correct?

Answer: Yes, it belonged to his employer – the San Bernardino County Government.

12(a). In fact, it belonged to his employer - the San Bernardino County government - and therefore Farook had no reasonable expectation of privacy in the phone. The county has consented to unlocking the phone. Why, at least in this instance, is that not sufficient for Apple?

Answer: As discussed, Apple does not have the technical capability to unlock the phone. The government asked Apple to create a brand new operating system that would weaken the security design and protections of all iPhones so that the government could then unlock this particular phone. Apple does not believe that the All Writs Act, on which the government based its order, grants the government such authority. No court has ever authorized what the government sought.

12(b). Doesn't this raise larger questions about the use of iPhones for business purposes if the employee holds the key to unlocking the device and not the employer? Even outside the context of a governmental request, can an employer come to Apple to have them override the auto-erase functions?

Answer: Employers cannot come to Apple to override device protections such as auto erase. Employers may elect to use or even require use of Mobile Device Management (MDM) software which allows them to remove a device passcode. Opting a phone into MDM requires the user of the device to unlock the device and enter the passcode a second time before installation of the software occurs. If MDM is not installed, it does not after the fact give the employer, Apple, or anyone else the ability to inspect or access data previously stored locally on the device.

13. What, if any, accommodation is made for employers who own phones that have been distributed to their employees for business-only purposes?

Answer: As we stated above, employers may use MDM software in connection with iOS which would allow them to reset a device's password. Employers may also register their ownership of a phone to allow them to request Apple disable on its servers the "Activation Lock" theft protection for an employer-owned device.

14. Is there any instance of national security, terrorist attack, or major gang-related violence affecting our communities where you would offer your assistance in unlocking a single iPhone? In other words, if you were presented with a "ticking time-bomb" scenario, would you offer to produce the necessary software work-around giving law enforcement access?

Answer: Under any scenario, even a "ticking time-bomb", Apple does not currently have the capability to extract data from a device that is protected by encryption that is keyed to a user passcode. We work hard every day to assist law enforcement because we share their goal of creating a safer world. Apple has 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 this team is not working with law enforcement. We know from our interactions with law enforcement officials that the information we provide is extremely useful in helping to prevent and solve crimes.

15. Is Apple acquiescing to requests for access from the governments of other countries as a condition of doing business there? China? Russia? How does Apple comply with requests from foreign governments for access to content?

Answer: Apple has not built a back door for any of our products. Apple has never shown any government any Apple source code beyond that which is

available on our website or through open source. We comply with lawful requests from governments around the world where we do business whenever we are able to provide responsive information, as we do in the United States. As our content is stored in the United States, we require MLAT or Letters Rogatory to provide content in response to requests from third countries.

15(a). It was recently reported that Blackberry had considered pulling out of Pakistan because the country requires "back doors." If Apple is doing business in a country like Pakistan that requires encrypted communications to have "backdoor" access, can we not presume that you are acquiescing to those countries' demands?

Answer: Apple has not built a back door for any of our products. Apple has never shown any government any Apple source code beyond that which is available on our website or through open source.

16. Are there any privacy considerations in this case considering the user of the phone is now dead and the owner of the phone (the former employer) has consented?

Answer: Apple opposition to the order in the San Bernardino case was in response to the government's attempt to vastly expand the scope of its authority under the All Writs Act. The privacy considerations are clear for all users: had the government prevailed in forcing Apple to weaken security for all iPhones, the private information that millions of users store on their devices would be at greater risk of theft from criminals, hackers, and others. Those subject to law enforcement inquiries represent far less than one-tenth of one percent of our hundreds of millions of users. But all of our users would be made more vulnerable if we were forced to build software to degrade security for any reason.

17. Does the auto-erase functions exist on iPhones operating on iOS 7 operating systems or earlier?

Answer: The auto-erase function exists on iOS 7 and earlier operating systems.

18. What percentage of Apple phones are being hacked by China? Other foreign governments?

Answer: Apple does not have data tracking that type of information.

19. Following up on Judge Orenstein's holding in the Eastern District of New York, what evidence do you have that Congress had specifically excluded under CALEA the

products that are currently manufactured by your company, such as iPhones and iPads?

Answer: CALEA's requirements apply to "telecommunications carriers," which are entities "engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." 47 U.S.C. § 1001(8)(A). Apple's role as manufacturer of the iPhone and as software developer of iOS does not fall within this definition. In addition, in at least some contexts, Apple is a provider of information services, expressly excluded from the definition of telecommunications carrier. Id. § 1001(8)(C)(i). Under CALEA "information services" means the "offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications," and "includes a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; electronic publishing; and electronic messaging services." Id. § 1001(6). Apple is substantially engaged in developing and offering products that provide such capabilities. For example, Apple's iTunes service allows customers to purchase, store, and access music, movies, television shows, games and apps via an Internet-connected Apple device, such as an iPhone or iPad. iTunes thus constitutes an "information service" under CALEA by providing "a capability for . . . acquiring, storing . . . [and] retrieving . . . information via telecommunications." Id. Similarly, iMessage allows Apple customers (connected over the Internet) to communicate by messages sent and received via their iPhone, iPad, Mac, and iPod touch devices, and iCloud enables Apple's customers to store photos, calendars, contacts and other information in the cloud so that they can be accessed by any of the customers' devices. Congress intended CALEA to cover telecommunications carriers, but exempt information service providers, "because the functions [they] provide[]" are "information services." In the Matter of Commc'ns Assistance for Law Enforcement Broadband Access and Servs., 19 F.C.C. Rcd. 15676, 15706 (2004). Here, Apple provides substantial information services, and even where it is not providing information services, as when it manufactures devices and installs operating systems, it is still not a telecommunications carrier.

Questions for the record from Representative Randy Forbes (VA-04):

1. Has Apple made any changes or modifications to its products that would make it easier for the Chinese government to get access to user communications?

> *Answer*: No. Apple has not built a back door for any of our products. Apple has never shown any government any Apple source code beyond that which is available on our website or through open source.

2. Did Apple's decision to move iCloud data for Chinese-registered users to China result in making more data available to the Chinese government?

> *Answer*: No. Users' iCloud data stored in China is encrypted, and the decryption keys remain in the U.S. where they are subject to ECPA. The data Apple moved to China was moved to improve customer usability by reducing network latency.

3. Will the tool that the FBI has asked you to build in San Bernardino work for other iPhone 5Cs? What about for newer phones?

> *Answer*: Had we built the new operating system as requested, we believe it would have worked for any iPhone 5c and, with some modification, for all iOS devices.

4. If Apple discovered that the government had a good way to successfully brute-force attack the phone, would Apple try to shut down whatever that method was?

> *Answer*: Whenever we learn of a vulnerability in our products that makes the private information of our users less secure, we fix it. To do anything else would be irresponsible. If we deliberately left that vulnerability unaddressed, we would be helping cyber-attackers in their constant and ever more sophisticated efforts to steal information.

Questions for the record from Representative Blake Farenthold (TX-27) and Representative Suzan DelBene (WA-01)

1. Has Apple made any changes or modifications to its products that would make it easier for the Chinese government to get access to user communications?

Answer: No. Apple has not built a back door for any of our products. Apple has never shown any government any Apple source code beyond that which is available on our website or through open source.

2. Did Apple's decision to move iCloud data for Chinese-registered users to China result in making more data available to the Chinese government?

Answer: No. Users' iCloud data stored in China is encrypted, and the decryption keys remain in the U.S. where they are subject to ECPA. The data Apple moved to China was moved to improve customer usability by reducing network latency.

3. Will the tool that the FBI has asked you to build in San Bernardino work for other iPhone 5Cs? What about for newer phones?

Answer: Had we built the new operating system as requested, we believe it would have worked for any iPhone 5c and, with some modification, for all iOS devices.

4. Is data stored in iCloud encrypted and was it also encrypted before the launch of iOS8?

Answer. Yes, with the exception of email, data stored in iCloud is encrypted, and those protections predate iOS 8.

5. If Apple discovered that the government had a good way to successfully brute-force attack the phone, would Apple try to shut down whatever that method was?

Answer: Whenever we learn of a vulnerability in our products that makes the private information of our users less secure, we fix it. If we deliberately left that vulnerability unaddressed, we would be helping cyber-attackers in their constant and ever more sophisticated efforts to steal information.

6. Can you explain in more detail the arguments you are making in the San Bernardino matter?

Answer: Our argument in that specific case was that the All Writs Act, first enacted in 1789 and on which the government based its entire case, simply does not allow the government to force Apple to create an entirely new

operating system to be loaded on to an iPhone for the purpose of weakening security measures. No court has ever authorized what the government sought, and no law supports such sweeping authority. This was a novel effort to dramatically expand the scope of the All Writs Act.

In addition, the government's assertion that the California case was only about one phone was false. If the government had prevailed in the case, we know that law enforcement agencies across the country and arguably the world would have sought the same outcome. In addition, once an operating system for one phone is created, it would remain a persistent vulnerability for criminals and hackers to use to attack all other iPhones.

Questions for the record from Representative Doug Collins (GA-09)

1. This debate has focused on Apple, but it is important to remember this issue affects not only Apple, but software and technology companies-large and small-across the country, including back home in Georgia.

The President of MotionMobs, an app development company in Georgia, states the problem clearly. While the FBI's request is undoubtedly burdensome for Apple, it is also precedent setting. And for a small company like MotionMobs, the kind of burden posed by the FBI' s request "could lead to bankruptcy." The FBI request also poses intellectual property concerns. It is critical that we take these points into account.

Mr. Sewell, I understand this is an important issue for you, but I'm equally concerned about the smaller companies who don't have your resources. The Justice Department claims that any software company should be able to make changes to their code to allow access to law enforcement. Is that your understanding as well?

> *Answer.* The burden of creating and maintaining reductions in security is one of the critical aspects of this ongoing conversation. Certainly, had the court accepted the government's views on the scope of the All Writs Act, then the government could force any company, regardless of size, to bear the burden of creating new software tools to facilitate access. The inevitable outcome would be one of less innovation and increased litigation, with increased risk to law-abiding customers of any U.S. company's products.

And if they make the change, can defense attorneys force them to appear to explain the changes, or require outside consultants to review their code?

> *Answer.* In the case you describe, we believe that defense attorneys would have the legal right to both examine the methods used to defeat the security in the code and to force company personnel to appear in court. This courtroom engagement alone represents a significant expense of resources for any business, but it would likely be particularly onerous for small entities that may not have in-house legal resources on which to rely.

Does that create IP protection risks? Security risks?

> *Answer.* Yes, the potential security vulnerabilities created by the government's proposed approach would pose huge risks to consumers by making their health information, banking records, location, and other information more accessible to criminals. There are also risks to intellectual property specifically. Businesses rely on products implementing technical measures such as encryption to ensure the integrity and security of the data they hold and transmit. This data often includes protected intellectual

property (IP) and other sensitive information about consumers and businesses across every sector of the economy, including the government itself. A requirement that those security measures be disclosed to defense attorneys and any outside consultants hired by the defense or the courts represent additional vectors for a security breach.

Similarly, the sharing of code to validate the origin of the data presents real conundrums for companies that rely on trade secrets, rather than patents, for IP protection. By disclosing the very specific methodologies used to collect, analyze, and refine the data, software companies could theoretically put the entire value of their product up for scrutiny by an endless stream of defense and court consultants.

Response to Questions for the Record from Susan Landau, Ph.D., Professor of Cybersecurity Policy, Worcester Polytechnic Institute

Questions for the record from Chairman Bob Goodlatte (VA-06)

Responses from Susan Landau, Worcester Polytechnic Institute

1. You suggest in your testimony that "law enforcement must develop the capability for conducting such investigations themselves" and that Congress should provide appropriately funding for that endeavor. So, you do not object to the FBI's recently announced solution that enables access to the San Bernardino terrorist's phone?

Based on what's been publicly disclosed, such a solution is appropriate. There should also be two other aspects to this solution: a policy defining the process to determine when federal investigators should aid state and local law enforcement, who are unable to deploy sufficient resources to conduct such investigations (see response to question 13a) and policies to govern release of information about vulnerabilities to the manufacturers (see response to question 2).

2. At least one commentator has suggested that the FBI should now share its solution with Apple so that Apple can patch that particular vulnerability. Isn't that counterintuitive to your proposed solution to enable FBI to hack into phones without Apple's help. Doesn't it undermine FBI's efforts to share the solution with Apple who will only work to take away FBI's access to patching the vulnerability?

Two fundamental security needs are in conflict. One is the FBI's ability to examine phone contents during the course of an investigation; the other the ability of the phones' owners to secure data on the phones, which is crucial not just for the private information present on phones (such as photos, fitness information, and the like), but also because smartphones are increasingly functioning as security devices (that is, being used as authenticators).

Such conflicting security requirements are hardly new. For decades NSA's Signals Intelligence and Information Assurance Directorates had similar conflicts on precisely the issue of revealing security vulnerabilities in communications infrastructure. In NSA's case, resolutions partially depend on the extent of US reliance on the communications technology discovered to have a security flaw (the Vulnerabilities Equities Process is described at: https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities). Because the vast majority of FBI investigations occur in the US, vulnerabilities used by the Bureau are likely to also be present in devices used by many Americans. Sharing the vulnerability with the manufacturer enables faster patching of all phones with that vulnerability, and is important given the cybersecurity risks currently faced by the U.S.

Were the FBI to share the vulnerability information with Apple, there would be a window of opportunity before the vulnerability was actually patched. During that time, the FBI could continue to use the vulnerability on other phones.

3. Would you say that the work-around solution that FBI has founds is safe in the hands of the FBI?

It appears that the FBI has not learned the details of how the vulnerability works, so yes it is (the Bureau can't reveal information it doesn't know). The fact that the vulnerability exists, however, means that others, including signals intelligence organizations of nation states and organized crime, will look for it, and, with time, undoubtedly find it. This could occur through discovery, or through theft or purchase.

4. Why does it matter whether the FBI possesses the internal capabilities to decrypt a device or communication or the provider possesses it? Wouldn't it be equally vulnerable to cyber hackers and criminals or enemy nations?

By requesting that Apple develop third-party access to a secured device, the FBI was effectively asking to create a weakness in the security system protecting iPhone 5cs. As we learned during the House Judiciary Committee testimony on March 1, had this capability been developed, it would have been frequently used by law enforcement agents around the country. Such routine use would substantively increase the risk that the iPhone security system would be subverted through rogue requests submitted to Apple. (Note that I am not suggesting that law enforcement would be submitting rogue requests. My concern is that other groups, including organized crime and other nations, would subvert the necessarily routine process needed to service the thousands of requests that would come in annually.) The capabilities Apple would have to develop would have increased the risk of insider attack as well as theft of the code from the company.

Were Apple to have developed such software, *all* iPhone 5cs would have been at risk (and perhaps other iPhones as well; that depends on platform-specific architecture). In addition, were Apple to have developed the software to decrypt a device or communication, that capability would be demanded by law enforcement of other nations, including those that fail to respect the rule of law.

5. What recourse does an employer have to get information from either a phone it owns but is used by an employee or a phone owned by an employee for work purposes, especially if all the employee has to do is not backup the phone?

Mobile Device Management systems (MDMs) can be implemented on work phones used by an employee and personal phones used by an employee for work-related tasks. Many vendors support MDM and many enterprises configure it, but it is not automatic; it must be deliberately configured. Use of an MDM arrangement is

elective on the part of the employer, but not all employers implement the system sufficiently well for it to work completely.

There are many types of MDMs offered by a variety of providers, and they function differently. Furthermore, contracts between the employer and user can change, and even a single provider's MDM arrangement can change in the future. Thus it is impossible to give a definitive answer to this question.

A partial answer is supplied by the fact that MDMs typically enable the phone's owner to wipe the phone, which means that a non-compliant employee (e.g., an employee who is not backing up their phone) risks losing all the data on their phone, including personal information stored on the device. This provides a strong incentive for backing up the phone according to the employer's requirements.

6. You have discussed how the Apple iPhone uses hardware encryption embedded on a physical chip. One recent story on Google also suggested that it is reviewing hardware-based encryption stored on individual chips. In layman's terms, can you explain the difference between hardware encryption and software encryption?

For the purpose of this question, "hardware encryption" means the encryption in an isolated piece of hardware (typically a chip). The encryption process and all its data are kept within what NSA calls a ``cryptographic boundary'' that prevents a compromise of the surrounding computer environment, particularly the operating system, from extracting data from the cryptographic processor by any means other than those the processor provides.

The reason that hardware encryption is viewed as potentially more secure than a software solution is that you can reprogram software, but swapping out the hardware is more difficult. And in hardware solutions, part of the key resides in hardware, meaning it cannot be retrieved by software.

7. In your testimony, you suggested that a locked phone can simply be brought into a Wi-Fi network and as long as the passcode and iTunes password match and the phone is charging, then the contents of the phone will sync to the iCloud. Then law enforcement can simply issue a search warrant for the what's in the cloud.

a. Why is the cloud so much more optimal a place for law enforcement to seek communications and associated data?

Data on the iCloud is encrypted by Apple, which holds the decryption key. (While users could encrypt data before saving it in the iCloud, there is no default option to do so—and no way to do it for standard iOS applications.) This means that Apple has the capability to access the data in unencrypted form, and thus so can law enforcement under court order.

b. Is it so much more secure than the phone that it can be both encrypted and accessible at the same time?

As a security measure, the iCloud data is encrypted. However, as noted, the iCloud encryption keys are held by Apple. This means that the data is accessible to Apple in unencrypted form.

If so, why isn't the technology used to run the cloud sufficient to protect the device?

There is a lot of information on phones that is not, and should not, be shared. The usual issue of concern is personal information— photos, private communications, etc. But from a security vantage point, the most important information on a phone is authentication information. Phones are being used to authenticate users to their online accounts of various sorts: email, financial, etc. Such authentication information should not leave the device except when authenticating the user to the account. Any requirement that all data on the phones be shared with a cloud provider would eliminate the ability of phones to serve as secure authenticators.

c. What about a remote-erase command? Wouldn't that kick in as soon as the phone is connected to Wi-Fi and charging?

That command could be disabled on the iCloud end on a per-user basis. This isn't that hard, since it is already possible to do so on a per-phone option.

8. If the forensics community already possesses solutions to accessing the data on an encrypted iPhone, doesn't that mean that even the end-to-end encryption can be circumvented?

Yes, there are many ways that the end-to-end encryption can be circumvented. One way can be because the actual system providing end-to-end encryption has a security flaw that thus enables wiretapping clear text after all. A second way is if wiretapping capability is downloaded on the phone. Even though the conversation itself is encrypted end-to-end, it is available at the phone in unencrypted form. Thus a wiretap on the phone can capture the communications content. Finally, if one has physical possession of the device, it is possible to download a wiretap onto the phone.

It is possible to download a wiretap onto a device through security flaws in either other applications on the phone or the phone's operating system; see my paper with Steven Bellovin, Matt Blaze, and Sandy Clark, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet" http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip. The key issue is that all complex systems, even ones architected to

be secure, contain vulnerabilities. As we all know, hackers, not Apple, ultimately enabled the unlocking of Farook's phone.

And if that's the case, then why should the government look to hackers instead of Apple to unlock the phone?

Hackers and Apple have very different motivations. Hackers who sell vulnerabilities are interested in prolonging the use of a vulnerability, while Apple's interest is in patching the security flaw as quickly as possible. We want to encourage that behavior in Apple—rather than encouraging the company to make poorly secured devices, which would leave the phone open to criminal hackers and spies.

9. If Congress enacts specific legislation to require device manufacturers and app designers to decrypt and unlock their technologies, isn't this incentive for foreign manufacturers to market products with stronger encryption than U.S. products? And couldn't this drive U.S. consumers to those foreign products, thus creating an even greater barrier for U.S. law enforcement?

Yes, and this is a strong argument that such legislation would harm U.S. manufacturers. It would also decrease the ability of U.S. law enforcement to get the information

This aspect of the problem is a replay of the situation in the 1990s and is part of the reason for the loosened export controls that came into play in 2000. Note that it will be impossible to regulate software deployment; we are not going to have US Customs check which apps are on a phone as people enter the United States.

We could regulate hardware by requiring that hardware encryption enable third-party access. But one, there is no simple solution from a technical vantage point (see some of the problems with split keys in response to question 11). And more importantly, weakening hardware security through requiring an access point means that smartphones cannot be trusted as secure authenticators. This would severely limit strong security solutions, *including those used by the US federal government.*

10. Even though the FBI has now been successful in bypassing the auto-erase functions of Farook's iPhone, that does not mean that all of the information stored on the phone will automatically become available to them, correct? Encrypted apps on the phone will still have to be separately accessed?

It depends on how the apps have been designed and whether logging into the phone also logs into the app, or whether a separate login is needed for the application.

11. The Director of the NSA has called for the use of "split keys" as a potential solution. Could you describe in layman's terms what is meant by "split keys" and whether such an option is workable in your opinion?

There are many versions of "split keys," but basically they are solutions in which the encryption key is split in a number of parts, say *n*, and some portion of them, *m*—where *m* can be smaller than *n*—are needed to recover the encrypted information (examples are 2or 3 split keys out of a possible 3; 2, 3, or 4 out of a possible 4; 2, 3, 4, or 5 out of possible 5; etc.).

There are serious problems with such a solution. A solution with few keyholders—a half dozen governments and as many companies—suffers from the "trust" issue; why should one government trust a system in which other governments, but not themselves, hold the keys. But if there are many keyholders—hundreds of governments, thousands of companies—it becomes impossible to secure the keys.

In other words, the split-key solution sounds good in theory, but collapses as soon as one begins to examine the details of how it would actually work in practice.

12. Is it possible for a bad actor to modify encryption or gain access to encryption keys?

Yes. There are many examples of this. The most recent—and very serious—one was a compromise of the Juniper VPN, which was done by replacing a parameter that generates random key bits. This vulnerability allowed attackers to monitor VPN traffic. See "On the Juniper backdoor" by Matt Green, http://blog.cryptographyengineering.com/2015/12/on-juniper-backdoor.html, for details on the attack.

13. You have been critical of solutions that involved updating CALEA because doing so, you argue, would only serve to increase security vulnerabilities. If we rely solely on the FBI's ability to create ad hoc solutions to surveillance or access problems, are we not also ensuring that law enforcement is always playing catch-up with criminals and national security threats when time is of the essence?

As we understand all too well, our society has become remarkably dependent on an insecure electronic communications infrastructure for both the control of critical infrastructure and for conducting business. The latter means not just selling items on eBay, but managing a globalized industrial manufacturing base, just-in-time inventory, remote work, etc. This is the context for the Apple/FBI iPhone case, and for the larger discussion of investigations involving secured electronic communications and devices.

Thus the answer to the question is both yes and no. The FBI needs to develop an investigative center with agents with a deep technical understanding of modern telecommunications technologies which will include capabilities of understanding not only where technology is and will be in six months, but where it may be in two to five years. Sometimes the FBI will be ahead of criminals and national-security threats, but, as the NSA well knows, it cannot always be ahead. Sometimes it will

have to play catch up. One of the important advantages of our highly interconnected electronic world is that even if playing catch up in decrypting texts or opening devices, the FBI will have a wealth of other electronic trails to follow as well.

a. If the FBI can't stay ahead of encryption technology, how do you suggest state and locals have the capability to do so?

State and local investigators already lack the technical expertise to investigate the multiple different types of cellphones, and this will only get worse with time and increasing complexity. Given the myriad number of communications technologies and the rapid rate of their innovation, it makes sense to fund a central source for solutions, and to develop a policy that determines the criteria for sharing those solutions. It will not be possible to develop solutions for all devices and all applications, but making choices about which cases to pursue and what resources to devote to them has always been part of law enforcement's task.

Congress should consider what the appropriate policy mechanism is for determining when to share electronic surveillance technologies; such decisions should not be made by the organization that actually does the work.

14. To pose a hypothetical: What if terrorists are currently planning a 9/11-like attack and storing their plans on encrypted phones? If any of the those phones were to be captured either before or after an attack, do you believe that the manufacturer of those phones should ever have a legal duty to provide the government access to content and metadata stored on the phones?

This hypothetical needs to take into account the various risks facing the US. So the issue is whether it is possible to provide such a capability without simultaneously creating serious holes that others can exploit.

Up until now the capabilities for serious cyberattacks have been limited to nations that have motivations *not* to attack the US in this way. But the situation is changing, and increasingly other nations have developed greater capabilities for cyberattack. With that change, the need to prevent creating serious holes that others can exploit increases.

15. Isn't preventing the United States government from lawfully accessing encrypted communications pursuant to a court order or search warrant based on probable cause fundamentally different than turning over the same information to hostile regimes or those foreign governments that do not respect the rule of law?

Yes, but this phrasing of the question doesn't adequately capture the issues faced by phone manufacturers. While U.S. government access pursuant to a court order is different legally from requirements by hostile regimes or foreign governments that do not respect the rule of law to turn over the same information, its practical consequences are the same. It is much easier for a vendor to say "no" to a totalitarian government if the vendor isn't capable of complying than if they have the capability but do not want to exercise it on that government's behalf.

Response to Questions for the Record from Cyrus R. Vance, Jr., District Attorney, New York County

House Judiciary Committee
Response to Questions for the Record from Chairman Goodlatte
Washington, D.C.

Cyrus R. Vance, Jr., District Attorney, New York County, New York

---

Question 1:

Now that the FBI has found a solution to unlocking the San Bernardino terrorist's iPhone, have you asked the FBI to share their solution with your office?

Response to Question 1:

Yes.

Question 2:

Are you aware whether the solution FBI has found would assist in your own investigations and backlog of phones to search?

Response to Question 2:

The lawful method employed by the FBI to open Syed Farook's iPhone reportedly works on only the particular model and operating system on that phone. Moreover, Apple could alter the operating system so that the FBI's solution would no longer work. Finally, tools of the kind used to open that phone cost far more than most local agencies can afford.

Most local police and prosecutors offices do not have in-house forensics labs. Many state and local law enforcement agencies would be required to send each device to an outside company for forensic analysis and decryption.

Question 3:

Are you also seeking outside assistance in unlocking the phones without Apple's help?

Response to Question 3:

Yes.

Question 4:

How many cases on average do you experience per year where encryption or locked phones prevent your office from accessing necessary investigative information that is likely to yield evidentiary value in solving a crime? What is your oldest case that is now being blocked due to an inability to access content on locked iPhones?

Response to Question 4:

We have been working on this issue since September of 2014 when Apple and Google adopted default device encryption for smartphones. We released a report on Smartphone Encryption and Public Safety in November of last year. As of that paper's release, we had 111 Apple devices that were completely inaccessible. The number of inaccessible phones has risen to approximately 250 devices, out of a total of 853 phones seized by my Office's Cyber Lab between October 2014 and April 2016. Note that these 250 devices are only those obtained by my Office's Cyber Lab in Manhattan; it does not include the number of inaccessible devices seized by the New York City Police Department, or by the District Attorney's Offices of the four other boroughs in New York City.

These 250 devices arise from a wide variety of cases, including murder, sex crimes, child abuse, and complex financial crimes.

Question 5:

What is the effect if Congress were to make a determination that under no circumstances can the government require access or even the mere option to use its own technology to decrypt devices that are previously secured with a passcode or encryption?

Response to Question 5:

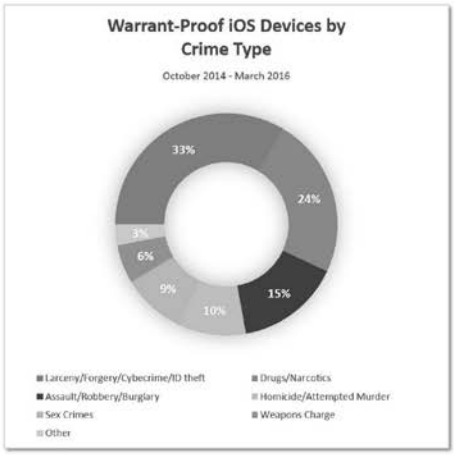
The impact would be felt largely at the state and local level, where 95 percent of criminal prosecutions are handled every year. Because many individuals – including criminals – now live a large part of their lives on smartphones, much critical evidence of crime resides on smartphones, including messages, photos, videos, calendars, and address books. Without smartphone evidence, certain cases will have to be dismissed because prosecutors will not be able to proceed to trial due to a lack of sufficient evidence. In some cases, victims will be waiting for a measure of closure that may never come, and defendants will be free to reoffend. In other cases, prosecutors may be able to obtain a plea to a lesser charge than the top count charged, because without the smartphone evidence, prosecutors will not be able to make the case for the top charge. It is not our position that default device encryption makes it impossible to bring *any* charges against *any* defendants. It does pose a substantial impediment to investigating thoroughly and completely. Plainly said, it affects the process of investigation, exoneration, and prosecution.

Question 6:

In your discussions with other DAs around the country concerning their challenges faced by encryption, have you noticed whether there is any particular crime that seems to be hindered more by encryption than others? For instance, are you noticing gangs using encryption over those exploiting children, or vice-versa?

Response to Question 6:

Affected cases run the gamut from violent crimes such as homicide, to cybercrime and identity theft. This is a breakdown of crime categories corresponding to inaccessible Apple devices received by the Manhattan District Attorney's Office's Cyber Lab from October 2014 to March 2016.



In a series of op-eds and in congressional testimony, we have told a number of stories from across the country – like that of Brittney Mills in Baton Rouge, and Ray Owens in Evanston – whose killers remain on the loose.

Question 7:

Apple has argued publicly that it does not have capability to assist the government with iOS 8 encryption. However, in the Eastern District of New York, Apple is currently contesting an order issued under the "All Writs Act" to assist law enforcement with a cell phone that has iOS 7 encryption, which Apple has the capability to do. If Apple is no longer willing to assist law enforcement when it has the capability to do so, how cooperative can they possibly be when discussing iOS 8, iOS 9, or future operating systems?

Response to Question 7:

This is why our office supports legislative action to require their cooperation when compelled by a court to do so.

Question 8:

You have pointed out that Apple and Google software runs nearly 97 percent of the world's smartphones. These are American-based companies. Have you encountered phones with software other than that of Apple and Google that happened to be encrypted, and if so, do you have any recourse to unlocking or decrypting those phones?

Response to Question 8:

No, all phones in cases currently being prosecuted by my Office are running on either the iOS or Android operating systems.

Question 9:

Are you participating in the FBI-run National Domestic Communications Assistance Center (NDCAC)? Is the NDCAC reviewing any technological solutions to assist law enforcement in gaining access to encrypted communications?

Response to Question 9:

Yes to both questions.

Question 10:

Is it realistic for state and locals to stay in front of technological solutions developed by companies such as Apple in order to remain able to lawfully access necessary communications?

Response to Question 10:

No, we simply do not have the resources. There is a deeply worrisome, inversely proportional relationship: The volume of encrypted devices are at the highest level for state and local enforcement agencies, where resources are at the lowest level.

Question 11:

Do you ever obtain technical assistance from the FBI in accessing communications on phones or computers that you have seized? Are there ever any legal or resource restrictions in preventing you from receiving the necessary technical assistance from

the FBI, particularly any that Congress might be able to solve with legislation or additional funding for the Bureau?

Response to Question 11:

The Manhattan District Attorney's Office has its own High Technical Assistance Unit and performs a wide variety of forensics across multiple device types for our investigations and cases. We have received and continue to receive technical assistance from the Federal Bureau of Investigation. We are not aware of any restrictions imposed by New York law that would prevent the FBI from sharing data with us, although there may be such restrictions imposed by federal law, and the costs of such sharing may, depending on the circumstances, be substantial. Furthermore, if the FBI were to provide technical assistance to us, and we were to rely on that assistance in a proceeding, FBI agents might be called upon to testify about the techniques or methods. This might be costly to the FBI and law enforcement generally.

Question 12:

In your law enforcement career, how would you rank this issue of encryption in terms of complicating investigations?

Response to Question 12:

Apple's introduction of a product that is beyond the reach of a search warrant into the stream of commerce – and marketing that product as warrant-proof – is entirely unprecedented. One of the largest companies in the world intentionally and explicitly frustrating its own ability to comply with court orders is entirely unprecedented.

Question 13:

What are some of the solutions that you are proposing, and do you foresee challenges in implementing them?

Response to Question 13:

We believe federal legislation is the only viable solution. State and local law enforcement does not have the resources of the FBI, and cannot afford to litigate these case by case, and rely on expensive lawful hacking solutions.

My Office — in consultation with cryptologists, technologists and law enforcement partners — has proposed a solution that we believe is both technologically and politically feasible: Keep the operating systems of smartphones encrypted, but still answerable to locally issued search warrants – just as they were until very recently. This can be achieved by a federal statute providing that any smartphone made or sold in the United States must be able to be unlocked — not by the government, but by the designer of the phone's operating system — when the company is served with a valid search warrant.

Our solution, as set forth in our November 2015 Report, is that these companies make their smartphones amenable to search warrants. We want Apple to offer the same strong encryption that it employed without any documented security problems before iOS 8. Previous mobile operating systems allowed the company to access data on a seized device with a valid court order. Apple has never explained why the prior systems lacked security or were vulnerable to hackers, and thus, needed to be changed.

Question 14:

When considering strong encryption without a "key" versus strong encryption with a "key," is it really an either/or proposition?

Response to Question 14:

Neither our proposed solution, nor any pending legislation we support, proposes a government-held key.

Question 15:

Director Comey has said that the FBI is engaging the private sector in discussions about how to best deal with the "going dark" problem. Are you having similar discussions with tech companies? How are those discussions going? Which major service providers are constructively working with you on this issue? Which ones are not?

Response to Question 15:

Neither our Office, nor any state or local law enforcement agency of which we are aware, received any prior warning about Apple's policy change. We read it on the company's website, which stated: "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."

On March 19, 2015, I, along with two members of my Office, two representatives from the United States Secret Service, and two representatives from the Alabama Office of Prosecution Services, participated in separate meetings with senior Apple and Google executives at their respective headquarters in California to discuss this more.

On March 31, 2015, and April 1, 2015, I sent letters to Apple and Google, respectively, setting forth questions that arose from our meetings with them. I have attached a copy of both my letters. (Copies of the letters were also attached as exhibits to my written testimony before your Committee.) I had hoped that the letters would foster a dialogue, but neither company has responded.

Question 16:

Are you aware of providers acquiescing to requests for access from the governments of other countries as a condition of doing business there?

Response to Question 16:

No. However, Apple's Reports on Government Information Requests - which are released every six months – show that it has complied with orders from foreign governments and law enforcement agencies.

It is our understanding that if a foreign nation's government wanted information from an American company, it also would have to go through lawful processes in the U.S., either pursuant to a Mutual Legal Assistance Treaty or a letter rogatory. If the foreign government used the MLAT process, the executive branch of the federal government would decide whether, in its discretion, the foreign government's request was proper. If the foreign government used a letter rogatory, a federal court would make that determination. In either case, the request could be refused if the information was sought for use in a proceeding that would violate human rights.

Question 17:

Don't your investigators use encryption? How do you reconcile the need for your investigators to have access to the strongest of encryption with the need for the general public to have access to the same strong encryption?

Response to Question 17:

We want Apple to offer the same strong encryption that it employed without any documented security problems before iOS 8. Previous mobile operating systems allowed the company to access data on a seized device with a valid court order. Apple has never explained why the prior systems lacked security or were vulnerable to hackers, and thus, needed to be changed.

Question 18:

Under what circumstances can the government compel a person to provide access to their cell phone? Is there a difference between whether a person uses a passcode (such as a four digit number) or biometrics (such as a fingerprint) to "lock" their cell phone?

Response to Question 18:

Case law holds almost universally that a defendant cannot be compelled (by, *e.g.*, a grand jury subpoena or order of the court) to provide the government with her or his passcode,

because such compulsion would violate the defendant's Fifth Amendment right against self-incrimination.[1] There are two potential exceptions to this rule.

First, it is an open question whether, instead of being compelled to provide the government with a passcode, the defendant might be compelled to unlock her or his phone *using* the passcode. There have been no cases considering this precise question, and although a court might conclude that it is no different from the situation in which a defendant is compelled to provide the government with the passcode, it might also determine that the situations are somewhat different.[2]

Second, if the existence of evidence on the phone is a foregone conclusion, then the defendant may have no Fifth Amendment privilege with respect to the contents of the phone, and thus may be compelled to provide the government with the passcode.[3] It would be difficult in most circumstances, however, for the government to establish with the requisite degree of certainty the existence of evidence in a phone that would clear the "foregone conclusion" hurdle.[4]

In any event, even if the government could lawfully compel a defendant to disclose her or his passcode – or to open her or his phone using the passcode – there is a substantial

---

1 The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const., amend. V. The amendment's prohibition against self-incrimination has been "incorporated" so that it applies to state criminal proceedings, as well as federal. *See Malloy v. Hogan*, 378 U.S. 1, 6 (1964); *Griffin v. California*, 380 U.S. 609, 615 (1965). The cases addressing the question whether a defendant may be compelled to provide her or his passcode to the government, and holding that such compulsion would violate the Fifth Amendment include: *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *U.S. v. Kirschner*, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010); *SEC v. Huang*, No. 15-269 (E.D.Pa.) (Sept. 23, 2015) (slip op. at 4-5); *Commonwealth v. Baust*, 89 Va. Cir. 267, 270-71 (Circuit Ct. of the City of Virginia Beach) (Oct. 28, 2014).

2 Professor Orin Kerr has suggested that because it is (or may, in many cases be) a "foregone conclusion" that a person knows the passcode to her or his own smartphone, it would not violate the Fifth Amendment to compel a phone owner to use her or his passcode to open the phone. *See* Kerr, "Apple's Dangerous Game," *The Washington Post*, September 19, 2014 (https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/) (citing *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009)). This may be correct, although it has not been tested in any case. *Boucher* suggests that if the *content* of the smart phone is known (a "foregone conclusion"), then requiring the passcode may not implicate the Fifth Amendment; it does not say that a person's knowledge of her or his passcode would satisfy the foregone conclusion requirement.

3 *See, e.g., People v. Havrish*, 8 NY3d 389, 395 (N.Y. 2007); *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *In re Boucher*, 2009 WL 424718 at *3; *In re Fricosu*, 841 F. Supp.2d 1232, 1237 (D. Colo. 2012).

4 Professor Kerr has also explored the argument that compelling a person to provide her or his password may not violate the Fifth Amendment because the provision of the password may not be incriminating, as that term is by the Supreme Court in cases such as *Hoffman v. U.S.*, 341 U.S. 479 (1951), and *Fischer v. U.S.*, 425 U.S. 391 (1976). *See* Kerr, "A Revised Approach to the Fifth Amendment and Obtaining Passcodes," *The Washington Post*, September 25, 2015 (https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/25/a-revised-approach-to-the-fifth-amendment-and-obtaining-passcodes/). Professor Kerr's analysis may be right, although it does not appear that any courts have adopted it, and therefore there are still questions about the application of the Fifth Amendment to efforts to compel persons to provide their passcodes to the government.

likelihood that any defendant who faces potentially serious criminal charges would simply refuse to comply with the subpoena or order, and go into contempt.[5]

In sum: In almost all cases, it will be legally impossible to compel a defendant to provide his or her passcode or to use the passcode to open her or his phone. In those few cases in which it might be legally possible to compel the defendant to provide the information, it would be impossible as a practical matter to compel a recalcitrant defendant facing serious charges to do so.

Question 19:

When the government takes possession of an iPhone as evidence, what can the government do to get into the phone for evidentiary purposes? What are the limitations? What about an Android phone?

Response to Question 19:

The applicable law enforcement agency may search the device pursuant to a judicially-authorized warrant after establishing probable cause, and subject to the encryption on the device. This applies to all types of devices.

Question 20:

After a serious criminal incident, how does law enforcement access a device (or app) to determine a suspect's contacts with other suspected criminals or co-conspirators? Or determine if another crime is imminent? What privacy or security interests exist in that situation?

Response to Question 20:

As in response to Question 19, in order to examine such evidence, the applicable law enforcement agency may search the device pursuant to a judicially-authorized warrant after establishing probable cause, and subject to the encryption on the device. This probable cause standard has long been recognized by our courts and legislature as the striking the correct balance between privacy and security.

---

[5] *See, e.g., In re Weiss*, 703 F.2d 653, 660-65 (2d. Cir. 1983).

○