GOING DARK: ENCRYPTION, TECHNOLOGY, AND THE BALANCE BETWEEN PUBLIC SAFETY AND PRIVACY

- - -

WEDNESDAY, JULY 8, 2015

United States Senate,

Committee on the Judiciary,

Washington, D.C.

The Committee met, pursuant to notice, at 10:05 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Charles E. Grassley, Chairman of the Committee, presiding.

Present: Senators Grassley, Hatch, Cornyn, Lee, Flake, Perdue, Tillis, Leahy, Feinstein, Schumer, Whitehouse, Klobuchar, Franken, and Blumenthal.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman Grassley. Before I read my statement, I would like to give you a bottom line. One word would be "conversation." Another three words would be "start a conversation." Or if a conversation has already started, then this would be part of continuing a conversation. But it is obviously something that those of us on the Committee feel is an issue that needs to have a little more highlight because it is a very major issue that we have to discuss, and my statement will go into detail.

Today's hearing is intended to start a conversation in

the Senate about whether recent technological changes have upset the balance between public safety and privacy. Just a few days ago, we celebrated the birth of our country. That occasion should serve as a reminder of the gifts bestowed upon us by the Founders, not only the Declaration of Independence adopted July the 4th, but the Constitution that followed it. And the protection of our privacy and civil liberties by the Bill of Rights, more specifically by the Fourth Amendment, provides a useful place to begin our conversation today.

The core of the Fourth Amendment is the requirement that, with limited exceptions, when a law enforcement officer is investigating a crime, the officer must obtain an individual warrant or a court order to conduct a search that would violate a person's reasonable expectation of privacy. And that order must be issued by a neutral and detached judge based on facts that demonstrate probable cause. Through this brilliant framework, for over 200 years now our constitutional system has preserved the rule of law, ensured our public safety is maintained, and protected our individual privacy and civil liberties in part through the separation of powers. But, recently, prominent law enforcement officials have been questioning whether the laws Congress has enacted over the years to adapt that framework to changing technology, such as the Communications

Assistance for Law Enforcement Act--and I will call that "CALEA," as it is known around here--whether or not that is adequate to the task for today.

What they have been telling us is that increasingly, even after they have obtained authority from a judge to conduct a search for evidence of a crime, they lack the technical means to do so. Director Comey and Deputy Attorney General Yates have recently spoken out about this issue, and I have heard about it from State and local officials in my State of Iowa as well. They describe two distinct but related components to the problem.

First, they report a decreasing ability to intercept real-time communications, such as phone calls, e-mails, texts, and other kinds of so-called data in motion.

And, second, they relate a similar concern regarding their inability to execute search warrants on encrypted phones, laptops, and other devices, which store what they refer to as "data at rest."

Companies are increasingly choosing to encrypt these devices in such a way that the company itself is unable to unlock them, even when presented with a lawful search warrant. These encrypted devices, they fear, are becoming the equivalent of closets and safes that can never be opened, even when a judge has expressly authorized a search for evidence inside them. In their view, this development

has the potential to impact the fair and impartial application of our laws by effectively placing certain places, and, therefore, certain people, outside of the law. These officials describe the cumulative effect of these changes on their ability to do their jobs as "Going Dark." It is not a new issue. But according to them, it is a problem that is getting dramatically worse, and it is having a real effect on their ability to protect the public and to bring criminals to justice.

The reason for these sweeping changes is not difficult to understand. Rapidly changing technology has made the way that we store and the way we communicate our personal data quite different than it was, obviously, in 1776--not just that, let alone even 5 or 10 years ago.

Today's revolution then is a technological one. It is a revolution that has resulted in a proliferation of new devices, networks, apps, and other modes of communication. And by leading this revolution, some of our finest American companies are enriching our lives. Through their ingenuity and through their innovation, they are allowing us to be in closer touch with our loved ones, sharing the things important to us in very new ways. However, as more of our lives have ended up on digital platforms, devices, and on the Internet, our data has increasingly become a target for hackers, criminals, and foreign governments.

We pick up the newspaper and read about breaches that have left personal data exposed almost on a daily basis. So we want our data to remain private; we want it to be secure; and it is natural that companies seek to respond to this market demand. But at the same time, these wonderful technologies are also being employed by those who seek to do us great harm.

In particular, Director Comey has talked about the challenges this issue presents the FBI in the national security context. According to the Director, ISIS is recruiting Americans online and then directing them to encrypted communication platforms that are beyond the FBI's ability to monitor, even with a court order. If this is accurate, it obviously represents a dangerous state of affairs.

So then this question: How do we balance the need for both public safety and privacy? Are there ways that we can provide law enforcement judicially sanctioned access to these platforms without compromising their overall security? Or are there other potential reforms that could simply shift the balance less dramatically? These are questions that have right now no easy answers.

I know many in our privacy and technology communities are highly skeptical that any reform can be accomplished without unacceptably undermining both the privacy interests

of our citizens as well as the international competitiveness of our technology companies. These are, no doubt, fundamentally important considerations. But as a start, we need to have an open and honest conversation that examines the costs and benefits both of potential reforms, as well as continuing down the path we are headed. And we need to do so with humility and respect for those who come to the issue from different perspectives.

Last year, the Washington Post ran an editorial on the "Going Dark" issue, describing our time as "an important moment in which technology, privacy, and the rule of law are colliding." Ultimately, the newspaper called for compromise. That is the spirit that the Framers brought to Philadelphia that gave us the Constitution and that eventually produced our Bill of Rights.

Today I hope the Senate takes a first step at seeing if any consensus is possible on this very important issue and a complicated issue.

Without objection, I would like to place into the record a few statements for the record that the Committee has received: one from the National District Attorneys Association, another from the Application Developers Alliance, and a third from the ACLU.

[The statements follow:]

/ COMMITTEE INSERT

Chairman Grassley. Thank you for listening to my long statement, and now Senator Leahy will give his statement.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator Leahy. Thank you very much, Mr. Chairman. Director Comey and Deputy AG Yates, thank you for being here. I also appreciate very much the earlier informative meeting, without going into what was discussed because of the classified nature, that you gave us on this subject. I think those kind of--I might say to the Chairman, as he knows, I used to try to do these similar things. Sometimes those informal meetings are even more productive than the formal ones.

We know how the Internet has transformed the lives of Vermonters and all Americans over the last 20 years. We use it to communicate, make financial transactions; we get our medical records, we file taxes. We store personal information, and I certainly store an awful lot of photographs I have taken, including photographs of both of you.

Critical to the digital revolution has been the development and use of strong encryption. Encryption ensures that if we send or store electronically--and I am thinking now of financial records and medical records and things like that--it is protected against hackers or

criminals or spies. But we also know that it is creating problems for law enforcement.

Two decades ago, during the so-called Crypto Wars, the FBI and others argued that strong encryption prevented investigators from obtaining access to information even when they had a court order.

Well, as one who was a prosecutor, I am sympathetic to these public safety concerns. You can use encryption to impede investigations by Federal, State, and local law enforcement, and I think we have heard from all of them. But as we learned in the 1990s, this--in many ways, it was simpler then, but it was still a complicated issue.

Some have suggested that technology companies should build special law enforcement access into their systems. But let us consider the risks of that approach. Strong encryption has revolutionized the online marketplace. It protects American businesses and consumers from cyber crime, espionage, identity theft, stalking, and other threats on the Internet. And if you undermine encryption, you could make our data more vulnerable.

In the 1990s, I opposed efforts to regulate the development of encryption technology. I was concerned that if you regulated encryption, you are going to stifle innovation, you would harm American businesses, you would impede technological advancement, undercut security, and, of

course, all our competitors worldwide would just go ahead and do it anyway, and we would be left behind.

Fifteen years later, the vast majority of security experts explain that creating special access for law enforcement would still introduce into the digital space significant security weaknesses--at a time when we need the strongest possible cybersecurity. Just yesterday, a group of the world's preeminent computer scientists and security experts released a report concluding that any special access for law enforcement would pose "grave security risks, imperil innovation, and raise thorny issues for human rights and international relations." Last month, nearly 150 security experts, tech companies, and other organizations wrote to the President making similar points, and I would ask consent that these materials be made part of the record.

Chairman Grassley. Without objection.

[The information follows:]

/ COMMITTEE INSERT

Senator Leahy. And even if the U.S. were to take steps to facilitate law enforcement access to encrypted communication, I think we have to ask ourselves how much would it help. You know that strong encryption is still going to be available from foreign providers, although they have their own problems, as this article in the Wall Street Journal yesterday showed, where it says a foreign company, an Italian company, a hacking software firm, was hacked. This was a firm that was supposed to be a specialist in hacking. They themselves got hacked.

But I also want to say that we have to ask ourselves, Do we put American companies in one position and the rest of the world in an entirely different one? Then we lose the edge that we have in innovation today.

I hope when we have some--I think it is important we are having this hearing today, but I hope when we have further hearings, we will have witnesses from the technology industry, which would be directly affected by any effort to regulate encryption. And I would ask that materials from that industry be placed in the record.

Chairman Grassley. Without objection.

[The information follows:]

/ COMMITTEE INSERT

Senator Leahy. But I think we are very fortunate, Mr. Chairman, to have Deputy Attorney General Yates here. It is her first appearance before this Committee since her confirmation. It is always good to see Director Comey, who was in Vermont a couple months ago. The only disadvantage to that, while I have always been used to pictures of me in the paper in Vermont, I was always the tallest one in the room. And they are asking, "Who is the little guy with Director Comey?" when it was in the Vermont press.

Thank you.

Chairman Grassley. I will introduce the witnesses before I administer an oath.

Our first witness is Deputy Attorney General Sally Yates. Ms. Yates was recently sworn into her current position. She previously served as U.S. Attorney for the Northern District of Georgia since 2010. Before that, she was a line prosecutor and supervisor with the U.S. Attorney's Office there, where she led a number of investigations and prosecutions and maybe most famously the prosecution of Olympic Bomber Eric Rudolph. Ms. Yates is from Georgia and received her undergraduate and law degrees from the University of Georgia.

Our second witness is FBI Director James Comey, and I often say how smart he is because he married a girl from Iowa. Mr. Comey took over the leadership of the FBI in

2013. He previously served under President George W. Bush as Deputy Attorney General, U.S. Attorney for the Southern District of New York, and Managing Assistant U.S. Attorney in the Eastern District of Virginia. Between his careers in public service, Mr. Comey was general counsel at Lockheed Martin and worked at a hedge fund. Mr. Comey is from New York, received his undergraduate degree from William and Mary, and went to law school at the University of Chicago.

So I thank both of you for being here, and before we begin, since this is an oversight hearing, I would like to swear you in, if you would. Do you affirm that the testimony you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Ms. Yates. I do.

Mr. Comey. I do.

Chairman Grassley. Thank you.

Ms. Yates, would you proceed, please? And we always have to remind people to turn on their microphones, so I might as well do that now.

STATEMENT OF THE HONORABLE SALLY QUILLIAN YATES, DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Ms. Yates. Well, good morning, Chairman Grassley, Ranking Member Leahy, and members of the Senate Judiciary Committee. Thank you for this opportunity to talk with you this morning about the information and collection problem that we commonly refer to as "Going Dark." I think that Senators Leahy and Grassley's statements this morning really pointed out a number of the difficult issues surrounding this problem.

Twenty-five years ago, I started my career at the Justice Department prosecuting pretty much every kind of case there is, from guns and drugs to financial fraud and terrorism. And during that time, the world has changed in really remarkable ways.

Technological innovations have changed the way that we communicate with our colleagues and our loved ones, and increasingly sophisticated means of encryption have helped to ensure that these communications remain private.

For many reasons, these have been very good developments, and these are developments that the Department of Justice embraces. But it is important that we not let these technological innovations undermine our ability to protect our country from significant national security

threats and from public safety challenges.

The Fourth Amendment of the Constitution and our criminal justice system provide a well-balanced framework for a careful balance between privacy rights and public safety, while adhering to the basic principle of judicial authorization established by probable cause and determined by a neutral judge.

That framework governs searches of everything, including all communications, regardless of whether they are by private letter or smartphone and regardless of whether we are wiretapping a landline or intercepting instant messages over the latest applications.

This framework has protected the interests that we all have in safety and in privacy for many years. But recent technological innovations threaten that careful balance. Although we still have the statutory authorities that Congress provided to us to protect the community, like the Wiretap Act and like FISA, increasingly we are finding that even when we have the authority to search certain types of digital communications, we cannot get the information that we need because encryption has been designed so that the information is only available to the user, and the providers are simply unable to comply with a court order or a warrant.

The need and the justification for the evidence has been established, and yet that evidence cannot be accessed.

Critical information becomes, in effect, warrant-proof. Because of this, we are creating safe zones where dangerous criminals and terrorists can operate and avoid detection. And it impacts us in two ways: We cannot get access to information that is stored on someone's smartphone, like a child pornographer's photographs or a gang member's saved text messages. This is known as "data at rest." And we also at times can no longer effectuate wiretap orders to intercept certain communications as they happen, like ISIL members plotting to carry out an attack in the United States or a kidnapper communicating with co-conspirators. This is known as "data in motion."

These technological changes come with real national security and public safety costs. In just the 6 short months that I have been serving as Deputy Attorney General, I have seen the threat picture from ISIL change. ISIL currently communicates on Twitter, sending communications to thousands of would-be followers right here in our country. When someone responds and the conversations begin, they are then directed to encrypted platforms for further communication. And even with a court order, we cannot see those communications. This is a serious threat, and our inability to access these communications with valid court orders is a real national security problem.

The current public debate about how to strike the

careful balance between private rights and public safety has at times been challenging and highly charged. I believe that we have to protect the privacy of our citizens and the safety of the Internet. But those interests have to be balanced against the risks that we face from creating warrant-proof zones of communication.

There are no easy answers to this dilemma, and reasonable people can disagree on where that balance should be struck. I do not think that we advance the analysis to vilify those who prioritize privacy for their customers. But from where I sit, as Deputy Attorney General, I believe that that balance must be struck in such a way that allows us to continue to enforce court orders to obtain the critical information that we need to combat crime and national security threats.

But regardless of how one believes that that balance should be struck, we can all agree that we need to have ongoing, honest, and informed conversations about how to protect liberty and our security.

I want to thank you again for giving us this opportunity this morning to highlight this growing threat to public safety. We must find a solution to this pressing problem, and we need to find it soon. The Government's ability to protect our Nation from our most significant threats, both foreign and domestic, depends on it.

I look forward to answering your questions.

[The prepared statement of Ms. Yates follows:]

Chairman Grassley. Thank you, Ms. Yates.

Now, Director Comey, thank you.

STATEMENT OF THE HONORABLE JAMES B. COMEY, JR.,
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. Comey. Thank you, Mr. Chairman, Senator Leahy. Senators, it is great to be back before the Committee. Thank you so much for this opportunity. And thank you, Mr. Chairman, for styling this as a conversation.

As Senator Leahy said, I have heard lots of folks refer to what went on 20 years ago as the "Crypto Wars." I am not looking to fight a war. I am not up here trying to win anything. I think the folks involved in this conversation in the private sector and in the Government care about the same things. I care deeply--it is part of my job, it is also part of my life--about security on the Internet. One of our primary responsibilities at the FBI is cybersecurity. Encryption is a great thing. It keeps us all safe. It protects innovation. It protects my children. It protects my health care. It is a great thing.

We also care about public safety. That is what I have devoted my life to. That is what Sally Yates has devoted her life to. I think all Americans care about the same things. There is not a war being fought here. There is, I hope, a conversation among serious people to figure out is there a way to maximize both, to keep ourselves secure on the Internet and, as best we can, to keep ourselves safe in our streets and our communities, because I do believe, as

the Deputy Attorney General has said, we stand at an inflection point. There has always been a crypto discussion, but the world has changed in the last 2 years. Decryption has moved from being something available to something that is the default, both on devices and on data in motion, as you said, Mr. Chairman. We are moving inexorably to a place where all of our lives, all of our papers and effects, all of our communications will be covered by universal strong encryption, and that is a world that in some ways is wonderful and in some ways has serious public safety ramifications. And I hope we can have a conversation about that before we get to that world and people start looking at us and saying, "What do you mean you cannot? What do you mean you cannot do what we pay you to do?"

The ISIL threat I think illustrates the inflection point. As the Deputy Attorney General said, this is not your grandfather's al Qaeda. This is a group of people using social media to reach thousands and thousands of followers, find the ones who might be interested in committing acts of violence, and then moving them to an end-to-end encrypted messaging app. Our job is to look at a haystack the size of this country for needles that are increasingly invisible to us because of end-to-end encryption. This is something we have to talk about as a

people.

The FBI is not some alien force imposed upon the United States. We belong to the American people. The tools we have are only tools given to us by the American people through this Congress. I am finding that the tools we are being asked to use are increasingly ineffective in our national security work and in our criminal work. And I think my job is to tell folks about that so we can talk about it.

I do not come with a solution. This is a really, really hard problem. I hear lots of folks say, "It is too hard, cannot be fixed." And my reaction to that is: "Really?"

I think Silicon Valley is full of folks who, when they stood in their garage years ago were told, "Your dreams are too hard to achieve; it is too hard," thank goodness they did not listen, and they built remarkable things that have changed all our lives. Maybe this is too hard, but given the stakes, given the importance of security on the Internet and public safety for the good folks of this country, we have got to give it a shot. And I do not think it has been given an honest, hard look, which is why I am so grateful for this conversation.

So thank you for this opportunity.

[The prepared statement of Mr. Comey follows:]

Chairman Grassley. Thank you both for your testimony.

Normally we have 7-minute rounds, but we have got two panels, so I think I am going to limit it to 5 minutes unless somebody objects to that.

Director Comey, you have spoken repeatedly about the impact that going dark is a problem and the problem it is having on the FBI's ability to protect the country from terrorism, particularly by Americans recruited by ISIS to carry out attacks here. You have spoken about how your job is to find needles in a haystack and that because of ISIS directing these recruits to encrypted messaging, the needles are now invisible.

You were kind enough to provide a classified briefing for Members of Congress and staff earlier today, but in order to have us have a public debate, the people deserve to hear as much as you can tell them about the issue without compromising anything.

So question: What more can you tell the American people about how the going dark problem is affecting FBI's ability to protect the United States from ISIL and other terrorists?

Mr. Comey. Thank you, Mr. Chairman. I think the American people need to know the terrorism threat today is very different. Al Qaeda, before 9/11 and in the years after 9/11, was focused on the national landmark, multi-

pronged sophisticated attack where they would carefully select operatives, put them in place, train, surveil over many, many months or years.

ISIL is totally different. ISIL is reaching out, primarily through Twitter, to now about 21,000 English language followers. There is a group of tweeters in Syria, and their message is two-pronged: Come to the so-called caliphate and live a life of some sort of glory or something; and if you cannot come, kill somebody where you are, kill somebody in uniform, kill anybody. If you can cut their head off, great. Videotape it, do it, do it, do it. They are pushing this through Twitter. So it is no longer the case that someone who is troubled needs to go find this propaganda and this motivation. It buzzes in their pocket.

So there is a device, almost a devil on their shoulder, all day long saying, "Kill, kill, kill, kill." And if they find someone--and they have found many of those someones in the United States who are interested in this. And we can see Twitter. We will see them give them directions to a mobile messaging app that is end-to-end encrypted and tell them, "Contact me here," and they disappear.

So I have investigations in all 50 States of people who are consuming this stuff. It is buzzing in their pocket all day long, and they are trying to seek meaning in some sick way, and they are responding to this. And then they

disappear and move over to mobile messaging apps. This is an enormous problem. It is very different. Al Qaeda would never vet an operative by tasking them. ISIL says, "Go kill, go kill, and here is a list of military members you can go kill. Go do it."

We are stopping these things so far through tremendous hard work, the use of sources, the use of online undercovers. But it is incredibly difficult. I cannot see me stopping these indefinitely. I am not trying to scare folks. I just want people to know this is a change in my world, in the top responsibility of the FBI, that implicates this going dark problem, they come together. And so I really think we have to talk about it.

Chairman Grassley. Okay. Ms. Yates, the going dark problem is not completely new. In 2012--so you are not responsible for this--there were reports that the FBI and the Department of Justice had settled on legislative proposals to expand CALEA. During an FBI oversight hearing that year, I told Director Mueller that Congress was "waiting patiently for the administration to put forth a proposal" that would address that issue. Such a proposal would have at least moved the debate forward, but here we are in 2015. We are hearing from both you and the Director that this is a major problem.

In January, the President acknowledged that, "The laws

that might have been designed for the traditional wiretap have to be updated." Yet this administration still has not come forward with a legislative proposal.

Question: Is the administration any closer to coming forward with a proposal and a legislative solution to the going dark issue? And then, also, what happened to the proposal from 2012, if you can tell us about that? Obviously, you were not in office then, so go ahead and tell us what you know.

Ms. Yates. Thank you, Mr. Chairman. The approach of the administration is not to try to have a one-size-fits-all legislative solution at this point to essentially cram down the throats of the technology industry. Instead, what we want to do is actually to work with the communications providers to try to figure out a way with them where we can get access to the information that we need through them, while at the same time we are protecting the privacy interests that all of us have, as well as the Internet security interests that we have.

So our goal here is not to mandate a legislative solution that might not be the best way to approach it for these different providers but, rather, to have each provider think about and work out a way where they will be able to respond to lawful court orders.

We are not seeking a front door, back door, or any

other kind of door. We are not seeking for the Government to have direct access to any of these communications. But we are seeking to work with the industry such that they will be able to respond to these valid orders.

Chairman Grassley. So we will not have a legislative proposal. Then let me ask you, along the lines of what you are trying to do is lead by persuasion, is the way I interpret it. Is there a process in place or a target timeline within the administration to reach the end results that you hope to reach?

Ms. Yates. And let me be clear. We are not ruling out a legislative solution if that is ultimately what is necessary. But we think that the more productive way to approach this, the best way to approach it, is to work with the industry to come up with individualized solutions for each particular company rather than a one-size-fits-all solution.

Chairman Grassley. Okay. Senator Leahy?

Senator Leahy. Thank you, and Senator Schumer has asked me to put his statement in the record, so I ask consent that we do that.

Chairman Grassley. Oh, I am sorry. What did you ask?

Senator Leahy. Chuck Schumer wants his statement in the record.

Chairman Grassley. Oh, yes, without objection.

Senator Leahy. Okay.

[The prepared statement of Senator Schumer follows:]

/ COMMITTEE INSERT

Senator Leahy. To sort of follow on what you were just saying with Senator Grassley, that in this case, just as the previous administration talked about and raised, appropriately, the concerns, did not have--the last administration did not have a legislative solution they are proposing, and that is the same situation today. You are raising the problems that are here, but--

Ms. Yates. That is right. We are not suggesting a legislative solution today. That may ultimately be necessary, but we are hopeful that it will not be.

Senator Leahy. Well, and that is very similar to the position of the last administration, and I do not mean that as a criticism of either administration. It is such a complex and moving target. But I think as the Director has pointed out, it is creating increasing problems for the FBI and for other law enforcement. I see District Attorney Vance in the audience and others. It is a problem for all of them.

A group of the world's leading computer scientists issued a report detailing the significant security risk, as they see it, of providing special law enforcement access to encrypted data. That is this report. And they concluded that the security risks are even greater now than they were in the 1990s when we first debated this. The report highlights that the technical challenges have become even

more difficult, and multiple countries seek their own methods of access. We learned what happened with OPM, the hack that affected millions of Federal workers and reduced confidence in the Government being able to protect data. And I know the device encryption presents a different set of security issues.

So would you agree that we have to carefully consider cybersecurity risks in any proposal?

Ms. Yates. Absolutely, Senator. We do have to carefully consider it.

I do want to clarify one thing, though, and that is that we are not seeking special law enforcement access to any information. Instead, what we are seeking is that the individual companies retain some ability to be able to respond to lawful orders. Many of our communications companies, in fact, retain that ability, and they do so with strong encryption. They retain that authority for a variety of reasons. Sometimes it is a business reason because they want to be able to sell ads, for example, to their customers. Sometimes they do it for security reasons because they want to be able to scan for malware. These companies find a way to be able to continue to have access to their customers' information while also providing strong encryption, and so that is what we are seeking--

Senator Leahy. I remember when we had a debate in this

Congress on the illegal sale of content on the various companies that have websites and how upset they were and got everybody all upset that we were somehow delving into their personal information, and so the legislation went nowhere. And then about a week later, it turned out one of the biggest of those companies was data mining their own customers, the sort of things they were warning them about, because they were selling ads.

Incidentally, that report, Mr. Chairman, I would ask that the report be part of the record.

Chairman Grassley. Yes, it will be part of the record, without objection.

[The report follows:]

/ COMMITTEE INSERT

Senator Leahy. I was struck, Director Comey, by your comment about devil on the shoulder, and without going into some of the classified things, not only the briefing this morning but in other briefings I have had, I am struck by so many of these people that have been brought into this network, their age, young people, the same as the horrific case of the young person who murdered the people in Charleston, obviously susceptible from a lot of the websites he read.

But didn't the FBI recommend on its website a series of safety tips for mobile phone users that users could employ encryption to protect the user's personal data in the case of loss or theft? I do not know if that is still on your website, but it was on there originally.

Mr. Comey. I am sure that we did. I hope it is still there. I think encryption for that reason is a very good thing, as I said earlier.

Senator Leahy. And, lastly, I know we are going to have a meeting, Deputy AG Yates. We talked about this briefly as we were leaving the meeting on sentencing reform. Does the Department have a position on the Smarter Sentencing Act and its impact on public safety other than the fact that we are spending about a third of the Department of Justice's budget on running the Bureau of Prisons?

Ms. Yates. Indeed we do have a position, Senator, and that is, we are strongly in favor of the Smarter Sentencing Act. We think it is critical not only to ensure that we are administering justice in a fair and equitable way, but it also is the only thing that makes any fiscal sense going forward.

Senator Leahy. Thank you. As an old trial lawyer, I would not have asked that question if I did not know the answer. Thank you.

Chairman Grassley. And, obviously, I was born at night, but not last night, and I know that question was a reference to me, and I want everybody to know that we are working hard on getting a sentencing reform compromise that we can introduce. And if we do not get one pretty soon, I will probably have my own ideas to put forward.

We will do it in this order: Senator Lee is next, and then Senator Feinstein.

Senator Lee. Thank you very much to both of you for joining us today, and thanks for all you do to keep us safe and to maintain law and order in our country in very difficult times. You both come to us with very impressive credentials and having considered a lot of these issues at great length.

Consumers have, understandably, demanded greater privacy protections, and tech companies have responded to

this by offering very strong encryption in the services that they offer.

There are now concerns regarding law enforcement's access to the data that it needs to disrupt criminal activities and secure convictions. These concerns are, of course, real and complex for reasons that you have outlined. They deserve serious thought, and it is, of course, Congress' job, it is Congress' duty to consider any appropriate solutions.

But I think we should be wary of reaching first for the most blunt and sweeping type of solution. We need to be wary of precipitously adopting the wrong approach.

Some have suggested that Congress should compel tech companies like Apple and Google to create a back door in their encryption walls through which law enforcement could gain passage if it secured an appropriate warrant. Now, that approach, the enactment of a new Federal Government mandate, threatens to undermine consumer choice, weaken American companies, and create a back door for Chinese, Russian, or perhaps other hackers from around the world. At least at this stage, we should be able to do better. So, again, I thank you both for coming to talk to us about these very important questions.

Now, you may be aware that last month the House overwhelmingly approved two amendments to an appropriations

bill that would bar any agency from attempting to mandate that a tech company provide a back door of some kind or another. With such a clear demonstration of political opposition to mandating back doors in mind, what alternative policy proposals have you considered by which Congress could address the so-called going dark concern?

Ms. Yates. First, Senator, we are not seeking a back door, and I understand why that makes people uncomfortable. Consumers have, rightly, demanded that companies be able to provide them with the kind of privacy and security that they need.

What we are seeking is to be able to work with the industry such that the companies themselves will retain an ability to be able to access the information and to provide that information to us with lawful court orders. This is not the situation of the 1990s where it was discussed at that time that the Government actually would retain keys and would have an ability to be able to access consumer information.

What we are talking about is the individual companies, many of which are already doing this right now for their own business purposes or other security purposes, while still maintaining strong encryption. What we are asking is that public safety and national security also be one of the factors that industry considers in determining what type of

encryption to use.

Senator Lee. So you are saying that in some cases the back door that you would want to access through a warrant already exists, the company has the key, it uses it for its own purposes internally?

Ms. Yates. Right. There are a number of the communications companies that do retain the ability to access their customers' information, and they do that with very strong encryption. They value privacy, and they value security as well. And we are able to execute warrants in court orders with those companies. It is the evolution of what they call "end-to-end encryption" where the only person who has access then is the user. And in those relatively rare but critically important instances where we need to be able to get those communications, the only one who can access it is the bad guy, and that creates a very dangerous situation.

Senator Lee. Are there companies with technologies that do not have that kind of capability? In other words, are there companies that don't have access to some devices, even for the company's own purposes, even when it is deemed to be in the interest of the company, who do not have access to whatever is encrypted and is on the device?

Ms. Yates. There has been an evolution--very recently, but there has been an evolution--where, yes, some companies

do not retain access either to data in motion or data at rest. And so what that means, for example, if we were to get some phones, some cell phones, it is essentially a brick to us. We cannot access any of the information on that phone. And that is a problem for a number of reasons. We know pedophiles, for example, those who are exploiting children, maintain their information, maintain the photographs and records of the children they are abusing on their phones. We cannot get that information, we cannot identify other victims, and we cannot identify others who are abusing and exploiting children because we cannot get access to that device. And we cannot get it because the company no longer has access to that device.

Senator Lee. My time has expired, but let me ask just one quick follow-up. As to those companies that do not have a key to the data in motion or the data at rest, either or both, what are you recommending that we do?

Ms. Yates. Well, we are recommending that you engage with the industry, as we are now, to work with them to be able to find a way, some technological way--and as Director Comey was saying, I, too, have a lot of confidence in the minds in Silicon Valley to be able to identify a way for us to be able--in those rare instances to be able to get access to that information through them, not directly but through them.

Chairman Grassley. After Senator Feinstein, it will be Senator Tillis, unless Senator Perdue comes back. Senator Feinstein?

Senator Feinstein. Thanks very much, Mr. Chairman.

Director Comey, I want to start by thanking you and the men and women of the FBI for all the extraordinary efforts that are taking place to keep this country safe. I am aware of what you are doing, and I just want you to know how grateful I believe Americans are for this service. It is not easy, I know, and I also know it is very costly. But I think the activities that are going on are really excellent, and so thank you very, very much.

I would like to read a paragraph from the district attorney of the largest D.A.'s office in America, and, of course, that is Los Angeles. Jackie Lacey writes to this Committee, "While I fully understand and appreciate the tremendous value of privacy, the terrible costs that Apple's and Google's actions will have on State and local law enforcement and on crime victims across the country must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the arms race between criminals and law

enforcement, the criminals will have won."

I actually think she is correct. I think this is a most serious problem, and I myself, who represents Silicon Valley, have tried to interact with them. In May, I met with the general counsels from several of the major Internet and social media companies, to include Google, Facebook, Yahoo, Twitter, and Microsoft. I met in California; also the general counsel from Microsoft came back to meet me here in Washington. And that was to discuss the terrorists' use of their products to recruit, inspire, and direct attacks. And I would like to just tell you what I understand the companies are doing.

Twitter, Facebook, and YouTube all, as I understand it, remove content on their sites that comes to their attention if it violates their terms of service, including terrorism. Those companies actually remove thousands of posts, tweets, and videos every month and take down user accounts. The companies do not proactively monitor their sites to identify such content, nor do they inform the FBI when they identify and remove their content. I believe they should.

So I think, as you have suggested, Director Comey, that there really are grounds to have these discussions and would like to suggest that you pull together the CEOs of these big companies and say directly to them what you have said to us. I have no question from an intelligence point of view

supporting virtually every one of your words. You are absolutely correct, because where we are going is to allow those who would do us enormous harm a respite from any kind of interaction with law enforcement. And that is the black situation that is increasingly existing.

So as you know, I have been very concerned about the proliferation of materials, particularly bomb-making materials, and particularly one of the latest publications which has a recipe for a non-metallic bomb that will go through a magnetometer, which is an actual recipe. It tells people where to sit on a place to have maximum effect. It tells people specific people to go after and kill and which airlines to get on.

Now, the question comes: Should this also be able to be picked up by anyone with a couple of clicks of their computer? It is my understanding that the Boston bombers received their materials on how to build the pressure cooker bomb from one of these manuals. Is that correct?

Mr. Comey. Yes, Senator.

Senator Feinstein. So I think it says a little bit about the depth and size of the problem that we face for civilian law enforcement as well as for any activity that is going to keep this country safe in being able to interdict a possible terrorist threat.

Let me ask a couple of questions. If the FBI was aware

of communications happening on messaging apps, regardless of whether those apps are used on Apple or Android devices, what judicial process is currently available to obtain those communications?

Mr. Comey. Well, in theory, a court order from a judge in a criminal case under Title III or a court order from a judge in a national security intelligence case. But if the data is strongly encrypted, we can collect it, but it will be gobbledygook.

Senator Feinstein. So what you are saying--

Mr. Comey. Strong encryption--

Senator Feinstein. --is you have no recourse--is that right?--if the data is encrypted, currently, for a national security concern, to obtain that data.

Mr. Comey. Right, if we intercept data in motion between two encrypted devices or across an encrypted mobile messaging app, and it is strongly encrypted, we cannot break it. This is sometimes--I hate that I am here saying this, but I actually think the problem is severe enough that I need to let the bad guys know that. That is the risk in what we are talking about here. I am just confirming something for the bad guys. Sometimes people watch TV and think, well, the FBI must have some way to break that strong encryption. We do not, which is why this is such an important issue.

Chairman Grassley. Senator--

Senator Feinstein. Mr. Chairman?

Chairman Grassley. Go ahead.

Senator Feinstein. This is where I think we need to go. I think we need to provide a court-ordered process for obtaining that data.

Chairman Grassley. Senator Tillis, and thank you, Senator.

Senator Feinstein. Thank you.

Senator Tillis. Thank you, Mr. Chairman. Director Comey and Deputy Attorney General Yates, welcome. Thank you both for your service. And, Ms. Yates, congratulations on your confirmation.

I would like to start with you. I think this is a very difficult subject for people watching this hearing or people reading a newspaper to understand what we are talking about. So I would like to start by having you describe--and your opening comments is what prompted me to ask this question. The process that we are talking about going through, I think that many citizens believe that if we had the capability that I agree that we need, we would suddenly be analogous to police cars just riding up and down the road watching every telephone conversation, every text message, every tweet, every Snapchat, and then deciding, well, there is criminal activity there, I have got to go after it.

Could you describe maybe in lay terms the process that you would have to go through to get to the point, to have already identified suspected criminal activity, to get to the point where you would want this capability to go further in your investigation?

Ms. Yates. Sure, and I think one of the things that is important that we do is to identify that we are not seeking any new authority that we do not already have. We already have the authority that we need under the wiretap statute and under FISA. What we do not have now is the capability to be able to execute that authority.

Now, before we can go out and we can get a wiretap, we have to go to a judge, and we have to lay out in great detail the information that we have that establishes that there is probable cause to believe that an individual is involved in criminal activity and that that phone, that device, is being used in furtherance of that criminal activity.

The judge has to review this, determine that he or she agrees with us that probable cause has been established, and then there are very strict rules about how long we can intercept the communications, as well as very strict rules about minimizing our review of any communications that do not relate to that criminal activity.

Senator Tillis. So there is a very specific and

thoughtful process that you go through to get this information, and right now, as Director Comey said, you get it, but it is gobbledygook. It would be analogous to getting some sort of warrant and getting documents that have been all been shredded and pieces deleted, it is unusable. And all you are really looking for is being able to use that information that you have rightfully obtained authority to look at to continue your criminal investigation.

Ms. Yates. That is absolutely right.

Senator Tillis. Okay. Director Comey, you are the first person to give me the chance to use the word "gobbledygook" in a hearing, so I appreciate that. But a question that I had for you really relates to the--when we are talking about intercepting and accessing criminal communications, I think you made a very good point which is also important for Americans to understand. We are fighting a war on terror, and we are fighting--one of the theaters of that war is our homeland. And you mentioned, I think, some 20,000 suspected activities in every State. I know you are trying to intercept and access criminal communications. Is encryption the only impediment that you are facing right now? Or are there other things that we should open this discussion to, to help you be in a better position to do your job?

Mr. Comey. Thank you, Senator. And just to quickly

echo what the Deputy Attorney General said, the design of the Founders is genius for a lot of reasons, but the Fourth Amendment prohibits--it is against the law, folks will go to jail if there are general warrants. If law enforcement is reading everybody's Snapchats or everybody's Instagram posts, you cannot do that. It is particularized based on probable cause. It is a tradeoff inherent in ordered liberty that our Founders came up with. It is genius. It governs my entire life.

With respect to the terrorism threat that we are facing, it is a--actually, I just lost my train of thought, Senator. I threw in the add-on. Can you tell me your question again?

Senator Tillis. It was about other things, other tools that you may want.

Mr. Comey. Thank you.

Senator Tillis. Or need.

Mr. Comey. Sorry for the gobbledygook in my head.

Senator Tillis. It is okay. You scared me. I thought I lost my line of questioning.

Mr. Comey. The encryption is a piece of a broader problem we call "going dark." Sometimes going dark includes just our ability to get companies to comply, who have the capability, to comply with the laws that exist today. That is actually a significant issue we face where folks could do

it but they say, "We are not going to do it." And so we are faced with a dearth of, a lack of enforcement mechanisms.

Then, obviously, locked devices is the one that I think resonates most with ordinary Americans, right? One of your kids disappears, and their cell phone is left behind, and it is one of the new phones that is locked. We will not be able to open it for you to tell you who they were texting with.

I have five kids. That is a big problem. That is a big piece of the going dark problem.

Senator Tillis. Well, thank you, and my time is up. I spent most of my time in the high-tech sector. I share your optimism with our brilliant innovators coming up with a way to do this in a way that I think will actually be a market opportunity for them. But I do wonder, because we are talking about Apple and Google, whether or not to make sure we set standards that there is not going to have to be at some point down the road some legislative standards, because there will be another Google, there will be another Apple, and we need to make sure we are laying the ground work where we are not rethinking this again a year or two from now.

Thank you.

Chairman Grassley. Senator Whitehouse, and then Senator Cornyn.

Senator Whitehouse. Thank you.

Let me just set out kind of a hypothetical case. A girl goes missing. A neighbor reports that they saw her being taken into a van out in front of the house. The police are called. They come to the home. The parents are frantic. The girl's phone is still at home. Before this technology, what would law enforcement have done to help locate that girl that they now cannot do if the phone is encrypted pursuant to these new technologies?

Ms. Yates. Before the evolution of the type of encryption that we are talking about today, the company would have retained access, the ability to be able to open the phone, and so--

Senator Whitehouse. The company would have done that.

Ms. Yates. The company would have. So we would have had to have gotten a warrant for the company to then open the phone--

Senator Whitehouse. The Government would not have. The company would have, and you would have had to get a warrant from a judge in order to access it, but you could.

Ms. Yates. But we could, and that is all we are seeking now is for the company to have the ability to be able to open the phone.

Senator Whitehouse. And they have made the essentially unilateral decision not to--or actually to close off that access, correct?

Ms. Yates. Some companies have, and some still retain that access, yes.

Senator Whitehouse. Mr. Comey, you mentioned that some folks could comply with requests, but they choose not to, some of these companies? Could you elaborate on that? Could you let me know if there is a record that is kept of these declinations by companies to cooperate with law enforcement and if that is a record that we could have access to on the Committee?

Mr. Comey. Senator, I am sure that we have a record of it. I cannot sit here and give you chapter and verse on it, but--

Senator Whitehouse. Let me make that a request for the record then.

Mr. Comey. Sure, and we would be happy to give you that.

Senator Whitehouse. Whatever you have that lets me know how that is happening.

Mr. Comey. Yes.

[The information follows:]

/ COMMITTEE INSERT

Senator Whitehouse. It strikes me that one of the balances that we have in these circumstances where a company may wish to privatize value by saying, gosh, we are secure now, we have got a really good product, you are going to love it, that is to their benefit. But for the family of the girl that disappeared in the van, that is a pretty big cost. And when we see corporations privatizing value and socializing cost so that other people have to bear the cost, one of the ways that we get back to that and try to put some balance into it is through the civil courts, through a liability system. If you are polluter and you are dumping poisonous waste into the water rather than treating it properly, somebody downstream can bring an action and can get damages for the harm that they sustained, can get an order telling you to knock it off. I would be interested in whether or not the Department of Justice has done any analysis as to what role the civil liability system might be playing now to support these companies in drawing the correct balance, or if they have immunized themselves from the cost entirely and are enjoying the benefits. I think in terms of our determination as to what, if anything, we should do, knowing where the Department of Justice believes the civil liability system leaves us might be a helpful piece of information.

So I do not know if you have undertaken that, but if

you have, I would appreciate it if you would share that with us, and if you would consider doing it, I think that might be helpful to us.

Ms. Yates. Certainly, we would be glad to look at that. It is not something that we have done any kind of detailed analysis. We have been working hard on trying to figure out what the solution on the front end might be so that we are not in a situation where there could potentially be corporate liability for the inability to be able to access the device.

Senator Whitehouse. But in terms of just looking at this situation, does it not appear that it looks like a situation where value is being privatized and costs are being socialized under the rest of us?

Ms. Yates. That is certainly one way to look at it, and perhaps the companies have done greater analysis on that than we have. But it is certainly something we can look at.

Senator Whitehouse. All right. Well, thank you, Mr. Chairman. I appreciate this hearing. This is a very important issue, and the people who are going to pay the price, whether it is all of us through a terrorist attack of some kind someday or whether it is just family by family, as law enforcement is crippled in its ability to respond to ongoing dangerous criminal acts, there is a real price to be paid. So there are two sides to this coin that we need to

look at very carefully.

Chairman Grassley. Thank you, Senator Whitehouse.

Now, Senator Cornyn, and then Senator Franken, and then I think it is Senator Hatch.

Senator Cornyn. Thank you to both of you for being here and for your service. This is a very important topic, and I appreciate the spirit in which you have presented this to us. But I do not believe that just because it is hard that that excuses us from using our best efforts to try to find a solution.

Director Comey, I guess there may be some people listening who think that this is a fanciful idea that somehow by encrypting communications between ISIL overseas and Americans here at home, that somehow that will save American lives. But can you state without equivocation that unless we are able to solve this problem, Americans will die?

Mr. Comey. Senator, we are going to do, as we do every day--I do nothing. I lead a remarkable organization. I have a whole lot of people who do a lot every day to do everything they can to make sure that does not happen. So as I said, the tools we are given are the ones the American people give us through you. Whatever we have, we will work 24 hours a day to make sure that does not happen. I just think it would be irresponsible for me not to come to the

Committee and say I see this tool, its effectiveness diminishing steadily, and I can imagine a future where it is useless to me. And I am left having to follow people physically to see if I can tell what is in their head, trying to get undercovers in to talk to them or sources in to talk to them. We will do all of that.

So I do not want to scare people by saying I am certain people will die. What I am certain of is on the current course, current course and speed, my ability to discharge my number one responsibility will be materially diminished in the not-too-distant future. It is being diminished today.

Senator Cornyn. It certainly raises the risk.

Mr. Comey. Yes, it sure does.

Senator Cornyn. I would just like to ask you, in terms of the framework of how we should think about this, if you are a regular American citizen and you are subpoenaed to come into court and you are sworn in by the judge, and you are asked a question, can you refuse to answer the question?

Mr. Comey. You can assert a Fifth Amendment right not to answer the question, and then if--

Senator Cornyn. Well, assuming there is no right against self-incrimination, it is just you are providing information about a crime in which you are not directly implicated, would there be any basis, to your knowledge, for a citizen to refuse to answer the question?

Mr. Comey. No. I think it is what they call "black letter law" that the grand jury is entitled to every man's, every person's evidence.

Senator Cornyn. And if you do not, the judge can hold you in contempt and put you in jail until you do comply with the court's order to answer the question, correct?

Mr. Comey. Yes, sir.

Senator Cornyn. Well, it strikes me that there may be some way of--just trying to think about the framework in which we ought to look at this, it strikes me as irresponsible, and perhaps worse, for a company to intentionally design a product in such a way that it prevents them from complying with a lawful court order, which is what Ms. Yates said you are seeking, a means to allow a response to a lawful court order. If you intentionally design a product in such a way that it prevents you from complying with a lawful court order, it strikes me that it is not a lot different. Maybe that is just food for thought. We ought to let that roll around in our brains awhile and think about that. But I think we need to think about how to think about this and not in sort of any absolutist terms that will result in a higher risk of people being actually successfully targeted by ISIL here in the homeland, and then just responding after the fact, which I know you do not want to do and we do not want to do

either.

Ms. Yates, congratulations again for your confirmation. I just want to ask you on something a little bit different. I see that former Attorney General Eric Holder had suggested that there is a possibility that the Justice Department was entering into negotiations with Edward Snowden for some sort of plea deal. Are you aware of any negotiations on behalf of the United States Government, the Department of Justice, with Mr. Snowden?

Ms. Yates. Having read that same article myself, I believe what Attorney General Holder was saying was that he believed that there could be some deal that was possible. I can tell you it is the position of the Department of Justice that Mr. Snowden needs to return to the United States and face justice.

Senator Cornyn. Well, I appreciate your response. I would just ask, Mr. Chairman, I have a list of a couple of pages of harm resulting from Mr. Snowden's disclosure of classified information that I would like to be made part of the record.

Chairman Grassley. Without objection, it will be made part of the record.

[The information follows:]

/ COMMITTEE INSERT

Senator Cornyn. And based on my reading of the relevant charging documents, statutes, and the United States Sentencing Commission Guidelines, Mr. Snowden should not face any less than 12 to 20 years in Federal prison for his acts of illegally disclosing national defense information. I understand that that is the outward limit, presumably, and that a plea bargain could entail something different. But the idea, as suggested in this article, that he would be subjected to only 3 to 5 years in prison strikes me as insulting and inappropriate. But thank you for your answer, and my time is up.

Chairman Grassley. Senator Franken.

Senator Franken. Thank you, Mr. Chairman, for this very complex problem that we are talking about today. Senator Cornyn, I think you put it very well, which is we need to think about how we think about this.

Deputy Attorney General Yates, some people have characterized this issue as requiring a balance of privacy issues with security issues. But you can also think of it, I think, as involving two kinds of security interests: on the one hand, law enforcement's interest in technologically unfettered access, and, on the other hand, our collective interests in the network and data security that strong encryption provides.

Network and data security protect not only individuals'

personal and financial privacy, but also protect the well-being of our critical infrastructure and the industries that drive our economy. And with each new story about a cyber attack or breaches, Americans learn more about just how significant a security interest that we have in strong encryption.

Before we or a regulatory body could really consider taking any kind of action in this arena, I think we first need to have a similarly clear understanding of the scope and the magnitude of law enforcement's security interest. To this date, we have not seen any real data about how often encryption is thwarting investigations. Can you shed any light on that? And if DOJ does not have numbers to share at this time, is that something that could be studied?

Ms. Yates. Thank you, Senator. And I want to tell you that we are the Department share your desire for strong encryption and share the desire that all of us in this country have for strong encryption.

What we are concerned about, though, is warrant-proof encryption that then elevates the concern for privacy and Internet security over our national security and public safety. We think that national security and public safety are factors that should always be considered in this balancing that we talk about here.

With respect to numbers of cases that were thwarted or

cases that we could not make, you know, it is really hard to prove a negative. For example, we do not go out and seek wiretaps now in applications where we know we are not going to be able to get that information. Preparing a wiretap application is a very time-consuming process, and when we know that that information is encrypted, we simply do not seek that warrant. So being able to give you hard numbers on the number of cases that have been impacted is really impossible for us.

But I can tell you from my experience as U.S. Attorney and the experience that I have now in my capacity as Deputy Attorney General, we are encountering it every day. I remember when I was U.S. Attorney and we would be up on wiretaps, and we would sometimes learn while we are up on a wiretap about a scheme to kill someone. Sometimes it was a witness. Sometimes it was a co-conspirator. Because we were up on that wiretap, we were able to thwart those plots and to stop people from being killed.

Now, with certain communications, we cannot be up on those wiretaps anymore. We do not have the ability to be able to listen and to be able to stop those violent acts from happening.

So I can tell you from personal experience it is happening, and it is happening every day, but we do not really have a mechanism--and I know that is frustrating for

you, but we do not really have a mechanism to be able to give you numbers.

Senator Franken. Right, but can there be--you are saying that there is no way to do a study that would yield any kind of valid numbers because you simply do not try to go after something you cannot go after?

Ms. Yates. Right, we do not go--we do not seek a warrant in a situation where we know we are not going to be able to get the information. We do not seek a wiretap when we know that it is encrypted and we know that we cannot get it.

Senator Franken. Okay. I am trying to talk about how vexing a problem this can be, and so, I mean, you know, when you think about the OPM breach, now that is data that we held, the Government held.

Ms. Yates. Right.

Senator Franken. And so I think that what I was talking about, this being also a security issue, I am just wondering, is there a danger, if we do this wrong, of there also being a national security risk there. That is what I was talking about.

Ms. Yates. I think you are right. If we do this wrong, it could potentially increase the risk, which is one of the reasons why we are not coming to you today with a one-size-fits-all solution, which is one of the reasons why

we really want to work with the industry on a company-by-company basis of what is going to be the best way for them to be able to ensure that their information remains secure, but in those instances where we have a valid court order, that we are able to get the information we need there. I think you are right, we have got to do this the right way.

Senator Franken. Okay. I am out of my time, but thank you, and thank you, Mr. Chairman.

Chairman Grassley. Senator Perdue, are you ready? Or I will call on Senator Hatch.

Senator Perdue. No, sir. I am ready. Thank you.

Chairman Grassley. Go ahead.

Senator Perdue. Good morning. Thank you. I really appreciate the courtesy of giving us a private briefing earlier today. I am so proud that we have people of your caliber in your slots on the wall. I mentioned that to Ms. Yates walking over this morning.

You know, 230 years ago, I do not think James Madison ever envisioned the Internet, but he struggled with this thing that we are struggling with today of the balance between public safety and personal privacy. And I look at the technology being developed, and it seems to be coming at us faster and faster. Here we have apps, we have platforms. This encryption is a very serious thing, and yet 1994 was the last time we had any real legislative adjustment here.

I think that was CALEA. You know, just to put that in perspective, that was when Navigator, Netscape Navigator was introduced in 1994. It was a long time ago. So we know this is a tough question.

Ms. Yates, you obviously have already had some conversation with the industry. I understand the conversation of trying to get everybody engaged. What is your plan relative to the idea of their responsibility as individual corporations versus this idea of public safety? And how do we engage them, with or without legislation?

Ms. Yates. Well, we have been engaging with the industry, and we have been having some productive conversations with individual companies and sometimes with groups in the industry. And, look, the companies are not the villains here. They are responding to market demands, both to protect the privacy of their customers as well as the information security of their customers. And so that is one of the reasons why we think it is so important that we not mandate a solution across the board but, rather, work with them individually, because what works for one company to be able to maintain the security of their information while giving us access when we have a court order might not work for the other.

We have been having some productive discussions. We are certainly hopeful that they will continue those

discussions and that perhaps they will even be more incentivized to be creative and to try to think of ways where they can still protect those really important privacy and security interests while being able to give us the information we need to protect our national security and our public safety.

Senator Perdue. Director, this process that we are talking about here, we know how long it takes to get legislation. When you get involved in an industry that has this many dimensions to it, you have got all these, like you said earlier today, these guys in a garage who have a new app, and there is one coming up every day, it seems. How do we catch up with that from an enforcement point of view and an interdiction perspective? I mean, this prevention is one thing that you guys are doing a great job over the last few years. I know most of that you cannot talk about. But how do you see the timing of this relative to your two responsibilities?

Mr. Comey. Senator, I think that it is, as the Deputy Attorney General said, something that we have to work on urgently. But I also agree it is an unbelievably complicated problem. The proliferation of innovation is a wonderful thing, but it also makes it hard to work with individual players because there is a new garage every single day, and there is a big international component to

this that I get that we have to figure out how to untangle as part of this so we do not hurt American innovation.

But I think the companies are run by good people. When we talk to them, they care about kids; they care about stopping terrorism. They care about the same stuff we do. It is just not their job to articulate the public safety risks here. That is our job. And so one of the reasons we are grateful for this conversation is so someone can articulate we have got a problem and bring the people together to try and solve it. Maybe it will require legislation. Maybe no one will have the incentive to be as creative as they need to be unless you force them to. I do not know. But I do think there is an urgent need to have this conversation.

Senator Perdue. So, real quick, I am almost out of time, but this front-door versus back-door decryption capability, could you speak to that, Director, just a bit, and also the single key versus split key potential? I know we are getting ahead of ourselves, but these are the conversations you are going to be having technically with some of these developers. That, in combination with how do you ever deal with the new encryption apps that would be coming--and these are not companies. These are individuals, and they are in their garages today coming up with the next level of sophistication.

Mr. Comey. The door metaphor throws me a little bit because, as the Deputy Attorney General said, we want people to be in a position to comply with judges' orders in the United States, which is rooted in our Constitution and part of ordered liberty. And so we want them, the creative people, to figure out how to comply with court orders. You should not be looking to the Director of the FBI for innovation. I can do many things well. I cannot think well about stuff like that. I need to tell you there is a problem, and great people need to think about it well and try and solve it.

I get a little bit discouraged when I hear people saying, "Cannot be done. There is only a choice between secure and insecure." And my response to that is, "Really?" I mean, there is no such thing as secure. There is only more secure and less secure.

So my question is: With all of us working together, how could we maximize both? Is it really impossible? Is it really binary? If you do it at all, it is all going to fall apart? I find that hard to believe. I know it was very hard in the 1990s. We have got a lot of smart people out there.

Senator Perdue. Well, thank you again for what you are doing.

Thank you, Mr. Chairman.

Chairman Grassley. Senator Hatch.

Senator Hatch. Well, I want you both to know I have enormous respect for both of you. Let me just say you perform critically important work in safeguarding our country and bringing criminals to justice.

At the same time, however, our constitutional laws recognize the importance of privacy and provide crucial checks on Government's ability to include private affairs. Protecting privacy means more than just preventing improper Government access. In our modern world where so much data is stored online or in electronic devices, it also means securing sensitive personal and financial information from hackers, identity thieves, and other bad actors.

Now, as Chairman of the Senate Republican High-Tech Task Force, I have had numerous conversations with industry leaders about the need for robust data protection. These leaders understand that today's consumers demand secure data and want assurances that their devices will not be hacked.

So, Mr. Comey, with that background, let me begin by asking you about vulnerabilities. If we require companies that produce encrypted software for devices to create so-called keys to unlock encrypted data, how confident are you that hackers will not be able to exploit the vulnerabilities to access sensitive personal and financial data? And doesn't providing a way around encryption expose consumers

to potential theft of personal information?

Mr. Comey. Thank you, Senator. I understand from a lot of people smarter than I that there is risk whenever you try to create and accommodate both strong encryption and the Government's need to have court orders be enforceable, that there is risk. The question is: How much risk? And how do we reduce that risk?

Now, a lot of smart people say you cannot, it is just impossible, and maybe that is where we end up. Maybe we end up in a place where the tools I have have to change in the way they have to change. But I just do not think we have given it the try as a country that it needs to be given.

Senator Hatch. Well, thank you.

Ms. Yates, as a sponsor of the Law Enforcement Access to Data Stored Abroad Act, or LEADS Act, which is currently filed, I am sensitive to the fact that when we require businesses to provide law enforcement access to data both here and abroad, other countries may expect similar access.

Do you have concerns that if we require companies to give us keys to unlock encrypted data, other countries will expect those companies to turn over such keys to them as well?

Ms. Yates. Thank you, Senator. First, we are not going to ask the companies for any keys to the data. Instead, what we are going to ask is that the companies have

an ability to access it and, then with lawful process, we be able to get the information. That is very different from what some other countries, other repressive regimes, from the way that they are trying to get access to the information. I know that there is concern, for example, that if there is an ability here in this country for the companies to be able to access the data, that other countries such as China will require the same thing. But in China and other countries, they do not follow the same lawful process that we do here. And if they did, then they could potentially get the same information. But China's system is not set up that way.

Our companies here make business decisions every day when they do business in repressive regimes about how they are going to operate, and this is really no different than that.

Senator Hatch. Okay. Do you have concerns that if we require companies to give us keys to unlock encrypted data, other countries will expect those companies to turn over keys to them as well? And as you know, many countries have far less robust privacy protections than the United States. I just wondered if you have any concerns there as well.

Ms. Yates. And that is the reason why we are not going to ask for the keys.

Senator Hatch. That is the big reason--

Ms. Yates. It is one of the reasons why we would not ask for the keys, is that the companies would retain the key, and they would simply provide the information to us. We would not have the keys to decrypt data.

Mr. Comey. Senator, could I just add a brief word on that? We are talking about using the United States Constitution, the rule of law, to obtain information in targeted, predicated investigations. If the Chinese are willing to sign up to that, it would be great for the Chinese people, neutral and detached magistrates, showing of probable cause.

So I am not sure I buy the "If we agree to do this within the framework of the United States Constitution, we will have to do whatever the Chinese ask us to do." That does not bowl me over.

Senator Hatch. Okay. Well, we can all agree that we want our technology industry to flourish, and one recent growth area has been apps that allow users to pay online or track their health data. These innovations depend on data security. If consumers know an app or device is vulnerable to hacking, they are not going to use it. Now, I worry that requiring companies to create keys to unlock encrypted data could undermine consumers' confidence in the security of their data and could chill innovation.

Do you share that concern? And if not, why not?

Mr. Comey. I do. I think the Deputy Attorney General does as well, which is why this has to be done very thoughtfully, because there is risk, if you do not do it the right way, that you will damage both, that you will hurt strong information security and you will hurt public safety because you will have hurt the entire Internet, frankly, and all the commerce that flows over it.

Senator Hatch. Well, my time is up, and I want to thank both of you for appearing here today.

Chairman Grassley. Senator Blumenthal, are you ready? If you are not, I will--go ahead then.

Senator Blumenthal. I am, Mr. Chairman. Thanks very much.

There has been some discussion, I know--first of all, thank you both for your great work. I really appreciate your service to our Nation, and on this issue particularly, which is complex and challenging and I think offers no simple or simplistic answers, and I appreciate your addressing it as thoughtfully as you have.

There has been some talk about what other countries do, and put aside China, which obviously has no guarantee and some would say no respect for the kinds of liberties and freedoms that bring us here today, but other countries that also have some respect, whether in Europe. What have other countries done to address this issue and this problem?

Maybe they offer some models or insights for our country. What is your perspective?

Mr. Comey. Thank you, Senator. I think all countries that care about the rule of law are grappling with this right now. I know that the French, in the wake of the Charlie Hebdo killings, passed intelligence legislation that strikes me as fairly sweeping. The Brits are wrestling with this same question right now. I think everybody--we may be--that small group may be a little ahead of where everybody else is, but they are all grappling with this same problem, because they can see both the present and, more importantly, the future that we can see.

Senator Blumenthal. Are they ahead of us, do you think? Are those countries ahead of us?

Mr. Comey. I am not sure that they--perhaps the French legislation is. The British legislation is largely about data retention. But I know also they are considering requiring access to certain communications. So I would say they are probably in about the same place.

Senator Blumenthal. And to what extent do you think the lowest common denominator may dictate what happens either here or elsewhere? Is there that danger?

Mr. Comey. I think America has a unique ability to drive this discussion because we are the source of the innovation, and that is the beauty of this amazing country.

It is here. The providers are here. Most of the clever apps are here. It is all here. So what we do matters enormously, which is why it is so important, as the Deputy Attorney General said, that we get it right, because the rest of the rule-of-law countries, especially our colleagues in Europe, will be strongly influenced by that model.

Senator Blumenthal. We are the source of the innovation, and to some extent, we are also the source of the greatest respect for those rights and liberties--or the most enduring and consistent respect for those rights and liberties. So I think it gives us a special leadership opportunity. I do not know to what extent that is an opportunity vis-a-vis countries like China that are in a different position so far as respect for the rule of law is concerned.

To what extent do you think it would--talking about innovation, would it help to just impose requirements on device manufacturers like Apple? Is that a potential solution?

Ms. Yates. It is certainly a potential solution perhaps down the road, but we do believe that it is important now, rather than seeking a legislative fix that is across the board, that we try to work with the individual companies, because what works for Apple might not be the best solution for another of the communication providers.

And we really think they know their systems best. They know the way they can maximize privacy and Internet security while still being able to comply with lawful court orders.

Senator Blumenthal. Are you satisfied with the degree of cooperation you have received?

Ms. Yates. We always would like more cooperation. We have been having some certainly productive discussions, but given the gravity of this problem and the urgency that we are facing now, I think that it is critical that we kick it up a notch.

Senator Blumenthal. And can we in this body be helpful?

Ms. Yates. Well, certainly to the extent that you can encourage the industry to work with us to try to find a solution that accommodates all of these really critically important interests, I think that would be welcome.

Senator Blumenthal. Well, you have my commitment to do so. My time is up. I cannot speak for the rest of my colleagues, but thank you again for your work on this, and I look forward to continuing this conversation.

Thank you.

Chairman Grassley. Senator Flake?

Senator Flake. Thank you, Mr. Chairman. Thank you for the thoughtful testimony and willingness to come here and speak in a classified setting as well. And I just like

the tone of this discussion because it really is in search of a solution here.

Let me just ask, what are you hearing from the local law enforcement? If that has been covered in previous questions, forgive me. But what is it overwhelmingly that you hear from them?

Mr. Comey. Tremendous concern. I think my colleague and friend Cy Vance, the district attorney in Manhattan, is a very, very thoughtful spokesperson for the view that State and local prosecutors and investigators have. But they are encountering it in data in motion, but actually most urgently in data at rest, stuff that is on a device, because the old days when you do a search warrant pursuant to a judge's order and find paper are almost gone. So they find devices in domestic violence cases, in gang cases, and they are increasingly encountering devices that are encrypted and cannot be unlocked. And I think that is an urgent problem for the bread--"bread and butter" makes it sound like it is not serious--for the ordinary work that is done every day in violent crime cases of all sorts.

Senator Flake. Just following up on that, what is more important, in your view, data at rest or data in motion? Or is one more important in the criminal law context as opposed to the terrorism context than the other?

Mr. Comey. That is a great question, Senator. I guess

my initial reaction is the data at rest is probably more important in the criminal investigations, especially the ones--nearly all investigations and cases are done locally in the United States. I think that is a bigger feature of their lives. In the national security context, especially when we are trying to find needles in a haystack where the communications are coming in motion, it is probably a larger feature for us. That is how I would divide it.

Senator Flake. If we decide, after robust discussion, that there is simply no way to have a front door or a back door, that encryption stands, what will we be forced to do in order to have a better balance between public safety and security? Is it double down in those areas where there is not an expectation of privacy? There are a number of areas that we can surveil. What is the response given that scenario if we do decide that we just cannot go there?

Mr. Comey. That is a really hard one. For example, to answer that on behalf of State and local law enforcement and my criminal investigators, I do not know what the answer is, because the future really is one where all of our papers and effects are covered by strong encryption. So I honestly do not know what we will do there. It may be we will have to evolve some sort of regime where it is easier to compel people to unlock their devices. But that runs into Fifth Amendment problems. So I do not know what the answer is

there.

In terms of our terrorism work, we will, I guess, have to make much more aggressive use of tools that might be able to go through the public part of social media and see what we can find, more aggressive use of undercovers and informants to try and fill that gap. But it is actually hard to sit here and explain to you how I am going to fill that gap, because I do not think I am.

Senator Flake. Well, thank you, Mr. Chairman. I appreciate the testimony and look forward to working through these issues with you. Thank you.

Chairman Grassley. I have one question. And I think Senator Lee and Senator Franken have questions.

Just one question for you, Director Comey. You have talked about how the going dark problem affects your ability to obtain evidence to prosecute. But can you also speak to how the going dark problem impacts law enforcement's ability to exonerate innocent people? Do you have any real-world examples from your experience on the subject?

Mr. Comey. I cannot think of a case off the top of my head. I am sure that we can find one. But the evidence is important both to find the guilty and to clear others who have fallen under suspicion, so logic tells me that in every case where I cannot get access to evidence, I cannot do either of those things. And so someone who the finger is

pointed out we will not be able to clear, just as we will not be able to figure out who the bad guy really is. But I bet we can come and find you cases where devices have been used to say so-and-so was not at the shooting actually, we can prove through texts or something that he was at home with his mother, so he is actually not guilty of this crime.

Chairman Grassley. Senator Lee, then Senator Franken.

Senator Lee. I just wanted to follow up on my prior line of questions. Let us suppose that we had a problem with people storing things in a particular type of safe, a home safety deposit box that had a secure combination lock, perhaps coupled with an iris scanner or something like that. It was made specifically so that nobody else could break into it. You as law enforcement officers wanted to get into it, but you could not without the cooperation of the person who owned it. Once it was programmed to both enter the combination lock and couple that with the iris scanner, no one else could get in. There was no back-door code supplied by the manufacturer.

In that circumstance, how do you think the manufacturer of this safe, this safety deposit box, might react if told or strongly encouraged perhaps by the Government that it needed to provide a back door? And, similarly, how do you think the people who owned those safety deposit boxes would feel upon learning that somebody at the corporate

headquarters or the manufacturer had a back-door method into it and that somebody working there perhaps could take that information with them and sell it to the highest bidder?

Mr. Comey. I think the company would be concerned, and I would hope we would have a conversation where we say, "So who are your customers that they are afraid that a judge will, based on a showing of probable cause, issue a search warrant to be able to get access to that? So who are you marketing this to exactly? And is that really something that caused you the level of concern that it did at first blush?"

And to the customer--first of all, I do not think we have encountered that yet. We would blow that sucker. I mean, we would get that open.

Senator Lee. You would blow it up.

Mr. Comey. You would blow it up. There is not a safe--I do not know of a safe in the world that cannot be opened.

Senator Lee. I guess you could blow up the iPhone, but it would be messy.

Mr. Comey. That would be the end of the data, too. So that is my reaction, which is I think ordinary Americans, when they hear this, think so long as it is pursuant to the Fourth Amendment, it is okay to live in a world where a judge can make a showing of probable cause and issue a warrant to get access to a safe or to a phone. I do not

exactly know where the great demand for this is coming from. I have not met ordinary folks who say, "You know what? I really want a device that cannot be opened, even if an American judge finds that it ought to be opened because it is really important."

Senator Lee. I assume the concern would like with people saying, you know, if one person gets out and there is one encryption key, somebody could break into a whole lot of houses and get a whole lot of valuables that they are not entitled to, and these are not people who are armed with a warrant. That would probably be the concern.

Thank you, Mr. Chairman.

Chairman Grassley. Senator Franken, and then, Senator Tillis, would you signal me if you want a second round? Because--you do not? You do not want a second round, okay. Senator Franken?

Senator Franken. Okay. Just quickly, Director Comey, in your written testimony you spoke about the importance of investing in developing tools, techniques, and capabilities designed to mitigate the increasing technical challenges associated with the "Going Dark" problem." Can you say a bit more about how these tools might function, to what extent you are already investing in these areas, and what kinds of additional resources do your agencies need?

Mr. Comey. Yes, Senator, it is not something I want to

talk about in this forum. I think I have told the bad guys a lot and do not want to go into particulars. But just as we invest in tools that will open safes or allow my Hostage Rescue Team to open a barricaded door to rescue somebody, we try to invest in tools that, if a judge gives us permission, we will be able to open a device or access something. As I said, what I am confirming here is we cannot break strong encryption. We have not found that tool. I do not think it exists. But we look for other ways around the margins, if a judge gives us permission, to be able to get into a room or get into a device.

Senator Franken. Okay. Fair enough.

Deputy Attorney General, I understand why you may not have numbers today when I asked about that. But going forward, could you track the number of times you run into technological obstacles and, therefore, do not seek a warrant or a wiretap? Could you keep track of that so that could inform the scope of this problem?

Ms. Yates. Certainly, Senator, we can work on ways where we try to gather information to be able to answer your question about how big of a problem is this, whether it is numbers or more specific examples to be able to do that, because this is the first time that we have really encountered warrant-free zones. This is new for us. And so we are grappling ourselves with how--not only to get our

arms around the problem, but how to quantify the problem as well.

Senator Franken. Okay. Thank you. Thank you both.

Thank you, Mr. Chairman.

Chairman Grassley. Before you two leave, I think we all thank you very much for continuing this conversation, enhancing the conversation. And since this institution of the Senate speaks with 100 different voices and it kind of gets diluted in the process and this is a very important subject, I would admonish you, because of your particular positions and being a single individual, to enhance the volume on this issue. It is something that is very important that needs to be solved.

Thank you all for coming.

Chairman Grassley. Would the next panel come, please? And before the next panel sits down, I would like to ask for affirmation. I will wait until you get to the table.

[Pause.]

Chairman Grassley. Before I introduce you, do the three of you affirm that the testimony you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. Vance. I do.

Mr. Lin. I do.

Mr. Swire. I do.

Chairman Grassley. Thank you. Now I would like to introduce all three of you before you speak.

Our first witness, Mr. Cyrus R. Vance, Jr., has for the last 5 years served as District Attorney, Borough of Manhattan, New York City. Mr. Vance was previously a lawyer in private practice in New York and Seattle and also served as an Assistant District Attorney, Manhattan District Office. Mr. Vance grew up in New York City, received his undergraduate degree from Yale, and graduated from Georgetown University Law Center.

Dr. Herbert Lin is senior research scholar of cyber policy and security at the Center for International Security and Cooperation and research fellow at Hoover Institution, both at Stanford University. Dr. Lin is also chief

scientist emeritus for the Computer Science and Telecommunications Board at the National Research Council of National Academies where he served 1990 through 2014. Dr. Lin also served as a professional staff member and staff assistant to the House Armed Services Committee. He received his doctorate in physics from MIT.

Finally, Peter Swire is Nancy J. and Lawrence P. Huang Professor of Law and Ethics at Georgia Institute of Technology and a senior counsel at a private law firm. Mr. Swire previously served as President Obama's Review Group on Intelligence and Communications Technology and was Chief Counselor for Privacy in OMB under President Clinton. He is also a senior fellow with Future of Privacy Forum and a policy fellow with the Center for Democracy and Technology. Mr. Swire graduated from Princeton and Yale Law School.

I want to thank all of you for being here today and giving us your opinions and expertise in this area. I will start with Mr. Vance.

STATEMENT OF THE HONORABLE CYRUS R. VANCE, JR., DISTRICT ATTORNEY, NEW YORK COUNTY, NEW YORK, NEW YORK

Mr. Vance. Thank you. Good morning, Chairman Grassley, Ranking Member Leahy, and members of the Judiciary Committee. Thank you very much for the opportunity to testify before you today as the Manhattan District Attorney, but also as a member of the Boards of the National District Attorneys Association and the American Prosecutors Association to give the perspective from local and State law enforcement on these issues.

I am very grateful to be here today because, as my Federal colleagues have indicated in their testimonies, new encryption technology is being introduced, most notably by Apple and Google, which may make it impossible in today's digital world to obtain evidence that is vital for prosecutors. And as the Manhattan District Attorney, I have come to realize in my 5 years that this digital world is, in fact, the 21st century crime scene. And I am here to ask for your help to ensure that law enforcement has lawful access to it.

I would like to address two of the questions, Mr. Chairman, that were alluded to today: How should we balance the benefits, the clear benefits of encryption technology and privacy rights with the responsibilities we have in law

enforcement to protect victims' rights? And, second, who gets to decide that balance?

Now, before September 2014, our investigators could access the relevant contents of a locked iPhone with a search warrant. Today, unless someone knows the pass code of that phone, we cannot. When you consider the use of smartphones by criminals and also by their victims, you begin to understand the profound impact this has on the pursuit of justice for everyday Americans.

Today's criminals, please make no mistake, are taking advantage of developing smartphone technology to commit crimes and to prevent their discovery. They communicate by text. They include their criminal conspirators in their contact lists. They videotape sexual abuses of children and distribute those images to other sex offenders hiding behind the anonymity of the Internet.

It is undisputed that phones are used by criminals committing murders, rapes, and robberies, and most of the thousands of felonies we prosecute each year, and key evidence is on those phones. And at this time, it is unfortunate, but criminals are literally and figuratively laughing in the faces of law enforcement. That is not hyperbole. I would like to give you a real example from a case in my office where a defendant in jail for a felony case is speaking with his friend on a recorded landline

outside of jail. And I am here quoting from the transcript.

"Apple and Google came out with these softwares that can no longer be unencrypted by the police....If our phones are running on the i0[S]8 software, they can't open my phone. This may be another gift from God."

Senators, that is not a gift from God but an unintended gift from two of the largest technology companies in the world. Full-disc encryption upsets the balance between privacy and public safety by allowing criminal activity to thrive in a medium now unavailable to law enforcement.

Apple and Google's decisions in particular to limit our access for the sake of only a marginal increase in privacy comes at a great cost, I believe, a cost that will be borne by the victims of crime and by our society as a whole. And of course, Director Comey and others have alluded to perhaps the most difficult circumstances where this issue may arise. What am I as district attorney to say to the parents of a missing son or daughter when they ask why we cannot access the phone that was left behind, which likely contains information that should lead or could lead to the young person's whereabouts? Is my response to tell them that an upgrade to an operating system stands between law enforcement and finding their child?

Like everyone here, all the prior speakers, I value my privacy. I understand there is a fear of mass security

breaches, collection of bulk data, and warrantless surveillance. And I believe, Mr. Chairman, that those are valid and legitimate concerns. But that is not the access local and State law enforcement seeks or expects. Our access to electronic data is grounded in and it is limited by the Fourth Amendment to our Constitution authorizing only reasonable searches based on probable cause, supported by a particularized search warrant, and only after approval by a neutral judge.

I have also read commentary that suggests we just want solving crimes and prosecuting criminals to be easier, to use this data to create a shortcut toward conviction. Our justice system was not designed, Senators, to make it easy to convict. Proof beyond a reasonable doubt, determined unanimously by 12 jurors, has always been a high bar. We need compelling evidence obtained lawfully, and that is how it should be. But with full-disc encryption, our ability to obtain important evidence and achieve justice for victims of crime is at best curtailed, at worst made impossible.

I, like others, am sure there are technological solutions to this problem. I, like others, have every confidence that the brilliant minds at Apple and Google, working with Federal legislators and considering the interests of victims of crime can figure this out.

As it stands today, Apple and Google have decided who

can access key evidence in criminal investigations. I do not and I cannot believe it is right that they should decide the path toward justice for victims around the country or for our Nation as a whole. I do not think by default we should cede this important decision to the tech industry. Senators, I believe this decision should and must be yours.

Thank you for the opportunity and the honor of addressing you.

[The prepared statement of Mr. Vance follows:]

Chairman Grassley. Thank you, Mr. Vance.

Now, Dr. Lin.

STATEMENT OF HERBERT LIN, PH.D., SENIOR RESEARCH SCHOLAR, CENTER FOR INTERNATIONAL SECURITY AND COOPERATION, RESEARCH FELLOW, HOOVER INSTITUTION, STANFORD UNIVERSITY, STANFORD, CALIFORNIA

Mr. Lin. Mr. Chairman, Senator Franken, members of the Committee, thank you for inviting me to testify today. I have worked on cybersecurity issues for many years, mostly at the National Academies, now at Stanford, but the views I present today are my own.

The previous panel discussed going dark, and I want to address three issues here:

First, the U.S. Government has framed solutions to going dark around what I am going to call the "concept of NOBUS access to encrypted data." NOBUS stands for "nobody but us" where "us" is the Government. This approach has generated polarization around two positions. One side says that NOBUS access inevitably weakens the security of a system and will eventually be compromised by a bad guy; and the other side says the opposite. Neither side can prove its case, and we see kind of a theological clash of absolutes.

To get out of this, I proposed to consider time scale. If it takes 1,000 years for a bad guy to figure out how to hack a NOBUS mechanism, that is probably secure enough. If it takes him 30 seconds, then everyone would agree that

mechanism is probably a bad idea. So somewhere between 30 seconds and 1,000 years, that mechanism changes from being dumb to probably being secure enough.

How do we estimate the time the bad guy needs? Well, we do not understand very well today how to make these estimates for computer systems. But we do know how to use certain methodologies for making such estimates in other domains. For example, an approach called "probabilistic risk analysis" is often used in estimating the time before a nuclear reactor experiences a meltdown. Generally speaking, one estimates the probabilities of various sequences of events that could lead to failure, what is called "fault tree and event tree analysis," and out of that comes an estimate that it will take 10,000 years or a million years, or whatever number you get.

Opponents and proponents of nuclear power use different numbers to make their estimates, but at least they use the same methodology, and they can identify where they disagree technically. That is a much better outcome, in my view, and progress over just shouting at each other over a table saying yes or no.

The most important thing about this approach is that it requires a specific plan, a specific design to analyze. Only when specifics are involved can you actually have a meaningful technical debate.

Would a similar approach work in analyzing a proposed NOBUS mechanism? I think so, but I could be wrong about that. That is what makes it a research problem. We need to assess whether such methodologies can be usefully applied to estimate how long it might take for a bad guy to hack any specific mechanism. But the Government has not provided any specifics, arguing, as we heard in the last panel, that the private sector should do it. At the same time, the vendors are not interested in doing it because they customers are not demanding access. And many of them do not think it is possible to do anyhow.

Without specifics, there is going to be no progress, and I believe that the Government is actually afraid that any specific proposal will be subject to enormous criticism, and that is certainly true. But the Government is the party that wants this kind of access, and rather than running away from such criticism, I think it should embrace any resulting criticism as an opportunity to improve on its initial designs, at least as a proof of principle that it is possible.

Exactly the same issues came up in the 1990s, only then the Government did propose a specific mechanism. When the National Academies studied the problem then, it made a recommendation that still makes sense today: a prerequisite for going down this path is for the Government to gain

experience about how to properly operate a Government-only system allowing such access, before deploying it on a large scale. If you do it without that experience, deploying it on a large scale across the entire Nation is just asking for trouble.

A final point is that asking the major vendors such as Apple and Google to provide NOBUS access is only the first step, as Director Comey implied in his comments about end-to-end encryption in the previous panel.

The next step after that is to impose access requirements on small applications developers and open source developers because they can build apps that bypass any such mechanisms built into the platforms. And then you have to prevent people from bringing into the U.S. apps from abroad that do not have such access, which means you have to build a firewall around the United States that blocks such apps and border inspections and import controls and all sorts of other things that make life very complicated.

Second, a partial alternative to NOBUS access is for law enforcement authorities to obtain legal authorization to take advantage of the vulnerabilities that already exist in all software. With proper legal authorization, law enforcement could hack the devices of bad guys to obtain unencrypted information when the bad guys themselves accessed it, and, of course, law enforcement does this to

some extent today with proper legal authorization.

Third, I want to point out that criminals are just like the rest of us in that they also forget passwords, and if they have not saved them somewhere, certain crimes will not happen because the bad guys will not be able to get at the data that they need to commit them. Also, remember that data is often backed up to the cloud by default. So criminals will want mechanisms that enable them to retrieve inaccessible data, and if they do, that is a way also that law enforcement can gain access.

I hope these comments are helpful, and I am ready to answer questions. I ask that a number of relevant documents that support my testimony be entered into the record. I have already provided these documents to staff.

[The prepared statement of Mr. Lin follows:]

Chairman Grassley. Professor Swire, before you begin, just in case we have a vote in the middle of your comments, I am going to go vote, and Senator Franken is going to stay here, and then he will ask questions. And then when I get back, I will ask questions.

Professor Swire?

STATEMENT OF PETER SWIRE, HUANG PROFESSOR OF LAW AND ETHICS, SCHELLER COLLEGE OF BUSINESS, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GEORGIA

Mr. Swire. Thank you, Chairman Grassley and members of the Committee, for the opportunity to testify today.

As my written testimony discusses, I have worked on encryption issues as a Government official and scholar for two decades. Under President Clinton, when I was Chief Counselor for Privacy at OMB, I chaired the White House Working Group on Encryption for the 1999 change that allows export of strong encryption. As the Chairman also mentioned, I was one of the five members of President Obama's Review Group on Intelligence and Communications Technology and testified before this Committee last year on those issues.

My testimony today is in three parts: the Review Group, the Going Dark argument, and with time available, the harm to U.S. technological leadership that would result from extraordinary access requirements.

First, the Review Group, after top secret briefings on encryption issues, concluded that strong cybersecurity and strong encryption should be vital national priorities. Our Recommendation 29 stated:

"We recommend that, regarding encryption, the U.S. Government should: fully support and not undermine efforts

to create encryption standards; second, we should not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and, third, increase the use of encryption and urge U.S. companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."

And so with full awareness of the going dark concerns, the Review Group, consisting of antiterrorist advisers to Presidents, senior CIA officials, et cetera, sharply criticized any attempt to introduce vulnerabilities into commercially available products and services. We found that these strong encryption policies would best fight cyber crime, improve cybersecurity, build trust in the global communications infrastructure, and promote national security.

Second, law enforcement asserts that it is going dark, but it is more accurate to say--and this has not been the theme today, but I really believe it is true--that we are in a "Golden Age of Surveillance" not darkness. So in detailed writings over a period of years, I have explained why the going dark image is factually inaccurate. Law enforcement has access to growing and unparalleled evidence due to the technological changes in the past 25 years.

Let me emphasize that I agree there are specific ways that law enforcement and national security agencies lose

specific previous capabilities due to changing encryption technology. As electronic communications and evidence evolves, there will indeed be certain categories of information that are no longer available.

Entirely absent from the law enforcement statements, however, is any recognition of the cornucopia of new evidence that our electronic communications provide, and consider three examples.

First, location information. For the first time in human history, most of us carry tracking devices, called "cell phones." And when you add in video surveillance and the upcoming Internet of Things, evidence about a suspect's whereabouts at a time and date is far, far more often available than ever before.

Second, information about confederates and co-conspirators. It is highly useful to law enforcement to know everyone that a suspect is in communication with. With texts, social network posts, e-mails, constant phone calls, and the rest, meta data on communications is available in absolutely unprecedented ways and volumes.

Third, as we all know from our daily lives, our personal information is in an array of other new databases for health care, financial services, online surfing, and everything else. Insights into suspects is further available through big data analytics.

Taken together, consider the evidence-generating machines and practices that fill our daily lives. I have wondered how much of the reduction in crime in the last two decades has been due to the unprecedented records that help law enforcement prove their cases.

Let us look at text messaging as a way to assess going dark versus the Golden Age of Surveillance. Relatively few text messages were sent 20 years ago, if you just think about your own experience. By 2010, the number exceeded 6 trillion per year. For the predominant share of these text messages, the content is available today from the provider. Even for the subset where the content is encrypted, law enforcement can gain access to the meta data linking suspects and witnesses to their entire graphs.

For text messages, it might be tempting to say that law enforcement could call the glass half-empty--some texts are encrypted--or half-full--some texts are in the clear. With over 6 trillion messages filling the glass, though, it takes nerve to say the glass is empty. Text messages are a prime example of a golden age of surveillance, of new, powerful, and pervasive evidence assisting law enforcement and not of going dark.

Chairman Grassley asked whether changing technology is upsetting the balance between public safety and privacy. For reasons stated here, the balance has indeed shifted in

the last 25 years, clearly in the direction of law enforcement having the evidence it never had before in human history.

Because of time, I will not be able to go through some of the ways that U.S. technological leadership would be threatened by having limits on U.S. tech companies. We saw in the 1990s that these limits were imposed on U.S. companies. Russia, Israel, and other countries gained technological advantages from that. It turned out that this was an expensive policy for the economy and also was futile because the bad guys could get strong encryption anyways. That will be true in the future under any of the considered proposals.

Thank you.

[The prepared statement of Mr. Swire follows:]

Senator Franken. I believe, according to my reading of the rules of the Senate, that, Senator Tillis, you are the Chairman of the Committee. Let me explain. I believe that you are in the majority, and by my reading of the rules, the Chair would have to be in the majority. If, however, the--

Senator Tillis. [Presiding.] Well, at the Chair's discretion in honoring what Senator Grassley stipulated, I think he has gone to vote. He will come back and in turn probably ask questions just after you. Senator, Senator Franken, I would defer to you for the first questions.

Senator Franken. Well, thank you, Mr. Chairman. Would it be okay, since I--

Senator Tillis. Would you just say that one more time before I have to step down from the chair?

[Laughter.]

Senator Franken. I know your mom watches these things on the Web.

[Laughter.]

Senator Franken. Certainly, Mr. Chairman, and it is quite an honor to serve with your son--I mean with you.

Let us see what I have here. Dr. Lin, thank you for your testimony. It is clear that this difficult issue is not just about hardware. Director Comey and Deputy Attorney General Yates spoke this morning about the availability and use of end-to-end encrypted messaging apps. Even if all

U.S. device manufacturers agreed to maintain the ability to give the Government access, there would still be developers offering fully encrypted programs or apps, whether authorized or unauthorized.

Can you speak about the kinds of measures you think would be necessary to address this moving target, so to speak? Would we have to dramatically change how we think about Internet governance?

Mr. Lin. It is not so much it governance as the fact that you would have to start imposing requirements on the apps that the American people were allowed to have access to. So, for example, you would start imposing requirements. You would have to say, for example, that no product in the Apple store or in the Google Play store could be marketed without having these exception--these law enforcement access requirements. And then you would have to say then nobody could download an application that was not part of the--that was not in these stores. Then you would have to start inspecting iPhones and Android devices that came in from abroad. When Americans go overseas, they come back. They can download an app overseas, and you have to make sure that that is not there.

So if you are serious about going down this path, the ramifications for product development and use in the United States are enormous.

Senator Franken. And that would affect that industry.

Mr. Lin. It certainly would not do it any good.

Senator Franken. Okay. So it would have a negative effect.

Professor Swire, to maintain our global competitiveness, it is crucial that American tech companies have access to European markets. Given your role years ago in development of the safe harbor agreement to allow data to flow between the EU and the U.S., I imagine you may be uniquely positioned to offer thoughts on the effect of requiring U.S. companies to issue full encryption might have on their ability to compete abroad. What would the ramifications of this be, do you believe?

Mr. Swire. Thank you, Senator. Well, since the Snowden revelations, there has been a number of studies about the economic impact and harm to U.S. sales abroad for cloud and other services. Those numbers are in the hundreds of billions of dollars. Major U.S. companies have had Government contracts canceled in the billions of dollars. And so the view that the United States companies would be cooperating by giving extraordinary access with the U.S. Government is exactly the view that causes the most harm overseas.

The magnitude of this, when you talk to people in the field, has been much greater than people anticipated. It is

continuing, and the encryption debates that are happening now reinforce the tendency in other countries to say stay away from U.S. products.

Senator Franken. And what do you say to Prosecutor Vance or to Director Comey when they say, well, we have got this, these parents have come home, and their daughter was last seen walking into a van, and her cell phone is there, and we want to see who was last in contact with her? What do you say to that?

Mr. Swire. I say there is basically two approaches. You can try to fuzz between them, but one approach is to create extraordinary access with the large costs and the technical problems and the harm to U.S. business overseas, et cetera, and then in some cases they will get information from the phone for the daughter. Or you can have strong cybersecurity as the default with all the benefits that come from that, recognizing that in a very small subset of cases--the Justice Department reports show numbers in the single digits per year or 12 in a year. In a very small number of cases, there will be new obstacles.

We have many new advantages. We will have some new obstacles. But the alternate regime has so many problems with it that have not been fully discussed today that building it is impractical and would be very, very expensive, and I do not think effective.

Senator Franken. Mr. Vance, you look like you wanted to say something.

Mr. Vance. I very much appreciate--

Senator Franken. Turn on your mic.

Mr. Vance. Thank you. I very much appreciate the complexities that have been identified by colleagues on the panel. But I do not believe that--speaking at the national level, unlike at the Federal level, we are actually speaking with instances of crime at scale where the inability to access smartphones and search them has a greater impact in terms of volume.

Senator, more than 90 percent of the crimes committed in America are committed at the local and State level. So I am here speaking on behalf of the 3,000 counties where the impact of Apple and Google's decision is going to be felt most directly. In our written testimony, I have given examples of cases, dramatic cases, where access to the contents of the cell phone through a search warrant were absolutely necessary.

So I do not want the Committee to believe that this is simply a Federal issue, that it deals with a limited number of cases. Indeed, the impact is going to be around the country and at the local level of all the citizens.

So as to what the technological solution is, I, like others here today, do not have it. But I do believe that,

as I said in my testimony, there is an enormous amount of intellectual capacity in not only just the companies who manufacture these goods but also in the academic world and at the Government level. And I do not believe that the option we should pursue when faced today with inaccessibility of access to lock smartphones, which is increasing as more iOS 8 devices come onto the market, is to say from a law enforcement perspective, "I guess that is it, I guess there is nothing we can do." There has to be something we can do.

You asked, Senator, if I can, about statistics. In our office, we started to keep some statistics once the iOS 8--actually, over the 5 years, but since particularly iOS 8 came out, and in that time frame, because we do--we have our own lab at the D.A.'s office in Manhattan because we have so many devices, we cannot always have them done timely by the police. Ninety-two devices came in running iOS 8 that we sought to analyze; 74 of those were locked at an 80-percent rate.

So in our office, in the last 6 months, iOS 8-run devices, 80 percent we were not able to get into because they were locked. Apple--

Senator Franken. So your testimony is quite different from Professor Swire's in terms of the number of cases this would affect, is what you are saying?

Mr. Vance. Well, certainly, if that is my experience in one office in Manhattan, 100,000 cases a year, that is going to be a parallel experience across the country.

Senator Franken. I am sorry, but I have to vote, and so I want to thank you all for your testimony, and I guess we will keep--oh, I know. I am going to recess until they--so I am not adjourning this at all, and I am not--I am going. But in the meantime, talk amongst yourselves. I hope Chairman Grassley will be back, so this Committee will be chaired by a proper member of the majority. But hang on.

[Recess 12:17 p.m. to 12:20 p.m.]

Chairman Grassley. [Presiding.] I hope you can understand that nobody can predict the rudeness of the United States Senate to three people like you that they schedule votes right in the middle of a hearing. I may be the last person you have to deal with. We will wait and see. But if nobody else comes back, then this will be it.

I am going to start with you, Mr. Vance. Some have suggested that law enforcement, being in the midst of the Golden Age of Surveillance, they contend that law enforcement is not going dark because it now has access to meta data, other information. In addition, these people say device encryption is not a problem because law enforcement can focus on obtaining e-mails, text messages, other data stored in the cloud, or even obtain passwords from users

themselves to access devices.

So question: Is meta data a good substitute for the content of communications in your investigation? And are either relying on access to cloud storage or obtaining passwords from users unrealistic options for State and local law enforcement? And your reason why or why not.

Mr. Vance. Thank you, Mr. Chairman.

Mr. Chairman, when you were voting, I made the point--and I would simply like to make it to you now that you are here--that the powerful testimony that we heard from our Federal colleagues is only a small part of the impact that inability to serve search warrants on companies for access to cell phones results in. Ninety-plus percent of the crime in America occurs in jurisdictions like mine, at the State and local level. And that includes in my jurisdiction everything from terrorism but in all jurisdictions rape, robbery, murder, identity theft, and other fraud.

So this discussion has over the last several months been focused upon the NSA and Federal issues. Mr. Chairman, I want you to know that I am here on behalf of district attorneys who have submitted letters for the record from many of the jurisdictions which the Senators here represent as well as prosecutive agencies and victims' groups saying this is very important at the local level and to make that point.

As to a direct answer to your question, it is my observation that the cloud is not the answer to access to information, and that is because, Senator, you may remember from my opening testimony a quote from an individual incarcerated talking to his confederate outside about the fact that Apple has upgraded its system and, if they use iOS 8, the Government cannot get into the phones.

Now, if a run-of-the-mill individual in New York City charged with a crime knows that, I think one can assume that criminals all over the country, if not the world, know that. And the reason that is important is because you can turn off your backup to the cloud with a switch of a button. And if you knew as a criminal whether you were involved in identity theft or scouting locations for homegrown violent extremism, or you were a sexual offender and took photos of young children which you traded peer-to-peer with others, what you would do knowing that if there is no backup to the cloud is turn off your backup and understand that, therefore, in front of you, like with my iPhone, I would have a device that, if it was turned off and locked, no one can open except me. And knowing that people are now taking advantage of that fact, that is what is going to be happening.

Another statistic, Senator, you were out when I gave it: We have started to monitor since September 14 the number of phones that come into our own lab at the D.A.'s

office, and we have to do a part of the forensics for our phones because we have so many. But of the roughly 92 iPhone 8's that came in in that time period, 70-plus of them were locked. And that means of that 70, we were really unable to move toward getting access to the contents. That includes crimes of murder and everything else.

Yes, meta data is helpful. Yes, as the professor indicated, we do have access that we did not have 20 years ago to information that helps us identify and solve crimes. But I think no one should misunderstand that this is not about getting a shortcut to conviction. To prove a criminal case requires convincing proof beyond a reasonable doubt. And I think anybody who is the victim of a crime or who knows someone who is the victim of a crime understands just how hard it is.

So the argument that you do not need the information, you can get it elsewhere, is one that at least from a prosecutor's perspective betrays a certain naivete and ignorance of just how tough it is for police officers and prosecutors to do the job that is expected of them.

Chairman Grassley. Dr. Lin--and then I will have a question for Professor Swire--in your testimony you proposed a method to test the risks associated with providing built-in law enforcement access to encryption. You suggest that this type of risk analysis might help to move the public

debate forward. Yesterday, a group of noted cryptographers and security experts also issued a report opposing law enforcement access to encrypted systems, but also posing certain questions and technological requirements for such a system.

Could you please explain your risk assessment analysis in a little more detail? And what methodology would you use to test law enforcement access to an encrypted system? And do you agree with the question and technology requirements put forward yesterday by other cryptographers and security experts?

Mr. Lin. Thank you, Senator. I have looked at that report, which just came out, as you noted, just came out yesterday, and it is a first-rate report. I would associate myself with most of the commentary in it, especially the call in it for more specifics. One of the problems that the debate to date has suffered from is that there is not a specific proposal on the table, and without that specific proposal, there is nothing to analyze.

So the approach that I am wanting to take is to see--to apply certain methodologies to see how long an exceptional access system, a NOBUS system, could be resistant to a bad guy hacking it, how long it would take. And as I say, if the analysis comes out that it takes 30 seconds, then it is a silly idea, that that mechanism is a silly idea. If it

takes 1,000 years, then maybe that is good enough. And so you want to be able to do the analysis to see where the number comes out.

Now, the problem here--there are two problems with the approach that I am suggesting. One is we do not have a good methodology for doing that, but we have some suggestions that it may be possible. That is a research problem, and I do not know how it will come out.

Even if it is possible, I do not know what the number will be when you actually go through the numbers, what the best credible estimate will be. And it may be that the best credible estimate comes out as, you know, it will last for 2 years, in which case it is probably something that we should not do. I mean, Director Comey alluded to the possibility that maybe it is "impossible." I think that is--what I just said is a more plausible interpretation of what "impossible" means. You know, if it would just last for 2 years without being hacked, then it is probably a bad idea. So that is the sort of thing that I mean.

Chairman Grassley. Okay. Dr. Swire, you recently wrote that, "If there is modest harm and enormous gain to be derived from using certain technology, society should logically adopt that technology."

Continuing to quote, "In 1999, the U.S. Government concluded that strong encryption was precisely that type of

valuable technology. It was worth going at least slightly dark in order to reap the many benefits of effective encryption."

It sounds like you agree with that, as a general matter on this issue, it is appropriate to try to find a balance between law enforcement interests, protecting public safety, and the other important interests at stake. Of course, one of those ways that our legal structure contributes to striking that balance is through the judicial process. In an op-ed to the New York Times back in 2013 about your work on the President's Review Group, you made clear that, "Public officials should not have access to otherwise private information without a court order, with emphasis upon `without a court order.'"

So my only question to you--or I guess really two questions: Do you think that in light of the rise of ISIS and the spread of default encryption, the current status quo strikes the right balance for society? And do you still believe that public officials should be able to gain access to otherwise private information so long as law enforcement has a court order?

Mr. Swire. Thank you, Mr. Chairman. There are a number of questions there. I might speak about court orders and then, very briefly, if I could, comment on Mr. Vance's example.

On the court order point, having court orders is part of the genius of the American system of Government, is part of what this Committee fights to uphold in every era. The question when it comes to technology mandates is what the mandates might be. So we could mandate, for instance--I am not saying it is a proposal--that the recorder on my phone be turned on by default, and then it would only be available with a proper court order, and that way we would have full judicial process, and we would have this wonderful set of information about everything I have said near my phone all along.

In that case, we could have absolutely fabulous court orders, but we might as a society decide we want some things that are not going to be turned on, that we are going to turn that off. And so we should have great judicial process, appropriate process, but we also have to decide when to mandate things technologically, and I think that the weaknesses in encryption are similar in that respect to turning on the recording, their weaknesses that cause more problems than they are worth.

The point to Mr. Vance's very sensible concerns from law enforcement--and as a junior lawyer, I worked in the Manhattan D.A.'s office. I have great respect for the history of that office and all that it does. I think in terms of meta data helping, one thing meta data helps is to

reveal co-conspirators, who is everybody you called and texted and e-mailed. In the old days, if you turned one co-conspirator in a criminal investigation, maybe you could get him to testify. But today, if you have a co-conspirator, you can give that person use immunity and compel them on pain of jail time to open up their phone for you, and then all the contents of everything they said to the main suspect are there plain for you to see.

There is a much more complicated set of techniques for finding out how to get this information than the debate has often said, and so realizing the full range of capabilities that law enforcement has should be part of the debate as well.

Mr. Vance. Senator, thank you. I did not know you had worked at the Manhattan D.A.'s office, but it is so nice to know that.

If I may--

Chairman Grassley. Go ahead, and then I will call on Senator Whitehouse.

Mr. Vance. Actually it is a case that we spoke about with Federal colleagues. There are individuals who maintain content on their phone that is so incriminating and disturbing that, if given the option between an order by the court to--an order including immunity, some kind of immunity, use immunity to open the phone or contempt, the

choice would be not to open the phone, number one.

Secondly, in New York State courts, at least, in the investigative level, we have transactional immunity as opposed to use immunity, which the Federal Government has. And transactional immunity means that if you provide testimony to a grand jury, not just that your words or what comes out of your mouth cannot be used at a future proceeding, but you are given an immunity bath about anything about which you testified. So the professor's suggestion about ordering immunity in exchange for something, in our courts would mean a person could commit crimes and simply be immune from prosecution altogether.

And, Senator, the last thing I would like to say is that there is a question that really I would hope the Committee would ask. When we traveled to Apple last March to talk with them about these issues, the question that we had for them, which has yet to be answered, is: What was wrong, what was insecure, what evidence of bad things happening took place under iOS 7 that changed when it became iOS 8? I am not aware--at least I am not aware of that the Apple iPhones were insecure or that there were breaches as a result of the iOS 7 software, certainly as it pertained to access to the device itself.

Now, there are a lot of doomsday scenarios that are being portrayed about hacking, and I think all those should

be taken seriously. But it has yet to be identified what exactly was insecure about iOS 7 when in that format the Government--the company maintained a digital key as well as the user.

Chairman Grassley. If it is okay with Senator Whitehouse, I am going to turn it over to you, and would you adjourn the meeting when you are done asking your questions?

Senator Whitehouse. Once I have grilled the witnesses mercilessly for vast amounts of time?

Chairman Grassley. And can I also, since I will be leaving for a 12:30 meeting, could I say thank you to all of you. And I suggested to the previous panel that we are continuing and enhancing a discussion in this area, and I am sure that you folks will feel free and want to and so you know we are open to it to continue your discussion with us and also to promote your points of view to maybe help us reach a point here where we find some effective process or compromise.

Senator Whitehouse?

Senator Whitehouse. [Presiding.] Thank you very much, Chairman Grassley. Let me welcome District Attorney Vance particularly here. I appreciate how busy the Manhattan D.A. is, and clearly it is a key matter for you when you have taken the trouble to prepare your testimony and come down here, and I appreciate it.

I know also you have been trying to work with the tech sector to try to get some common understandings. How would you describe the nature and direction of those conversations?

Mr. Vance. Senator, they are summarized in two letters appended to our written this: a letter to the general counsel of Google and to, I think, the chief legal officer at Apple. I traveled last March to both companies to try to better understand their perspective and for them to understand ours. So I believe that we had cordial and interesting meetings, but I was left at the end of those meetings with some important questions unanswered, and because of that, I wrote letters to both individuals asking for answers to those questions. And as I say, those letters are attached to my exhibit.

Answers to questions we do not have, Senator, are: What exactly was the vulnerability of devices under iOS 7 versus iOS 8?

Senator Whitehouse. One is dated March 31st of this year; the other is dated April 1st, the following day, of this year. Have either been answered?

Mr. Vance. To date, they have not been answered, and the question I asked to both, and I am quoting from the letter: If Google kept a key so that it was able to unlock phones, would the phones be more vulnerable to hackers than

if Google had no structure key? Is there a key or similar device that Google might keep without sacrificing the security of Android devices from hackers? Is there a way to measure or quantify the vulnerability of hackers of Android phones, A, if Google kept a key as compared to, B, if it did not keep a key? And then, Senator, respectfully, I think are the questions that need to be answered in order to have an accurate assessment about industry's claim that they are going to be made unduly vulnerable and law enforcement's desire to gain access to evidence.

Senator Whitehouse. When they do answer, may I ask you to send a copy of their answers to the Chairman and the Ranking Member so that they can be distributed to the Committee? The record of this particular hearing may well have closed, as it only lasts for 1 week, so good luck. But if it does not come in in a week, if you could send it to Chairman Grassley and Ranking Member Leahy, then the Committee can distribute it to those of us who are interested in their responses. I would appreciate that if you would do so.

Mr. Vance. Thank you.

Senator Whitehouse. You also run an office that has an unusually wide array of offenses that you prosecute, everything from very simple low-level street crime to very significant financial fraud to national security

investigations. Clearly, you have mentioned a couple of things. You have mentioned time-sensitive investigations, a kidnapping or a child snatching where you need quick access to all the information you can. You have mentioned investigations where the content itself on the phone is criminal--pictures of child abuse and so forth. And I know you have a vivid concern about national security.

Could you just put for the record a little bit of context about any particular cases or types of cases that you could describe so that people who are not prosecutors on this Committee have a sense of how this plays out in the public safety responsibilities that you bear in those areas?

Mr. Vance. I would be delighted to, Senator, and let me give you first an example of where the ability to open the phone itself was critical to obtaining justice in a serious case.

In 2012 in our office, there was a murder. The murder was committed by a gunman who went into a room where a number of men were seated around, completely legally having a conversation, and one of the men in the room had his iPhone and was taping his friends as they were joking around and talking.

When the door knock was heard, the young man with the phone, a father of two, turned his phone to the door, and in the door you could see on the iPhone a picture of a man with

a gun. The man filming was shot and killed by the man with the gun whose picture is on the iPhone video. The iPhone video drops, the phone drops, and recorded the voice of the shooter threatening everyone in the room what he will do to them if they go to police. iOS 6. If that had been iOS 8, when that phone had dropped, the pass code to the phone would have died with its user. We would not have been able to obtain the actual killing itself memorialized on a video on the phone. We were able in that instance to obtain it, and he was sentenced to 35 years to life after he was successfully prosecuted.

In Evanston, Illinois, today, in Cook County, where people are very concerned about gun violence--and Anita Alvarez, the D.A. there, who wrote a letter of support to this Committee--in early December, a young father of six was murdered at gunpoint in the early morning hours. There was no surveillance video. There were no external ways that one could prove who came and who went. And we also were--those prosecutors sent a search warrant and opening order to Apple and Google, and because those devices are operating--those phones that were recovered beside the victim were incapable of being opened under the 15 technology, police and prosecutors are not able to gain access to those phones, and that homicide remains unsolved, the killer remained unapprehended.

There are many, many, many, Senator, more instances that I could go to. We have included a number in our materials. But one example I gave you shows how, if we had not had the ability to access the phone, we would not have been able to prosecute a murder case, and another one shows that today, with this new encryption technology, we are not able to get into the phone and obtain evidence which may well lead to understand who murdered the father of six.

This is the State court experience every day in 3,000 counties around the country. I have always thought it was ironic, personally, that the victims, the true victims of this security upgrade preventing search warrants to be executed on phones, the true victims are going to include the customers of Apple and Google themselves who are going to be victims of crime and are going to be unable to have law enforcement access to phones of the conspirators that would prove they are the victims of crime. And at the end of the day, Senator, I think this is a matter of such significance that it is a policy question which has to be decided by you, the lawmaker. It should not be, in my opinion, up to industry to say this is where we draw the line on access to information which we know may be critical not just on national security but on protecting our citizens in every city and town across the country.

Senator Whitehouse. And I would add particularly if

they have no liability for what goes wrong and only the benefit for being able to market this technology.

Mr. Lin, I think Senator Klobuchar is going to be joining us, so I am going to take a little bit of extra time here. You used the term "NOBUS access," which is not a term I have heard before. The access that I think we are talking about here is an access that the company maintains, the service provider maintains, and until recently, always has, and then the operation of law under the Fourth Amendment to get a warrant and secure the information that is held by the company.

Does NOBUS mean something different than what I just described?

Mr. Lin. Sir, it depends on the context. If you imagine a company that for its own business reasons has decided never to provide key recovery or backup and so on to market that service, then NOBUS access is what--basically it says that the company itself does not have access, and then law enforcement, the U.S. Government, does have access to it under some means. And--

Senator Whitehouse. But that is not what anybody is asking for here. What we are asking for, at least to the extent that there is an ask on the table to be debated, is that there be a mechanism that has been the case heretofore where the company itself maintains access to the information

and then yields it only when a judge has signed a search warrant that allows that information to be shared with law enforcement because law enforcement has proven probable cause that evidence of a crime is contained in that information.

Mr. Lin. But under the circumstances you describe, the only purpose of asking the company to--of requiring the company to do it is, in fact, to provide Government access. That is the scenario that you just proposed.

Senator Whitehouse. Yes.

Mr. Lin. And so effectively it does count, because the company itself by assumption has no reason to want to get to its data.

Senator Whitehouse. Well, they may have a reason to want to get to their data if they have an interest in helping law enforcement fight either terrorism or crimes in which the content is itself contraband, criminal content--

Mr. Lin. Fair enough.

Senator Whitehouse. --for and which there is an emergency with a family member lost and you need access to it. That is not a goal that a corporation necessarily would take no interest in, and I suspect if there were a civil liability component so that they own both sides of the risk equation, they might pretty quickly decide that this was a piece of the social safety net that protects all of us that

is worth preserving. So--

Mr. Lin. Sir, with the--

Senator Whitehouse. It would be their decision to make, of course, but I think it is not without meaning or value to a company to maintain that, and heretofore they have for a variety of other billing reasons and business reasons.

Mr. Lin. Well, I agree with you that if the world were adjusted in such a way that they did have liability, the business interests change. And I think that is what you are proposing, and I think--

Senator Whitehouse. Well, thinking about, anyway. I do not want to say I am proposing. If I were to propose it, you would see a bill. All I observe is that there is an imbalance in which the companies get the reputational and business value of being able to market their product as super-encrypted and unbreakable, but have none of the costs that society bears once evil people decide that they are going to take advantage of that technology and law enforcement remedies such as District Attorney Vance has elucidated are taken away by their technology.

Mr. Lin. I love it as a research problem, and I am going to try to find some students who are going to work on it with me. The idea that you propose is not one that I have heard prominently in this debate, and it is a new idea,

and--

Senator Whitehouse. It is actually a really old idea. It goes all the way back to the earliest founding of the country where the Founding Fathers fought to have civil juries because they were worried that politicians might screw things up if there was no test where, back then 12 good men and true, now 12 good people and true could make a decision about who was responsible for what kind of misconduct.

Mr. Lin. The idea is new to this debate, and I commend you for--you know, thank you for introducing that into this debate. It is worth studying.

Senator Whitehouse. Okay. I do not have confirmation Senator Klobuchar is actually on her way, so rather than run the proceedings out further, I will ask District Attorney Vance if he has any closing comments, and then close the hearing.

Mr. Vance. Senator, I just thank you and all the Committee for inviting me and us here today. I understand that I must make a formal request to put letters that have come in to the Committee from victims' groups and law enforcement and have those--

Senator Whitehouse. Without objection, the letters that you propose to us, as long as you get them into us within the week that the hearing is open, will be added to

the record of the hearing.

[The letters follows:]

/ COMMITTEE INSERT

Senator Whitehouse. And thank you in turn for agreeing to provide the responses from the technology companies to the Chairman and to the Ranking Member whenever they come in. And, indeed, here is Senator Klobuchar. Your timing is perfect. I was just about to give up, but here you are.

So I will turn the gavel over to Senator Klobuchar since it has been turned over to me, and all the mundane business of closing out the record and all that sort of stuff has been taken care of. So you have the floor. You have your questions, and you have your panel, and I yield.

Senator Klobuchar. [Presiding.] Okay. Thank you very much. Sorry I was late. We were at the White House--always a good excuse--trying to save the Ex-Im Bank. So I appreciate you guys still hanging around here after a long hearing.

I was here for the first hour of the testimony of the Deputy Attorney General and the FBI Director, and so I thought I would follow up on one question I was actually going to ask them, which was Apple's announcement with their new system last fall included a specific reference to the fact that the company could not circumvent encryption to assist law enforcement. It said, "Unlike our competitors, Apple cannot bypass your pass code and, therefore, cannot access this data. So it is not technically feasible for us to respond to Government warrants for the extraction of the

data from devices in their possession."

So I want to know if you are concerned about this kind of messaging sending a signal to consumers and other companies that they should be seeking encryption that prevents legitimate law enforcement access. I guess I would start with you, Mr. Vance. Thank you for your work also.

Mr. Vance. Thank you. I know as a former prosecutor you understand it very well.

Senator, first of all, like so many people here, I am an Apple/Google fan. I want to put that on the record. I wrote my remarks on an Apple laptop using Google Docs. So I understand the value of what they do. But I was very concerned when the iOS 8 came out and that marketing language was included on Apple's website. I think it does send a signal--it certainly sent a signal to me in law enforcement, and, by the way, I am not aware that Apple or Google had any dialogue with law enforcement whatsoever before it conducted this upgrade to assess its potential impact. But I was concerned. I addressed that concern to them directly when I traveled earlier this year, in March, to speak with them. I communicated it, and I do not believe that my conversations were enough to convince them to return to the status pre-iOS 8, which is really what ultimately I think was working. We had a system where, prior to September of 2014, where I am not sure exactly what the risk

was that was causing so much trouble. Apple has not identified how its phones were at risk on September 13th of 2014, but no longer at risk on September 17th of 2014. And part of the problem is you cannot get into the box. You are not really getting data about the impact of these matters by the company itself. What you are hearing is industry and experts saying this is going to have a big impact, this makes us much more vulnerable. But I have yet to actually hear what was vulnerable about the Apple iPhone.

Senator Klobuchar. I guess I would ask you, Dr. Lin and Professor Swire, in your view, to what extent are companies obligated to help law enforcement access data when they have a warrant in light of this announcement on the products?

Mr. Lin. Well, I am not the lawyer here, but it strikes me that if a company does not have the technological capability to do something, there is nothing it can do in response. That was--

Senator Klobuchar. But suppose they would have the technological ability if they changed their product?

Mr. Lin. If they did have the technological capability to, then I think they are obligated under all of the penalties that attend to not complying. I do not think there is any question about it. I do not think that anybody has disputed that.

Senator Klobuchar. Professor Swire?

Mr. Swire. I would like to offer some observations, and this is partly responding to Mr. Vance's points, which are well taken, what was different the day before or the day after. I think as someone who teaches cybersecurity to grad students in computer science, I have a slightly different perspective of people living in that community, which is some things did change with Snowden, and in particular, the tech community was very surprised at how many things were broken in how many ways. As story after story came out, there were just a lot of different operating systems, a lot of different particular devices, et cetera, that turned out to be broken at scale.

And so in their technical report issued yesterday by all the cryptographers, they talked about some jargon about perfect forward secrecy, but I think the English version of it is we do not want to have systems where, once they are compromised, they are broken at scale and millions of devices are compromised. And the concern is when you have a master key sitting there, if that gets broken once--and a lot of things were broken--then we can have massive breaches at scale.

And so when you see these very big flaws and bugs and breachers, customers start to expect an upgrade. And so what we have seen across the line from sophisticated

customers wanting good security for their own products is better security than we had pre-Snowden. And I think the Apple announcement, properly understood, is part of the upgrade the whole industry is trying to do because they found out they had flaws they did not know they had.

Senator Klobuchar. Yes, I believe that. It is just having been a prosecutor in law enforcement when things were a lot simpler, I know that we would use this kind of data to track murderers, to track people who were on the loose who had hacked people up. I mean, these are not little things. And I just remember being told by law enforcement, "Well, we cannot say how we got that," you know? This is a long time ago. I mean, they were not violating the law. It is just that they were able to get that data. And now if they cannot get that data, I am very concerned. You know, we are all thinking about cybersecurity and hacking, and my view of it is if the purpose is to protect people from hacking, if we just do nothing and do not go after the bad guys and just let them do it and we do not have access to be able to do it, it is just going to get worse.

And I understand this privacy concern, and that is why somehow allowing the law enforcement to get in to get this data and differentiating that from hackers and not equating law enforcement with hackers to me is the answer, because if you do not have law enforcement to go after the hackers,

they are just going to keep doing it and finding new ways.

Mr. Swire. The point that I am making is a security concern, not primarily a privacy concern, which is: Are we going to have systems that we know can be compromised at scale? And we want to build systems that are not subject to that. And we saw a lot of public reporting--a lot of which I wish we had not had as public reporting. We saw a lot of public reporting of hacks at scale, and the industry is responding by tightening up security.

Senator Klobuchar. Mr. Vance?

Mr. Vance. Certainly we have seen and are very concerned about hacks at the mass data level, but I am still not aware of someone or anyone hacking into Apple, grabbing the digital key that it held in my phone, which was only good for my phone, and that causing the digital chaos that is associated with either Snowden or Target or Home Depot.

Senator Klobuchar. Target would be from Minnesota, so you might not want to use that exact example.

[Laughter.]

Senator Klobuchar. There are many others: T.J. Maxx.

Mr. Vance. We have got JPMorgan. We have got plenty of our own.

Senator Klobuchar. Nordstrom's. Okay.

Mr. Vance. And so I understand there is a theoretical concern, but it seems to me that from everything we know,

Apple held on to these individualized keys in a way that was secure unless something has happened that I do not know about.

Mr. Swire. So Google and Apple both have fabulous security engineers, but there has been reporting that Google had a database of the foreign intelligence targets that the FISA Court was going after that included a lot of information about Chinese nationals, and there has been reporting that the Chinese Government got into that database to know who had been compromised.

So we have some of the best computer security people in the world working at these companies and public reporting about breaches, so I do not think it is some abstract worry. It is something we have had reporting on.

Mr. Vance. We should move them to the Phone Division.

[Laughter.]

Senator Klobuchar. Okay. Well, very good. I want to thank all of you, and I want to also thank you, Mr. Vance, for your good work on sex trafficking and what you have bee doing.

Mr. Vance. Thank you.

Senator Klobuchar. I really appreciate that. As you know, Senator Cornyn and I had a bill that finally passed in the Senate that we hope will be helpful, but I want to thank you for that as well.

Mr. Vance. Thank you also.

Senator Klobuchar. All right. Thank you. I do not need a gavel. I will use the water. Did Senator Whitehouse or Senator Grassley cover the hearing record being open? Okay. The hearing is adjourned. All right. Thanks.

[Whereupon, at 1:01 p.m., the Committee was adjourned.]

C O N T E N T S