Exhibit LL

CQ CONGRESSIONAL TRANSCRIPTS
Congressional Hearings
March 1, 2016 - Final

House Judiciary Committee Holds Hearing on Encryption Security and Privacy, Panel 2

LIST OF PANEL MEMBERS AND WITNESSES

PETERS:
So listen, I want to thank you for being here. I wanted to just conclude by saying that I didn't hear very -- did listen carefully to your opening statement. I thought it was very constructive. I think you appreciated the two objectives we have here which is to both preserve privacy and to deal with San Bernardino. You heard that comment hard cases make bad law. They're still hard cases and the problem we see in terrorism now is this, the onesies and the twosies and the notion that we would have invulnerable communications I think is something that we should all be concerned about.

I hope that you and the panel to follow you all be part of the constructed discussion if you got a way to serve both objectives and that the lines won't be too hard drawn on either side so we can do that. And I appreciate Mr. Chairman the chance to thank Director Comey for being here and I look forward to the next panel.

COMEY:
Thank you.

PETERS:
I yield back.

GOODLATTE:
Sure, thanks gentlemen.

Director, you've donated three hours of your time to our efforts today, or more, I'm sure in getting ready so we thank you very much for your participation and for answering a multitude of questions and we are looking for answers so if you have more to add to the record later, we would welcome that as well. Thank you very much.

COMEY:
Thank you, sir.

ISSA:
Chairman, would you entertain a unanimous consent while we're changing panels?

GOODLATTE:
I would.

ISSA:
And I would ask unanimous consent that a letter I received late yesterday from a constituent in the technology business concerning this case be placed in the record. This is Emily Hirsch.

GOODLATTE:
Without objection, we will be made it a part of the record. We ask the witnesses on the second panel to please come forward and be seated.

And now that Mr. Sewell has been afforded similar attention to the attention previously accorded to Director Comey, I'd ask that the press move back so we can begin the second panel.

(UNKNOWN)
Mr. Chairman, I would not assume that was not directed to Miss Landau, this photography.

GOODLATTE:
Thank you. We welcome our distinguished witnesses for today, the second panel. And if you would all, please rise. I'll begin by swearing you in.

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

(UNKNOWN)
I do.

GOODLATTE:
Thank you very much. The record reflect that all the witnesses responded in the affirmative and I'll now introduce the witnesses.

Bruce Sewell is senior vice president and general counsel of Apple. Mr. Sewell serves on Apple's legal team and oversees all legal matters, including global security and privacy. Prior to joining Apple, Mr. Sewell was deputy general counsel and vice president of Intel Corporation. He received his Bachelors Degree from the University of Lancaster and a J.D. from George Washington University.

Dr. Susan Landau is professor of Cyber Security Policy at Worcester Polytechnic Institute. Originally trained as a theoretical computer scientist, Dr. Landau is an expert in cryptographic applications. Within cyber security policy, her work focuses specifically on communication surveillance issues. Dr. Landau earned a Bachelors Degree from Princeton University, a masters from Cornell University and a PhD from the Massachusetts Institute of Technology.

Our final witness, Mr. Cyrus Vance Jr., is the district attorney of New York County. Mr. Vance is currently serving his second term as district attorney after being re-elected in 2013. He also serves as co-chair of the New York State Permanent Commission on Sentencing. Previously, Mr. Vance worked in private practice and taught at Seattle University School of Law. He is a graduate of Yale University and the Georgetown University Law Center.

All of your written statements will be entered into the record in their entirety and we ask that each of you summarize your testimony in five minutes or less. To help you stay within that time, there's a timing light on the table. When the light switches from green to yellow, you have one minute to conclude your testimony. And when the light turns red, that's it, your time is up.

And we'll begin with you, Mr. Sewell. Welcome.

SEWELL:
Thank you very much, Mr. Chairman. Thank you members of the committee and ranking member.

GOODLATTE:
Make sure that microphone is on and pulled close.

SEWELL:

Thank you for that technology hint. Thank you, Mr. Chairman. It's my pleasure to appear before you and the committee today on behalf of Apple.

We appreciate your invitation and the opportunity to be part of the discussion on this important issue, which centers on the civil liberties that are at the foundation of our country. I want to repeat something that we've said since the beginning that the victims and the families of the San Bernardino attacks have our deepest sympathies. We strongly agree that justice should be served and Apple has no sympathy for terrorists.

We have the utmost respect for law enforcement and share their goal of creating a safer world. We have a team of dedicated professionals that are on call 24 hours a day, seven days a week, 365 days a year to assist law enforcement. When the FBI came to us in the immediate aftermath of the San Bernardino attacks, we gave them all the information we had related to their investigation. And we went beyond that by making Apple engineers available to advise the FBI on a number of investigative alternatives.

But now, we find ourselves at the center of a very extraordinary circumstance. The FBI has asked a court to order us to give them something that we don't have, to create an operating system that does not exist. The reason it doesn't exist is because it would be too dangerous. They are asking for a backdoor into the iPhone, specifically, to build a software tool that can break the encryption system which protects personal information on every iPhone.

As we have told them, and as we told the American public, building that software tool would not affect just one iPhone. It would weaken the security for all of them. In fact, just last week, Director Comey agreed and I think we heard the same here today that the FBI would likely use this as precedent for other cases involving other phones. We've heard from District Attorney Vance who's also said that he absolutely plans to use this tool on over 175 phones that he has in his possession.

We can all agree this is not about access to one iPhone. The FBI is asking Apple to weaken the security of our products. Hackers and cyber criminals could use this to wreak havoc on our privacy and personal safety. It would set a dangerous precedent for government intrusion into the privacy and safety of its citizens. Hundreds of millions of law-abiding citizens trust Apple's products with the most intimate details of their daily lives, photos, private conversations, health data, financial accounts and information about a user's location and the location of that user's family and friends.

Some of you may have an iPhone in your pocket right now and if you think about it, there's probably more information stored on that device than a thief could steal by breaking into your house. The only way we know to protect that data is through strong encryption.

Every day, over a trillion transactions occur safely over the internet as the result of encrypted communications. This range from online banking and credit card transactions to the exchange of health care records, ideas that will change the world for the better and communications between loved ones. The U.S. government has spent tens of millions of dollars through the open technology fund and other U.S. government programs to fund strong encryption. The review groups on intelligence and communications technology convened by President Obama urged the U.S. government to fully support and not, in any way, subvert, weaken or make vulnerable generally available commercial software.

Encryption is a good thing. We need it to keep people safe. We have been using it in our products for over a decade. As attacks on our customer's data become more sophisticated, the tools we need to use to defend against them need to get stronger too. Weakening encryption would only hurt consumers and well-meaning users who rely on companies like Apple to protect their personal information.

Today's hearing is entitled, "Balancing America's Security and Privacy". We believe we can and we must have both. Protecting our data with encryption and other methods preserves our privacy and keeps people safe. The American people deserve an honest conversation around the important questions stemming from the FBI's current demand.

Do we want to put a limit on the technology that protects our data and, therefore, our privacy and safety in the fact of -- in the face of increasingly sophisticated cyber attacks? Should the FBI be allowed to stop Apple or any company from offering the American people the safest and most secure products it can make? Should the FBI have the right to compel a company to produce a product it doesn't already make to the FBI's exact specifications and for the FBI's use?

We believe that each of these questions deserves a healthy discussion and any decision should only be made after a thoughtful and honest consideration of the facts. Most importantly, the decision should be made by you and your colleagues as representatives of the people rather than through a warrant request based on a 220-year-old statute.

As Judge Orenstein concluded yesterday, granting the FBI's request would thoroughly undermine fundamental principles of the constitution. At Apple, we are ready to have this conversation. The feedback and support we're hearing indicate to us the American people, too. We feel strongly that our customers, their families, their friends and their neighbors will be better protected from thieves and terrorists if we can offer the best protections for their data at the same time our freedoms and liberties we all cherish will be more secure. Thank you for your time. I look forward to your questions.

GOODLATTE:
Thank you, Mr. Sewell. Ms. Landau, welcome.

LANDAU:
Thank you, Mr. Chairman and members of the committee. Thank you very much for the opportunity to testify today.

The FBI has pitched this battle as one of security versus privacy but a number of the members have already observed it's really about the security versus security. We have a national security threat going on and we haven't solved the problem at all. What the smartphones got to do with it? Absolutely everything. Smartphones hold our photos and music, our notes and calendars, much of that information sensitive, especially the photos.

Smartphones are increasingly wallets and they give us access to all sorts of accounts. Bank accounts, drop box and so on. Many people store proprietary business information on their smartphones even though their personal smartphones even though they know they shouldn't.

Now, NSA will tell you that stealing login credentials is the most effective way into a system. In fact, Rob Joyce of the Tailored Access Operations said so in a public talk a month ago. Here is where smartphones are extremely important. They are poised to become authenticators to a wide variety of systems, the services. In fact, they are already being used that way, including at some high-place government agencies.

Now, District Attorney Vance will tell you that -- has said that large-scale data breaches have nothing to do with smartphone encryption, but that's not true. Look at today's New York Times where there's a story about the attack on the Ukrainian power grid. How did it start? It started by the theft of login credentials, of system operators. We've got to solve the login authentication problem and smartphones are actually our best way forward to do it, but not if it's easy to get into the data of the smartphones.

Now, the committee has already observed that there are many phones that will be -- that will go through the process of being unlocked, not just the one in San Bernardino. And what that means for Apple is that it's going to have to develop a routine to do so. Now, what happens when you have -- when you sign a piece of code to update a phone and you're signing a piece of codes that's an operating system affirm where you do it once? You do it occasionally? It's a whole ritual and there are very senior people involved. But, if you're dealing with phones that are daily being updated in order to solve law enforcements cases, then what happens is you develop a routine. You get a webpage. You get a low-level employee to supervise it. And then it becomes a process that's easy to subvert.

I have lots of respect for Apple's security, but not when it becomes a routine process to build an update for a phone. And what will happen is organized crime or nation-state will do so, using an update to then hack into a phone, maybe the phone of the Secretary of the Chief of the Federal Reserve, maybe a phone of an HVAC employee who's going to go service a power plant. What we're going to do is decrease our security. That's the security risk that's coming from the requests.

Now I get that law enforcement wants data protection that allows them access under legal authorization. But an NSA colleague once remarked to me that while his agency have the right to break into certain systems, no one ever guaranteed that that right would be easy to do so. The problem is when you build a way in for someone who isn't the owner to get us the data, well, you built a way in for somebody else to get in as well.

Let me go to Caliah (ph) for a moment. Caliah (ph) is the security nightmare. I know that Congress has intended it that way but that's what it is. If you'll ask the signal as intelligence people they'll to you. There are many ways for nefarious sorts to take advantage of the opening offered by law enforcement. Instead of embracing the communications and device security we still badly need, law enforcement has been pressing to preserve 20th century investigative techniques. Meanwhile, our enemies are using 21st technologies against us.

The FBI needs to take a page from the NSA. You may recall that in the late 1990s, the NSA was complaining it was going deaf from encrypted calls? Well, they've obviously improved their technology a great deal. According to Mike McConnell, from that time until now, NSA had better sigint than any time in history. What we need is law enforcement to developed 21st century capabilities for conducting electronic surveillance.

Now, the FBI already has some excellent people and expertise but FBI investment and capacity is not at the scale and level necessary. Rather than

asking industry to weaken protections, law enforcement must instead develop a capability for conducting sophisticated investigations themselves.

Congress can help. The FBI needs an investigative center with agents with deep technical understanding of modern telecommunications technology and also because all phones or computer, modern computer -- deep and expertise in computer science, only the teams of researchers, who understand various types of field of devices.

They'll need to know where technology is and where it will be in six months and where it will be in two to five years, communications technology in two to five years so that they can develop the surveillance technologies themselves. Expertise need not be in house. The FBI could pursue a solution where they develop some of their own expertise and closely manage contractors to do some of the work.

But however, the bureau pursues the solution it must develop modern state of the art capabilities. It must do so rather than trying to get industry to weaken security. Your job is to help the FBI build such capabilities, determine the most efficient and effective way that such capabilities could be utilize by state and local law enforcement for they don't have the resources develop that themselves and to also fund that capabilities.

That's the way forward that does not put our national security at risk. It enables law enforcement investigations while encouraging industry to do all it can do to develop better and more effective technologies for securing data and devices. That was a win-win and where we should be going. Thank you.

GOODLATTE:
Thank you, Ms. Landau. Mr. Vance, welcome.

VANCE:
Thank you. Good afternoon, Chairman Goodlatte, Ranking Member Conyers and members of the House Judiciary Committee. Thank you so much for allowing me to participate today.

I'm testifying as a district attorney but on behalf of the National District Attorneys Association. And I'm very grateful for you giving us the opportunity to be here because much of the discussion in the prior panel and in the comments by the other speakers here has been about the federal government and about the issue of security and cyber crime in the federal context. But it's important, I think, for us to recognize that state and local law

enforcement agencies handle 95 percent of the criminal cases each year around the country. So, we have a very deep interest in the subject matter of this hearing today and thank you for allowing us to participate.

Apple and Google's decision to engineer their mobile devices to, in an essence, be warrant-proof has had a real effect on the traditional balance of public safety versus privacy under our Fourth Amendment jurisprudence and I agree with the comments, I think, of everyone here, including the many members of the house that we really need Congress to help solve this problem for us and it's -- why it so important that you are undertaking this effort. But I think in looking at this issue there are some basic facts from the state law perspective that really are very important to this debate but are not in dispute.

And number one, as Tim Cook said in his open letter to his customers of Apple of February 16th of this year, smartphones, led by iPhone, have become an essential part of our lives. Nothing could be more true. We are all using our cell phones for every aspect of our lives.

Number two, is that smartphones are also essential to criminals. Our office investigates and prosecutes a huge variety of cases from homicide to sex crimes, from international financial crime and including terrorism cases. And criminals in each of those cases use smartphones to share information, to plan and to commit crimes, whether it's through text messages, photographs or videos.

Number three, criminals know that the iOS 8 operating system is warrant-proof. Criminals understand that this new operating system provides them with a cloak of secrecy. And they are, ladies and gentlemen, quite literally, laughing at us. And they are astounded that they have a means of communication totally secure from government reach. And I don't ask you to take my word for it. In one lawfully recorded phone conversation from Rikers Island in New York, an inmates talking about the iOS 8 default device encryption called it and I'm quoting, a gift from God.

Number four, the encryption Apple provided on its mobile devices prior to iOS 8, that is before October 2014, was represented to be both secure for its customers and, importantly, was amenable to court authorized searches. We know this because Apple told us this.

Apple characterized its iOS 7 operating system as the ultimate in privacy. It touted its proven encryption methods and assured its users that iOS 7 could be use with confidence in any personal or corporate environment. During the time when iOS 7 was the operating system, Apple also acknowledged that its

responsibility to help, again in Apple's own words, police investigating robberies and other crimes, searching for missing children, trying to locate a patient with Alzheimer's disease or hoping to prevent the suicide.

So Apples experienced, I believe, with iOS 7 demonstrated that strong encryption and compliance with court orders are not mutually exclusive. Default device encryption has had a profound impact on my office and others like it. In November of 2015 my office published a white paper on public safety and encryption and in that -- and that time, there were 111 iPhones from which we were locked out, having obtained search warrants for those devices.

Now, two and a half months later, when we submitted our written testimony for this committee, the number was 175. Today, it is 205, which represents more than one out of four the approximately 700 Apple devices that have been analyzed by our office's own cyber lab since the introduction of iOS 8. And of course that problem isn't just in Manhattan.

Prosecutors in Houston had been locked out of more than 100 iPhones last year, 46 in Connecticut, 36 in Chicago since January and those are just a few of the thousands of phones taken at evidence each year around the country. So centuries of jurisprudence that have been talked about today have held that no item, not a home, a file cabinet, a safe or even a smartphone just beyond the reach of the court order search warrant. But the warrant-proof encryption today gives two very large companies, we believe, functional control over the path to justice for victims of crime, including who could be prosecuted and, importantly, who may be exonerated.

So, our point, Mr. Chairman, is that we believe this line being drawn which is in public safety in privacy is extremely important. It's affecting our lives. It's affecting our constituent's lives and we believe that you should be drawing it and we ask you to address this problem quickly. Time is not a luxury for state and local law enforcement. Crime victims or communities can afford it. Our laws require speedy trials. Criminals have to be held accountable and victims are, as we speak, and we know in this audience, asking for justice.

GOODLATTE:
Thank you, Mr. Vance. We'll now be proceed with questioning of the witnesses under the five-minute rule and I'll begin by recognizing myself.

Mr. Sewell, Director Comey created a dichotomy between this being a technology problem or a business model problem and said that Apple was addressing this as a business model problem. Is that a fair contrast or is this something else?

SEWELL:
It's by no means a fair contrast, Mr. Chairman. I've heard this raised before. It was raised in New York. It's been raised in San Bernardino and every time I hear this, my blood boils. This is not a marketing issue. That's a way of demeaning the other side of the argument. We don't put out billboards to talk about our security. We don't take out ads that market our encryption. We're doing this because we think that protecting the security and the privacy of hundreds of millions of iPhone users is the right thing to do. That's the reason we're doing this.

And to say that it's a marketing ploy or that it's somehow about P.R., it really diminishes what should be a very serious conversation involving this Congress, the stakeholders, the American people. Just with respect to the New York case, Judge Orenstein last night took on this issue head on and he said, in footnote 14 on page 40, he said, "I reject the government's claim. I find Apple's activities and the position that they are taking conscientious and not with respect to P.R. or marketing."

GOODLATTE:
Director Comey and Mr. Vance seem to suggest that the security provided by encryption on prior devices is fine. But advancing encryption technology is a problem. What do you think about that?

SEWELL:
So, it's important to understand that we haven't started on a path of changing our technology. We haven't suddenly come to the notion that encryption, security and privacy are important. At Apple this began back in 2009 with our encryption of FaceTime and iMessage. We've been on path from generation to generation as the software and the hardware allow us to provide greater security and greater safety in privacy to our customers. What happened between iOS 7 and iOS 8 was that we were able to transform the encryption algorithm that is used within the software and the hardware of the phone to provide a more secure solution.

GOODLATTE:
We are moving to end-to-end the encryption on many devices and apps not just Apple iPhones. Why is that happening?

SEWELL:

I think it's a combination of things. From our perspective at Apple, it's because we see ourselves as being in an arms race, in an arms race with criminals, cyber terrorists, hackers. We're trying to provide a safe and secure place for the users of our devices to be assured that their information cannot be accessed, cannot be hack or stolen. So from our perspective that end-to-end encryption move is an effort to improve the safety and security of our phones.

From the terrorist perspective, I think it's an effort to communicate in ways that cannot be detected. But the terrorists are doing this independently of the issues that we're discussing here today.

GOODLATTE:
Now, if the FBI succeeds in getting the order that is in dispute that Apple has appealed to a final resolution overlying that takes and they then get Apple to develop this device that will allow the 10 times and your -- by the way, all of us here, we can't turn that off, so.

SEWELL:
But we could show you how to do that.

GOODLATTE:
I know but inside our firewall here, we can't do that. So, we understand the reason. But that creates a separate vulnerability, does it not, for people who device falls to be apprehended (ph), they could willfully try 10 times and erase whatever hasn't been backed up on the device. For me that as it may, if they were to get you to develop that code and apply it and then to crack the four-digit code to get into the device, once they get in there, they could find all kinds of other restrictions that Apple has no control over, right, with regard to apps that are on the phone, with regard to various other communications features that the consumer may have chosen to put on there. Is that correct?

SEWELL:
That's absolutely right, Mr. Chairman. One of the most pernicious apps that we've seen in the terrorist space is something called telegraph. Telegraph is an app that can reside on any phone. It has nothing to do with Apple. It can be loaded either over the internet or it could be loaded outside of the country. And this is a method of providing absolutely unencrypt -- uncrackable communications.

What happens here is that Apple is forced to write a new operating system to degrade the safety and security in phones belonging to tens or hundreds of millions of innocent people. It will weaken our safety and security but it will not affect the terrorists in the least.

GOODLATTE:
Thank you very much. My time has expired. The gentleman from Michigan, Mr. Conyers, is recognized for five minutes.

CONYERS:
Thank you, Mr. Chairman, and welcome to the witnesses. Let me start off with Professor Landau. Director Comey has just testified that until the invention of the smartphone, there was no closet, no room, no basement in America that the FBI could enter. Did encryption exist before the invention of the iPhone?

LANDAU:
Encryption has existed for centuries and in particular they've been fights over encryption and the use of encryption in the '70s about publication, in the '80s about, whether NIST or the NSA would control the development of encryption for non-national security agencies, in the '90s about whether there would be export controls on devices with strong encryption.

The White House changed those rules in 2000. We expected to see widespread use of strong encryption on devices and on applications and the technologist's response to Apple is, "What took you guys so long?" How in the face of all the cyber security problems that we've had did it take industry so very long to do this?

CONYERS:
Well, as our technical expert, let me see this. Is there any functional difference between asking Apple to break its own encryption and what FBI has demanded in California?

LANDAU:
I'm sorry. Asking Apple to break -- I don't quite understand the question.

CONYERS:
All right.

LANDAU:
What Apple is being asked to is to subvert the security controls and go around. So it's not breaking the encryption but it's subverting its own security controls.

CONYERS:
Right.

LANDAU:
And is there any functional difference between that end (ph)?

CONYERS:
And what the FBI has demanded in California?

LANDAU:
What has demanded in California is that Apple subverts its own security controls.

CONYERS:
Let me ask Mr. Bruce Sewell the same question. What is the functional difference between ordering Apple to break its encryption and ordering apple to bypass its security so the FBI can break the encryption?

SEWELL:
Thank you, Ranking Member. Functionally, there is no difference. What we're talking about is an operating system in which the passcode is an inherent and integrated part of the encryption algorithm. If you can get access to the passcode, it will affect the encryption process itself. What we're being asked to do in California is to develop a tool, atoll which does not exist at this time that would facilitate and enable the FBI in a very simple process to obtain access to the passcode. That passcode is the cryptographic. So essentially, we are throwing open the doors and we are allowing the very act of decryption to take place.

CONYERS:
I was hoping you'd go in that direction. Let me ask you do this, there's been a suggestion that Apple is working against law enforcement and that you no longer respond to legal process when investigators need your assistance. Is

that accurate?

SEWELL:
It's absolutely false. As I said in my opening statement, we care deeply about the same motivations that motivate law enforcement. The relationship with law enforcement falls within my job at Apple. The people that we have who assist law enforcement everyday are part of my team and I'm incredibly proud of the work they do. We have dedicated individuals who are available around the clock to participate instantly when we get a call. As we discussed a little bit earlier in Director Comey...

CONYERS:
I want to squeeze in one more question before my time runs out.

SEWELL:
All right. I'll try to be very quick. We do everything we can to assist law enforcement and we have a dedicated team of people who are available 24/7 to do that.

CONYERS:
Why is apple taking this stand? What exactly is at stake in the San Bernardino case?

SEWELL:
This is not about the San Bernardino case. This is about the safety and security of every iPhone that is in use today. And I'd like to address one thing that Director Comey raised. This is -- there's no distinction between a 5C and a 6 in this context. The tool that we're being asked to create will work on any iphone that is in use today. It is extensible. It is common. The principles are the same. So the notion that this is somehow only about opening one lock or that there is some category of locks that can't be open with the tool that they're asking us to create is a misnomer. It's something that we needed to clarify.

CONYERS:
Thank you for your responses.

GOODLATTE:

The chair recognizes the gentleman from Wisconsin, Mr Sensenbrenner for five minutes.

SENSENBRENNER:
Thank you very much, Mr. Sewell. And I think you know that I have been one of the privacy hawks on this committee. The whole debate over the USA Freedom Act was whether the NSA should go to court and give them some time of an order or a warrant specifically miming the person or persons whose data is requested. Here, the FBI, you know, has done that. In your prepared testimony, you said the questions about encryption should be decided by Congress rather than through a warrant based on a 220-year-old statute. I point out the Bill of Rights is about the same age. Now, the FBI is attempting to enforce a lawful court order. Apple has every right to challenge that order as you have done but why is Congress and not the court the best venue to decide this issue?

SEWELL:
Congressman, I think that, ultimately, Congress must decide this issue. So I'm completely in support of the decision that you're articulating. I think we find ourselves in an odd situation in our court in California because the FBI chose to pursue in an ex parte fashion a warrant that would compel Apple to do something. We do that not as extension of the debate, not as a way to resolve this issue, we do that as a way to cut off the debate because the court would have grant the release that the FBI is seeking. We would be forced to do the very thing which we think is that issue and should be decided by the American people. We would be forced to create...

SENSENBRENNER:
Hey, now what's your proposal, legislative response? Do you have a bill for us to consider?

SEWELL:
I do not have a bill for you to consider.

SENSENBRENNER:
OK, thank you. That answers that. Now, the FBI has provided some fairly specific policy proposals to ensure that law enforcement can can access encrypted data with a warrant. What policy proposal would Apple support? You don't like what the FBI said. What's your specific response?

SEWELL:
What we're asking for, Congressman, is a debate on this. I don't have a proposal. I don't have a solution for it. But what I think we need to do is to give this an appropriate and fair hearing at this body which exists to convene and deliberate and decide issues of legislative importance. We think that the problem is we need to get the right stakeholders in the room. This is not a security versus privacy issue. This is a security versus security issue and that balance should be struck, we think, by the Congress.

SENSENBRENNER:
Well, you know, let me make this observation. You're having dealt with the fallout of the Snowden revelations and the drafting and garnering support of the USA Freedom Act. I can tell you, I don't think you're going to like what comes out of congress.

SEWELL:
Congress, we will follow the law that comes out of this process. We certainly understand.

SENSENBRENNER:
OK. OK, well, the thing is I don't understand. You don't like what's being done with the lawfully issued warrant. And most warrants are issued on an ex parte basis where law enforcement submits an affidavit before a magistrate or a judge. And the judge determines whether the allegations of the affidavit are sufficient for the warrant to issue.

Now, you're operating in a vacuum. You told us what you don't like. You said that Congress opted debate and pass legislation. You haven't told us one thing about what you do like. When are we going to hear of what you do like so that Apple has a positive solution to what you were complaining about?

You said it's Congress' job to do it. Now, we won't shirk from that. This hearing, you know, is part of this debate. The FBI has provided some policy suggestions on that. You haven't said what Apple will support. So all you've been doing is saying is no, no, no, no. Now, our job in Congress, honestly, you know, as we did with the Freedom Act and as we are doing with the Electronic Communications Privacy Act update is to balance our belief that there should be privacy for people who are not guilty or suspected of terrorist activity and that there should be judicial process which there has been in this case. And, you know, I guess that what you're position is because you don't

have anything positive, you know, is to simply leave us to our own devices. Well, we would be very to do that but I guarantee you, you aren't going to like the result. I yield back.

SEWELL:
Congressman, I do think we have said what we stand for and what we believe this constant placing.

SENSENBRENNER:
No. You know, the thing is, is may ask Congress to do something and I asked you what Congress should do. You said, we have nothing. Then I said the FBI has provided specific policy proposals to ensure law enforcement is able to get this information. Now, here we're talking about the iPhone of a dead terrorist that was not owned by the terrorist but was owned by San Bernardino County.

Now, you know, the thing is, is that I don't have a government iPhone. I have my own iPhone which I use extensively. But the terrorist had, you know, a government iPhone which belonged to the government. I think the government of San Bernardino County specifically would like to get to the bottom of this and you're resisting it.

I said my piece.

GOODLATTE:
The time of the gentleman has expired. Gentleman from New York, Mr. Nadler, is recognized is five minutes,

NADLER:
Thank you, Mr. Chairman. Let me begin by welcoming my constituent and the great district attorney of New York County, Cyrus Vance and saying that I appreciate his enlightenment of the district attorney's use of this dilemma that we all face. Let me also suggest in answer to Mr. Sensenbrenner's questions that I assume that Apple may have legislative suggestions for us after the courts come out with their determinations and Apple decide they like their determination. So they don't like the determinations, at which point Apple and a lot of other people and institutions, I assume, will decide on specific legislative proposals. And it may very well be that this Congress will wait to see what the courts do. But we will see.

Let me then begin my questions. District Attorney Vance, Director Comey suggested earlier today that the release sought by the FBI is limited to this

one device running this particular operating software in this one case. Now, I gather that you've mentioned you have over 200 phones facing a similar problem that you don't really think that this case will be limited to the one device. So obviously, it's going to set a precedent, maybe not the only precedent, for a large of devices including the ones that you're interested in.

VANCE:
Well, there may well be an overlap between action in federal court where the FBI is in litigation and in state court. I do believe that what we should be seeking collectively is not a phone by phone by phone solution to accessing devices and the content when the problem was we should be creating a framework in which there are standards that are required to -- for a court to authorize access to a device and that it's not based upon litigation as to whether you can get to West Coast phone or East Coast phone.

NADLER:
I assume that, eventually, either the court will set one standard or Congress will.

VANCE:
Right.

NADLER:
I have to consider it.

VANCE:
Yeah.

NADLER:
Professor Landau, several of your colleagues recently published the results of as survey of over 600 -- and this is similar to a question I asked Director Comey Dlcomey, several of your colleagues recently published the results of a survey of over 600 encryption products that are available online. More than 400 of these products are open-source and made or owned by foreign entities. If Congress were to pass a law or, for that matter, if the courts were to impose a requirement that forcing U.S. companies to provide law enforcement with access to encrypted systems, would that law stop bad actors from using encryption open from open sources or foreign sources?

LANDAU:
Absolutely not, absolutely not. And what Apple's product does is it makes encryption easy by default. And so it means that, as I said, the Secretary to the Chair of the Federal Reserve, the HVAC employee, the chief of staff in your office. Of course, your office should be protected anyway but the regular person using a phone has the phone Secured. What the change -- if Congress were to pass a law prohibiting use of encryption on Apple phones or however you -- you know, you wouldn't say it's just for apple. What it would do is it would weaken us but not change it for the bad guys.

NADLER:
And if someone purchased a phone from a foreign company can have the encryption that we prohibit in an American from creating?

LANDAU:
If someone purchased a foreign phone, somebody could just download the app from abroad. They don't have to buy a foreign phone. They can just download the app from anywhere.

NADLER:
And let's assume the Congress decided to prohibit purchase of foreign encryption systems, is there any practical way we can enforce that?

LANDAU:
No. So -- I mean you would have to start inspecting so much as it comes over the internet that it becomes an intrusive...

NADLER:
So what you're saying is that we are really debating something that's undoable?

LANDAU:
That's right. And we were there 20 years ago which the open-source issue was part of the reason for the U.S. Government to change in export controls which is part of what enabled...

NADLER:

OK. Let me ask two very quick questions before my time runs out. Mr. Sewell, the Eastern district Court yesterday in its ruling has been referred to -- cited no limiting principle to the legal authority behind the FBI's request as a reason to deny the order. Is there a limiting principle in the San Bernardino case?

SEWELL:
Absolutely none, Congressman.

NADLER:
None. So it can be expanded indefinitely. And finally, Mr. Sewell, your brief, Apple's brief to the court lays out several constitutional concerns, this computer code speeches to protect them to the First Amendment. What are the First and Fifth Amendment question? Well, let me just ask, what are the First and Fifth Amendment case -- questions does this case raise? We've been talking about statute but let's ask about the First and Fifth Amendment questions.

SEWELL:
Right. Good question, Congressman. And bear in mind that what we're being asked to do is write a brand new computer code right in new operating system. The law, with respect to the applicability of computer codes to speech, I think is well- established. So this is compelled speech by the government for the purpose of the government...

NADLER:
Which is a First Amendment problem.

SEWELL:
Which is absolutely First Amendment problem. And bear in mind that this speech which Apple does not want to make, this is our position. On the Fifth Amendment, the issue is conscription, the issue is forced activity, forced labor.

NADLER:
Does anybody else on the panel want to comment on that question? None? Thank you. My time is expired, Mr. Chairman.

GOODLATTE:

The gentleman from California, Mr. Issa, is recognized for five minutes.

ISSA:
Thank you, Mr. Chairman and I'll pick up where you left off on forced labor. Do you know of any place in our history in which -- except in time of war, when things are commandeered and people are told do that or when police are in the hot pursuit, do you know a time in which people were forced to apply their inventive genius against their will?

SEWELL:
Congressman, I'm not aware of it. There's still cases during the war that must (ph) be applicable.

ISSA:
Sure. And I certainly understand a different time and different set of circumstances. Now, I want to do two things. So Miss Landau, I'm going to come to you first. Your expertise is encryption. You were probably very young but you remember 20 years ago the argument wasn't that the FBU and then the Late Mike Oxley and others that were championing that if we allowed more than 256 bit encryption, then the FBI couldn't easily decode it and that would be the ruin of their investigations.

LANDAU:
Right. And what you get instead is over the last 20 years, the NSA has increasingly supported the secured technologies for private sector communications infrastructure including the 256 bit algorithm.

ISSA:
OK. I'm going to ask you a quick question and it's old technology because I'm very good with analog world but this happens to P.A. January 29, 2015. Patent is already in the record and its patent on, basically, self-destructing the contents inside if someone tries to forcibly open it.

Now, the funny thing is I was looking for the old patent that's going back decades and decades because the military and others have used this. They've had acids and even more punitive, if you will, responses inside when we wanted to secure it. It's not a new technology but there's a new twist on it. Aren't we, in a sense, the equivalent of saying, "Well, you can make something that destroys the documents but then you have to tell us how to defeat it?

LANDAU:
That's exactly right.

ISSA:
OK. And I'm looking and saying that there's no history on that but we've had plain safes for a very, very long time. This isn't new. Do you know of any shredder company that's been told that they have to show you how to reassemble what they've shredded?

LANDAU:
I don't study shredding companies but I'd be would be very surprised if they were.

ISSA:
Mr. Vance, have you ever ordered a shredding company to put the paper back together, use their inventive genius?

VANCE:
Of course, I haven't, Congressman.

ISSA:
OK. So, you're asking, in this case, for somebody to create a product for your service and I want to focus on that and I'll get to you, I promise. But, Mr. Sewell, I'm going to look at you as the representative of one of the great technology companies in our country, Apple gets its great technology people, I assume, from Stanford and MIT and other great universities, right?

SEWELL:
We do. Yes, we do.

ISSA:
And you don't get all the graduates, right?

SEWELL:
No, we don't. We wish we do.

ISSA:

So when I was talking to the director and saying, "Well, if you take, and it's a hypothetical. My level of knowledge is way less than any of your folks and probably any of the FBIs but if you take this hard drive, solid state hard drive, you pull it apart and even use the word mirroring, obviously you'd some discussion at some point, and you make as many images as you want, then you have a true original that even if the self-destruct occurs, that original, you throw it away, you take another one. So, that part of what this asking you to do, they can do themselves by pulling the chip out and having it imaged, if you will, in all likelihood. We're not saying for sure but he hadn't checked it. So that's a possibility, is that right?

SEWELL:
I believe so. We don't know what the condition of the phone is and we don't know what the condition around this.

ISSA:
Sure. And of course, we're not really talking about one phone. We know that. We're talking about thousands of phones. And as I understand, the technology used in your chip is you have burnable traces in your chips. So randomly or in some way when you're producing each chip, you burn traces which create the encryption algorithm and that's internal. So the chip has its algorithm separate from the software. But that chip, when interfacing with an image, if you keep giving it new images, that's the part that changes.

So, isn't it at least conceivable that as to that phone and perhaps the 175 in New York and others, that the FBI or NSA could, in fact, come up with an elegant brute force attack that would work on your phones and also would work on hundreds of other types of phones around the World and that that technology with, if you will, those brilliant young minds from Stanford, MIT and Kent State, my alma mater, you know, could in fact, produce something that would not be available to the public, they would have control over and they would be able to make it more universal than just trying to go through your source code which, is it correct, they've never asked for. Is that right?

SEWELL:
We've never been asked for a source code.

ISSA:
OK. Mr. Chairman, if anyone else wants to opine on that, I would appreciate they'll be able to.

GOODLATTE:
Sure. Thanks, gentleman. And I recognize the gentlewoman from California, Ms. Lofgren, for five minutes.

LOFGREN:
Well, thank you very much. I think this hearing is very helpful and just to get it on the record, Mr. Sewell, I mean, you're not objecting -- let me step back. If you have something and you are served with a warrant, you give that something up. Is that correct?

SEWELL:
It's absolutely correct, yes ma'am.

LOFGREN:
So the issue here is you don't have it, you've got no way to get it, therefore, you can't give it, right?

SEWELL:
That's correct.

LOFGREN:
No it that were possible to do something that would get just this one thing without opening the door to everybody else's stuff, would you have a problem with that?

SEWELL:
Let me...

LOFGREN:
Oh, let me rephrase that because you're in court.

SEWELL:
Sure.

LOFGREN:
That would be a different issue than breaking encryption, generally, wouldn't it be?

SEWELL:
The best analogy that I can come up with that I've been struggling with is how do we create the right kind of analogy for this situation. If Apple had a box somewhere that we could guarantee, we could assure 100 percent certainty that anything that was put in that box was not susceptible to thievery, to attack, to corruption. If we had such a place in the world, we wouldn't be here today.

LOFGREN:
Right.

SEWELL:
I think what we would have done is gone to our customers and we would have said, "Give us your passwords." We can absolutely...

LOFGREN:
Correct.

SEWELL:
... 100 percent protect them. And then if you lose your phone, if you need our help, we can just give you the passcode.

LOFGREN:
But you didn't do that because you can't guarantee that which is why you encrypted this phone?

SEWELL:
Exactly right. And now the bizarre situation is that, essentially, the FBI is saying, "We all realize it's silly that everybody would give you your password. But instead, we want you to build a tool that will get those passwords and you're -- we're telling you, you can put that tool in this box doesn't exist.

LOFGREN:
So let me ask you this, is it possible, theoretically, to create code that would preclude you from creating a system that would allow you to defeat the ten try erase function?

We could write a program that would suppress that protected method.

LOFGREN:
So you couldn't do what it is you're being asked to do.

SEWELL:
Right. We're being asked to do three things. But we -- it is capable. We are capable of doing those three things. The issue is what's the consequence of doing that.

LOFGREN:
Right. But the question is also -- I mean this hearing cost me to go in and turn on the ten erase function which I neglected to do before the hearing. Thank you very much. But, you know, as you go forward, people are insecure about what's safe.

SEWELL:
Absolutely.

LOFGREN:
And, you know for example, you don't have -- and I think for good reason what's in iCloud is not encrypted. Is it possible to encrypt the data in iCloud?

SEWELL:
Yes. Actually in the iOS 8 and 9 generation, we have encrypted the iCloud data. It's encrypted in a different way than it was before and we think in a more secure way.

LOFGREN:
Right. But you can still provide access to that.

SEWELL:
It is encrypted in a different way and so...

LOFGREN:
But you could change that if you wished?

SEWELL:
Yes.

LOFGREN:
Now, let me ask you this, Dr. Landau. You were involved with that paper that was published, I think, last year.

LANDAU:
Yes.

LOFGREN:
Thank you. That was an excellent paper. And I think for anybody who has danced ahead to read some pages two or three times to understand it but for anybody and I would have to ask unanimous consent, Mr. Chairman, to put that paper in the record from the cryptographers.

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

LOFGREN:
If you just go to the questions at the end, you see that this is a fool's errand. We'll never be able to do what is being asked us by the FBI. It's a practical matter, it is just not achievable. But I'm interested in your take on -- you know, Director Comey, you know, they don't want the master key, they just want this one bypass on security. Isn't that exactly the same?

LANDAU:
It's wrong and it's just as pursuance (ph) said, once they've built that software, that software works for other phones. Of course, it has to have the serial number of the particular phone. So Apple has to sign, you know, has to take the software, put in a new serial number and sign it so the new phone accepts it and that's where all the security risks come in because it becomes a routine process and as I mentioned during my remarks, routine processes get subverted.

LOFGREN:

I'll ask the final question. It was asked earlier by my colleague Mr. Richmond, about whether somebody, these other countries have better security than we do. If I take my phone, my iPhone, with the current operating system to Russia or China, can they break into it?

SEWELL:
With respect to the phone itself, we believe that the encryption we provided in iOS 8 makes that effectively impossible. With respect to the things that are going on at the internet level, there are very sophisticated techniques that can be used by malicious actors who have access to the internet itself. There are ways to fool the internet into thinking that something is what it isn't. And so I think there is a vulnerability still in that regard. But on the phone, what we've tried to do is to remove that possibility with iOS 8 and 9.

LOFGREN:
Thank you very much for all of you for your testimony.

GOODLATTE:
The chair thanks the gentlewoman and recognized the gentleman from Texas, Mr. Poe, for five minutes.

POE:
Thank you, Chairman. Thank you all for being here. Fascinating, important discussion on this issue of as you say security and security. As you know, I'm a former prosecutor and a former judge and dealt with warrants for 30 years either requesting them or signing them. And this particular case, I think we're really talking about two cases now. We're not talking just about the San Bernardino case but the New York case as well, different facts, different issues.

Fourth Amendment, we have discussed. Fourth Amendment, that didn't really apply too much to this situation because the possession of the item is lawful in the possession of government. I do think it's ironic, however, we're talking about privacy. United States is supposed to lead on the issue, I think, on the issue of privacy. We're the only one that has a Fourth Amendment. But we see that other countries seem to have more concern about privacy in their technology than maybe we do. I find that somewhat ironic.

Let me ask you a couple of questions. You discussed the idea of constitutional right, right of privacy, but in one of your testimonies, now I think it was Mr. Nadler from New York, he and I have a language barrier problem

so I'm not sure I understood his question. You mentioned the First Amendment and the Fifth Amendment, is that correct?

NADLER:
I did. That's correct.

POE:
Briefly explain how you see this is a First Amendment issue as well as a Fifth Amendment issue. We don't need to talk about the Fourth Amendment. We've discussed that.

SEWELL:
The Fifth Amendment issue derives from the fact that we're being asked to a write code and the code is speech and the Supreme Court has held that speech is protectable. So we're being asked to speak by the government. That speech is not speech that we want to make. And the First Amendment provides us with protections against being compelled to speak by the government. So that would be the First Amendment argument in a nutshell. The Fifth Amendment provides us with protection from conscription, protection from being forced into labor at the governments will except under the most extraordinary of circumstances which I discussed with Congressman Issa. But that's the Fifth Amendment issue.

POE:
Right. Thank you. What -- this request, the results of the request, how would that affect Apple worldwide in other countries?

SEWELL:
Well, there are a number of parts of that question, Congressman, so thank you. The way that this would affect Apple is that it would affect our customers. It would affect everyone who owns an iPhone and it would create a risk for everyone who owns a phone that their data could be compromised if their security could be compromised.

With respect to the international question, I agree with you. I think America should be leading on this issue and I think that the world is watching what happens right now in our government and what happens even today with respect to this particular debate. Our ability to maintain a consistent position around the world, our ability to say that we will not compromise the safety and security of any of our users anywhere in world is substantially weakened

if we are forced to make that compromise here in our own country. So I urge this Congress and I urge the government, generally, to understand and to take a leadership role. Give us the strong support that we need to resist any effort by other governments to weaken security and privacy.

POE:
One of the questions that was asked, it was talking about what is your solution and I actually agree with Mr. Nadler. I know this is going to bother him a little bit, that there may be after all this litigation, then there may be a solution that we haven't thought of yet. But would not one option be Congress take into position that prohibits the back door key security system, the viper system, as I call it, from...

SEWELL:
Thank you, Mr. Poe.

POE:
I said that earlier but you stepped out. The viper system from being imposed, required, prohibit that from government requiring that type of system in specific technology like an iPhone.

SEWELL:
I think that is certainly one possibility, yes.

POE:
So prohibit the key. Let me consider -- ask you something else. If courts rule that you're required to develop the technology, develop the software, would that have -- would that software be able to be used on all those other hundreds of phones that are out there that the government lawfully has in their possession but they can't get into?

SEWELL:
Absolutely. There is nothing that would preclude it from being used on any iPhone that is in use today.

POE:
And my last question, would other countries, then if we -- U.S. takes the position thou shalt give government the key or what will other countries like China require or request or demand of Apple?

SEWELL:
So to date, we have not had demands like that from any other country. The only place that we're having this debate is in our own country. But I -- as I said before, I think if we are ordered to do this, it will be a hot minute before we get those requests from other places.

POE:
Right. Thank you, Mr. Chairman. I yield back.

GOODLATTE:
The chair thanks the gentleman and recognized the gentleman from Georgia, Mr. Johnson, for five minutes.

JOHNSON:
Thank you and I thank the witnesses for being here. Mr. Vance, what's the difference between a company being ordered to use its best efforts? I think the language is, let's see, an order, a court order requiring reasonable technical assistance. What's the difference between a court order requiring reasonable technical assistance to accomplish the bypassing or disabling of the auto-erase function versus a civil subpoena or a court order pursuant to a subpoena, motion to compel the delivery of information under that person's custody and control? Is there a difference?

VANCE:
I'm not sure, Congressman, there is a difference. They're both court orders that are directing an end result. One may be in a civil context, one in a criminal context. But I would say that in this discussion, it's very much a part of our history in America that when companies produce items or objects or commerce becomes ubiquitous in a particular area, that the company has to have a realization that part of the group of people who are using its products are using it to commit criminal purposes. Take a look at banking system, currency transaction reports.

So, we -- once it became obvious that criminals were moving cash through the banks, the response was you have to create and file transaction reports when cash is moved. So when a company -- when two companies like these two hugely successful and important companies own 96.7 percent of the world's smartphone market and we know that criminals are using the devices

to commit crimes, we've heard some of those stories, I don't think that it is new in American history or in the context of business ethics or oversight for companies to have to adapt to the realities of the product they've created.

JOHNSON:
Because they are the only ones that can -- a bank that received the cash would be the only entity in a position to submit a currency transaction report.

VANCE:
It would be the only one required to. If someone else had information about it, they could submit it but it would be the only one who had firsthand knowledge.

JOHNSON:
OK. Now, Mrs. Landau, is it your opinion that the government should not have the ability to compel Apple to use its best efforts to accomplish a technical feat? Is that your opinion?

LANDAU:
So there are two answers to that. If you're asking me as a lawyer question, then I'm not a lawyer and I'll dodge. But if you're asking me as a technologist, then I will say that it is a security mistake. It's a security mistake because that code...

JOHNSON:
Because what Apple would do would inherently cause an insecurity in their system.

LANDAU:
That's right. And it will be the target of organized crime and nation-states because it will be very valuable for somebody who puts a phone down as they go through customs, for somebody who goes to a business meeting and they're not allowed to bring their phone in because it's a meeting under a nondisclosure and the phone is sitting outside for a few hours, all sorts of situations, the phone will become very interesting and if there's code that can actually get into the phone and get the data, that code is going to be the target of nation-states...

JOHNSON:

So once Apple creates the code, then it makes it susceptible to being stolen and misused.

LANDAU:
That's right., that's right. There's not...

JOHNSON:
So, therefore, Apple should not be required to comply with the court order.

LANDAU:
I'm not answering a legal question. I'm answering the security question. The security question, it makes a real mistake.

JOHNSON:
Yeah, OK. And Mr. Sewell, you would agree with that?

SEWELL:
I would agree if we're forced to create this tool that it reduces the safety and security not within our own systems...

JOHNSON:
Well, now, let me ask you a question. What about the security and safety of those whose liberty can be taken and lives can be taken due to an ongoing security situation which the FBI is seeking to get access to information about? Do those -- is there an interest in the public security that we're talking about here?

SEWELL:
Congressman, that's what...

GOODLATTE:
The time of the gentleman has expired but Mr. Sewell may answer the question.

SEWELL:
That's what makes this such a hard issue because we're balancing two very different but very similar issues, private security, the security of people who use iPhones, the location of your children, the ability to prevent your children

from being kidnapped or harmed versus the security that's inherent in being able to solve crimes. So it's about how do we balance these security needs, how do we develop the best security for the United States. If you read the statements by general -- any of the encryption specialists today will say that defeaturing or debilitating encryption makes our society less safe overall. And so, that's what we're balancing. Is it the right thing to make our society overall less safe in order to solve crime? That's the issue that we're wrestling.

JOHNSON:
Thank you. I yield back.

GOODLATTE:
The chair recognized the gentleman from South Carolina, Mr. Gowdy, for five minutes.

GOWDY:
Thank you, Mr. Chairman. Mr. Sewell, you just mentioned the balancing. Can you give me a fact pattern where Apple would consent to the magistrate judge's order in California?

SEWELL:
Congressman, we will follow the law if we're ordered.

GOWDY:
NO, I'm asking for a fact pattern. You mentioned balancing. I want you to imagine a fact pattern where you balance the interest in favor of what the bureau is asking you to do as opposed to your current position. Give me a fact pattern.

SEWELL:
Congressman, what I said was we have to balance what is the best security for the country. Not balance when we should give law enforcement what they're asking, but balance what's the best security for the country.

GOWDY:
I thought that's what we were balancing is public safety versus privacy. You also mentioned the First and Fifth Amendment. Can you give me a fact pattern where Apple would consent to the order of the magistrate judge?

SEWELL:
Congressman, what I said was privacy, security, personal safety.

GOWDY:
Perhaps I'm being ambiguous in my asking of the question. Can you give me a fact pattern where you would agree to do what the bureau is asking you to do in California, whether it would be nuclear weaponry, whether it be a terrorist plot? Can you imagine a fact pattern where you would do what the bureau is asking?

SEWELL:
Where we would create a tool that doesn't exist.

GOWDY:
Yes.

SEWELL:
... in order to reduce the security and safety...

GOWDY:
Yes.

SEWELL:
... of our users.

GOWDY:
Yes.

SEWELL:
I'm not aware of such a fact.

GOWDY:
So there is no balancing to be done. You have already concluded that you're not going to do it.

SEWELL:

No, I've said we will follow the law. If a balance is struck, if there is an order for us to comply with, we will...

GOWDY:
There is an order.

SEWELL:
That order is being challenged at the moment as we speak. There's an order in New York that says...

GOWDY:
I'm glad you mentioned that. I'm glad you mentioned the order in New York. That's a drug case. So you would agree with me the analysis in drug cases is very different from the analysis of National Security Cases. And even if you didn't agree with that, you would agree that in footnote 41, the magistrate judge in New York invited this conversation about a legislative remedy which brings me back to Chairman Sensenbrenner's question, where is your proposed legislative remedy?

SEWELL:
So we don't have legislation to propose today, Congressman.

GOWDY:
Well then how will we know whether or not you think it strikes the right balance if you don't tell us what you think?

SEWELL:
Congressman, when we get to the point where we -- where it's appropriate for us to propose legislation, not just Apple, but the other stakeholders that engaged in this process, I'm sure there will be legislation.

GOWDY:
Well, let the record reflect, I'm asking you for it now. I would like you to tell us what legislative remedy you could agree with.

SEWELL:
I don't have an answer for you today. No one's had an answer to that.

Can you give me why? Can you -- I don't know whether apple has lobbyists. I suspect that you may have a government relations department. Possibly. Can you submit legislation to Chairman Sensenbrenner's question that you could wholeheartedly support and lobby for that resolves this conundrum between you and the bureau?

SEWELL:
It is my firm belief that such legislation can be drafted. I do not have language for you today, Congressman.

GOWDY:
Well, but see, Mr. Sewell, we draft it and then your army of government relations folk opposes it. So I'm just trying to save us time. The judge in New York talked about a lengthy conversation. Sometimes, circumstances are exigent where we don't have time for a lengthy conversation. So, why don't we just save the lobbying and the opposing of whatever, Cedric Richmond or Hakim or Luis and I come up with, why don't you propose it? Tell us what you could agree to.

SEWELL:
Congressman, we're willing to and we've offered to engage in that process.

GOWDY:
Well, the legislative process or with the debate process?

SEWELL:
Both, of course.

GOWDY:
Will you submit legislation to us that you could live with and agree with?

SEWELL:
If after we have the debate to determine what the right balance is, then I think that's a natural outcome.

GOWDY:
Well, how long is the debate going to last?

SEWELL:
I can't anticipate that, Congressman.

GOWDY:
Well, let me ask you this. You mentioned the First Amendment which I found interesting. Are you familiar with voice exemplars?

SEWELL:
I'm sorry, is that a case, Congressman?

GOWDY:
No. Voice exemplars are ordered by courts and judges for witnesses or defendants to actually have to speak so a witness can see whether or not that was the voice that they heard during a robbery, for instance. How about -- because you mentioned you have a First Amendment right to not speak. What about those who have been immunized and still refuse to cooperate with a grand jury and they are held in contempt and imprisoned? So there are lines of cases where you can be forced to speak.

SEWELL:
Congressman, we've made an argument, a constitutional argument, if the courts determine that that argument is infirm, then we will...

GOWDY:
I'm asking you whether or not you agree there are exceptions.

SEWELL:
You've given me two examples that I've not heard of before.

GOWDY:
All right, how about back to the Fifth Amendment because I'm out of time. Real quickly the Fifth Amendment you say you are being conscripted to do something. But there's also a line of cases where folks are conscripted to perform surgical procedures or cavity searches or other things I won't go into in mixed company where they are looking for contraband. So that's a nurse or a doctor or an anesthesiologist that is conscripted by the government. You would agree?

SEWELL:
I'm not familiar with these cases.

GOWDY:
All right, here's what I'll do. I'm out of time. I'll get you the cases I'm relying on if you'll help me with the legislative remedy. Deal?

SEWELL:
I look forward to the cases.

GOWDY:
Deal. Thank you.

GOODLATTE:
The time of the gentleman has expired. The chair recognized the gentleman from Florida, Mr. Deutsch, for five minutes.

DEUTSCH:
Thank you, Mr. Chairman. I would start by saying I don't -- this is really hard. I don't -- I'm not looking to Apple to write the legislation to balance these very difficult issues between privacy and public safety. It's -- I don't expect you to do it. I expect us to grapple with it. And that's what we're trying to do here today. And I had raised this point earlier but I -- it's a perfect lead-in to the questions I want to ask.

This focus on surgical procedures and we can force the government can force a surgical procedure to be done. It sounds like it's somehow equivalent and, well, certainly if we can do that, then we can require that a company create a way in to its phone. Except as I said earlier with Director Comey, that surgical procedure is going to be done by the person that the government says should do it and there is no one from around the world who from their remote location is going to be able to figure out how to conduct surgery on that individual. Yet in this case, and this is why this is so hard for me, in this case, there are people all over America and around the world who will be trying to figure out how to utilize whatever it is that's created here, if this is where this goes, to access the phone. And Director Comey earlier, Mr. Sewell, Director Comey said it's a three-step -- he believes it's a three-step process that they're asking. Can you just speak to that process?

I absolutely can. Thank you, Congressman. First, I agree with you that this is not a problem which -- there are people that are trying to break into these systems. There are people who are trying to steal this information if it existed. And their capabilities are increasing every day. So, this is not a threat which is static. This is a threat which is increasing. The three parts that we're being asked to develop are, first, a method to suppress the data deletion after ten failed attempts. The second thing that we're being asked to suppress is the time delay between successive attempts. Both of these are specifically tailored to deal with the situation where your phone is stolen or some bad person is trying to break into it and it's specifically designed to defeat the brute force attack.

DEUTSCH:
Right.

SEWELL:
The third piece is interesting because the third piece is the government asking for us to rewrite the code that controls the touch screen and allow them to put a probe into the phone and to bypass the need to enter numeric digits through the touch screen. The only reason that that makes sense, Congressman, is if you anticipate that this is going to be technology used on other phones and other phones that likely have more complicated passcode.

DEUTSCH:
Thanks. So, that's the question. And, Mr. Sewell, it's a question for you and, Mr. Vance, it's a question for you. And I -- this is one where if I believe -- if I understand that what's being asked of you is to create this way in to this one phone, then I want you to do it. I do. And I can get pass a lot of these privacy issues if I believe that it's once in and then can then be disposed or destroyed and that will be the end of it. The question is, is that the case? And when you create it for this one, is it something that can be used on other phones? Director Comey I don't think was clear about that, so I'd ask you that question. And, Mr. Vance, I'd ask you the same question.

VANCE:
If I can...

DEUTSCH:
Please.

VANCE:
... refer to actually the doctor's own paper, you need the phone physically at Cupertino to open it. And I refer you to her...

DEUTSCH:
I don't -- but I don't have much time. I'm not sure I understand what that means. I just want to know, cutting to the chase, I just want to understand if this is created, is it something that not just -- that could be used by you in the pursuit of justice, but by the criminal cyberterrorist hackers and really dangerous people who are looking to do bad things everyday of the year going forward?

VANCE:
Congressman, my point is simply that if this code is created and you were looking at the risk to other devices, other Apple phones in the world, those phones are going to have to come to Cupertino to be opened. This is...

DEUTSCH:
Well, let me ask Mr. Sewell before we -- I only have a couple seconds, left.

VANCE:
But that was incorrect...

DEUTSCH:
Well the -- but the question is even if that's correct, I'd like you to speak to it. Is it true that the hackers of the world, that there will be those that try to find a way to get around having to take the phone to Cupertino in order to conduct whatever operation is necessary to break in?

SEWELL:
Yeah. Unquestionably, Congressman, and that's exactly the risk and the danger that we foresee. With respect to the comment that Mr. Vance just made, in fact, the request that we got from the government in this case was that we should take this tool and piece -- put it on a hard drive and send the hard drive to the FBI. The FBI would then load that hard drive into a computer, hook the phone up to the computer, and they would perform the entire operation. So that this whole tool is transportable on a hard drive. So, this is a very real possibility.

DEUTSCH:
So, should we be concerned, Mr. Vance? I mean, look, I want to get into this phone but shouldn't we be concerned if that's accurate that there's something that's being created that's transported on a hard drive that winds up on another computer that there is at least the risk that that gets stolen and then -- and suddenly you -- there is -- not just into a bad person and these terrorists that we desperately want to get and get this information, but suddenly, all the rest of us who are trying to protect ourselves from the bad people and who are trying to protect our kids from these bad people are potentially at risk, too?

VANCE:
Congressman, I respectfully disagree with the colleague from Apple but I will confess that I -- you know, his knowledge of the company is great. Apple has created a technology which is default disk encryption. It didn't exist before. It exists now. Apple is now claiming a right of privacy about a technology that it just created that right of privacy didn't exist before Apple created the technology, number one.

Number two, I can't answer how likely it is that if the Federal Government is given a source code to get through the front door of the phone, that is at risk of going viral. I think it may be overstated to suggest that. But I can tell you this, if there's an incremental risk that providing the source code creates a vulnerability, what is that risk. Don't tell us just millions of phones might be affected. Tell us -- I think we can do better than just giving us broad generalizations without specifics.

But I can tell you this, the consequence -- the other side of the weight, the consequence is in cases all over the country right now in my jurisdiction, your jurisdiction, everywhere, families like the Mills family, are not getting justice. And the direct consequence of this disk encryption is that innocent victims all over the country are not getting their cases solved, prosecutors are not doing the job that they have been elected and sworn to do, and there is a significant consequence to default disk encryption that I think needs to be balanced against a speculative claim of increased insecurity.

LANDAU:
I'd like to just add a couple of comments. This is not about a new right of privacy. It's about a new form of security. And if we think about how the phones are used and increasingly how the phones are used, I certainly have

two factor authentications I use for my phone but there are ways of using the phone as the original authentication device.

And if you make the phone itself insecure, which is what is being asked for by law enforcement, you preclude that and that is the best way to prevent the stealing of login credentials, the use of a phone as authenticator.

In terms of the risk of the disk and so on, it's not the risk of the disk going out because the disk is tied to a particular phone. The risk is that somebody will come into Apple and provide a rogue certificate that they, you know, they're from law enforcement or wherever and will get the ability to decrypt a phone that should not be decrypted, whether it's the Chinese Government or an organized crime group or whatever. That's the risk we're facing.

VANCE:
May I -- Congressman, with the Chairman's permission?

DEUTSCH:
My time is up. The chairman has been generous.

GOODLATTE:
Well beyond the time, but briefly.

VANCE:
The professor has not answered what about the people, the residents, the citizens, the victims, whose cases are being put on the side and not addressed while we have an academic discussion, an important one?

DEUTSCH:
Well, it's an important academic discussion because before these phones existed, the evidence that you're talking about didn't exist in the form that you've had access to. Now the technology is moving to a new generation and we're going to have to figure out a different way to help law enforcement but I don't think we say we're not going to ignore these vulnerabilities that exist in order to not change the fact that the law enforcement is going to have to change the way it investigates and gathers evidence.

GOODLATTE:
The time of the gentleman has expired. The chair recognized the gentleman from Illinois, Mr. Gutierrez.

Thank you, Mr. Chairman. First of all, I'd like to ask through the chair if Congresswoman Lofgren has a need for any time, I'd like to yield to her first before mine.

LOFGREN:
Well, thank you very much. You know, I don't know you, Mr. Vance, but I'm sure you're a great prosecutor. I do know Mr. Sewell. He's a great general counsel but the person that really knows technology on the panel is Dr. Landau. And I'm interested in your comments about the vulnerabilities that would be created by complying with the magistrate's order. And some have suggested that it's speculative and, you know, academic and the like. But is that what your take on this is?

LANDAU:
Absolutely not.

LOFGREN:
And the theory -- I mean, we are moving to a world where everything is going to be digital. And you could keep track of, you know, my, you know, when I'm walking around the house I'm in, my temperature, opening the refrigerator, driving my car, and if that all is open to a legitimate warrant, I'm not downplaying the problem the prosecutors have but this is evidence you currently don't have access to. How vulnerable is -- are -- is our country going to be? That's the question for you.

LANDAU:
Extremely vulnerable. David Sanger's article in today's New York Times is about the Ukraine Power Grid says that they got in as I mentioned earlier through the login credentials. It's based on a DHS memorandum that talks about locking down various systems. I served for a number of years on NIST's Information Security and Advisory -- Security and Privacy Advisory Board and we used to talk to people from the Power Grid, and they would say, "Oh, it's okay, we're not -- our systems aren't connected to the internet." Well, they were fully connected.

We are -- whether you're talking about the Power Grid, the water supply, whatever, we're connected in all sorts of disastrously unsafe ways. And as I mentioned earlier, the best way to get at those systems is through login credentials.

Phones are going to provide the best way to secure ourselves. And so, this is not just about the personal safety of the data you have on your phone and it's not just about the location of where your family is, and it's not just about the business credentials, but it's really about the, as you say, Congressman Lofgren, it's really about the way that we are going to secure ourselves in the future. And what law enforcement is asking for is going to preclude those strong security solutions.

It also is a very much a 20th century way of looking at a 21st century problem. And I didn't get a chance to answer Congressman Gowdy, but the FBI, although it has excellent people, it hasn't put in the investment. So Director Comey said, we talked to everyone who will talk to us, but I was at a meeting -- I briefed at FCC a couple of years ago and some senior people from DOJ were there and I said, "Well, you know, NSA has scale X and Y." And DOJ said, they won't share it with the FBI except in exceptional circumstances." They keep it for themselves.

We're in this situation where I think law enforcement needs to really develop that skill -- those skills up by themselves and then that you ask about what it is this committee can do. It's thinking about the right way for law enforcement to develop those capabilities, the right level of funding. The funding is well below what it should be but they also don't have the skills.

GUTIERREZ:
Thank you. So, I'm happy I yielded the time to you. I always know it's one of the smartest things I do is work with Congresswoman Lofgren on this committee. But I just want to share with you, look, I understand the competing interests here. But I think, Mr. Sewell, you should understand that I love your products. You know, I used to think, you know, house, then a car, now I think technology between what they charge me for the internet, all the stuff I buy, just to get information everyday, it's -- but don't worry, I can afford it. I'm not going into the poorhouse because of it. So I'm excited about all of the new things that I get to and how it improves my life.

And so I'm thankful to men and women in technology for doing that. But a lot of times in this place, there's adversarial positions taken and I would hope simply that we would look for a way in which we put the safety interests of the American people. I understand that you think that if we find a back door that that causes all kinds of insecurities. But in this committee, I'm going to work with Congresswoman Lofgren but I'm also going to work with Trey Gowdy.

We're going to work a lot of time bipartisanship and this place has many times promote it but very, very rarely rewarded in this place because everybody is, "Oh, you should take one position or another." I'm going to take a position for the American people. While you might dispute, I kind of look at Apple as an American company. I look at Toyota as a Japanese company, BMW as a German. I look at you as an American company. And so, that's the way I see you, you can dispute that. You may look at yourself as an international entity, but I always look at you as U.S. pride.

When I take this phone as a member of the intelligence committee and I take this phone to China, the intelligence community of the United States, the first thing before I get off that plane, they take it away from me.

So there are bad actors out there already intervening with your products or I don't think the fine people of the intelligence community would take away one of the things that I need the most in my life. So having said that, I hope we might find a way so that we could balance the security needs and the safety needs of the people of the United States and their right to privacy. I think it's essential and important. I want to thank you guys for coming and talking to us and let's try to figure it out all together. Thanks.

SEWELL:
Thank you, Congressman. And I absolutely I agree with what you said, and I think that -- I am proud to work for Apple and I think Apple embodies so many of the most valuable characteristics that make up America, make America a great place. We stand for innovation. We stand for entrepreneurship, we stand for empathy. We stand for all boats rising.

So, I'm very proud. And we are an American company and we're very, very proud of that. The point about security outside of the United States is exactly the point that drives us. We are on a path to try to create the very best, most secure and most private phones that we can. That's a path that will probably never end because the people that we're competing with, the bad guys not just in the United States but all over the world, are on an equally aggressive path to defeat everything that we put into the phone. So we will continue from generation to generation to improve the technology, to provide our users with a safer experience.

GUTIERREZ:
Thank you, Mr. Chairman.

GOODLATTE:

The gentleman from Louisiana, Mr. Richmond, is recognized for five minutes.

RICHMOND:
And I'm happy to follow Luis, because I guess we're going to start -- I'll start where he left off and I think about a 9- year-old girl who asked, you know, why can't they open the phone so we could see who killed my mother because I was there and heard it happen? So, let me start with this. If the FBI developed the ability to brute force open a phone, would you have a position on that?

SEWELL:
Without involving Apple, without having Apple...

RICHMOND:
Yes.

SEWELL:
... complicit (ph) in that. I don't think we have a position to object or not object to that. I think if the FBI has a method to brute force a phone, we have no ability to stop them.

RICHMOND:
But are you okay with it?

SEWELL:
Well, I think that privacy and security are vitally important national interests. I think that if you weaken the encryption on the phone, then you compromise those vital importance.

RICHMOND:
I'm not asking you about the encryption. If they could brute force open a phone, do you have a problem with that? Is this -- it's -- I think that's just an easy question.

SEWELL:
Then, I'm sorry, perhaps I'm misunderstanding. If the FBI had the ability to brute force a phone, I would suggest that that's the security vulnerability in the phone. So, I would have a problem with it, yes.

RICHMOND:
Let me ask you another question, because I see you're a lawyer, I'm a lawyer. And I would feel awful if I didn't ask this...

LANDAU:
Can I just say something for a second?

RICHMOND:
In a second. Let me get through this question. Brittany Mills had a 5S phone operating on an 8 -- with 8.2 IOS. Does Apple, any employee, subcontractor, subsidiary or anyone that you know of possess the knowledge or the ability to open that phone or unlock that phone?

SEWELL:
We don't and I am glad that you asked about the Mills case because I think it's instructive about the way that we do work together cooperatively. I know that we met with members of your staff...

RICHMOND:
Look, and I'm not suggesting that you all don't. But I just want to know, does anybody have the ability to unlock the phone, first? And if you tell me no, then I get a no in public on the record and I feel a lot better about what I'm doing.

SEWELL:
Let me be clear. We have not said that we cannot create the tool that the FBI has asked us to create.

RICHMOND:
Right. No, I'm not asking about creating anything. I'm saying, does it exist now? Do you know anybody or does anyone have the ability to do it right now?

SEWELL:
Short (ph) of creating something new, no.

RICHMOND:

Now, in a -- oh, I'm sorry, Miss. I promised to let you answer.

LANDAU:
I just wanted to add that in security, we have an arms race. People build good products, somebody finds a vulnerability. It could be the FBI. It could be not the FBI. I may not tell anybody about the vulnerability, but we have this arms race where as soon as somebody finds a problem, the next roll of technology comes out and that's the way we do things.

RICHMOND:
So what would be your feeling if the FBI developed the technology that they can plug something into the iPhone?

LANDAU:
I think that the FBI should be developing the skills and capabilities to do those kinds of investigations. I think it's absolutely crucial and I think that they have some expertise but it's not at the level that they ought to have. And I think we're having this conversation exactly because they are really using techniques from -- they're using a mindset from long ago, from 20 years ago rather than the present.

RICHMOND:
So they're antiquated?

GOODLATTE:
Will the gentleman yield?

RICHMOND:
Sure.

GOODLATTE:
Because I just want to clarify both Mr. Sewell and Ms. Landau did not say subject to the unauthorized court order warrant.

LANDAU:
Well, I certainly did not subject to that.

GOODLATTE:

They're not suggesting they develop this technology and then do what they think is they best. They have to do it subject to a warrant.

LANDAU:
Of course, thank you.

RICHMOND:
And I am glad you cleared that up because I want to make sure that everybody understands what I'm saying.

I don't think any of this should happen without a court order. Now, you know, maybe I watch too many movies and maybe I listen to Trey Gowdy too much, some people would suggest if I listen to him at all, that's too much. But in the instance that there's a terrorist that has put the location of a nuclear bomb on the phone and he dies, how long would it take Apple to develop the technology to tell us where that nuclear bomb was? Or would Apple not be able to develop that technology to tell us in a short period of time?

SEWELL:
The first thing we would do is to try to look at all of the data that surrounds that phone. There is an enormous change in the landscape over the last 25 years with respect to what law enforcement has access to. So when we have an emergency situation like that, whether it be a lost child or the airplane, when the Malaysia Airline went down, within one hour of that plane being declared missing, we had Apple operators cooperating with telephone providers all over the world with the airlines and with local, well, the FBI to try to find a ping, to try to find some way that we could locate where that plane was. So the very first thing that we would do in this situation is to bring to bear all of the emergency procedures that we have available at Apple to try to find it.

RICHMOND:
Thank you. Mr. Chairman, can I just clarify, because I don't want anyone to leave out of here thinking that Apple has not been cooperative with our district attorney in the effort to access the data. And, in fact, they came up with new suggestions. But my questions are just about the government's ability to just brute open a phone at any point with a court order. So, I don't want to suggest that Apple has not been working diligently with my DA who has also been working diligently, thank you, Mr. Chairman. I yield back.

SEWELL:
I appreciate that, Mr. Congressman.

GOODLATTE:
The chair thanks the gentleman. And I recognize the gentlewoman from Washington State, Ms. DelBene, for five minutes.

DELBENE:
Thank you, Mr. Chairman. Thanks to all you for being here and for enduring this for a while. It's very, very important. In the earlier part of the hearing, Director Comey said that it is not a company's job to worry about public safety and I think that that is -- would be very concerning for a company to send that message given that we have technologies that impact people's everyday lives in so many ways and I assume you agree with that, Mr. Sewell.

SEWELL:
I absolutely do. I do not subscribe to the position articulated by Director Comey.

DELBENE:
I worked at Silicon Valley Companies, Sun Microsystems and Google and that's certainly not what I saw in either of them.

In the Brooklyn case decided yesterday, Judge Orenstein stated in his opinion that the world of the internet, of things the connected devices on sensors that we see coming forward, the government's arguments would lead quickly to a world of virtually limitless surveillance and intrusions on personal privacy. So I'd like to explore the issue of encryption and securing the internet of things a little bit.

We often talk about security by design when it comes to the internet of things and I'm sure we can all imagine the horror stories of insecure internet of things types of devices like appliances being hacked to cause a fire or spying through baby monitors, hacking into a car or tampering with a home security system.

So, I'm wondering, Dr. Landau, I'm wondering if you could comment on what it means in the encryption context and whether directives we've heard from the FTC, for example, to adopt security by design in the interest of protecting consumers from malicious actors is inherently incompatible with what you might call insecurity by design should that be mandated by the courts?

LANDAU:
Well, here you're in a situation where the companies often want to collect the data. So, for example, if you're using smart meters, the company wants the data. The electric company wants the data to tell your dishwasher, "No, don't turn on at 4:00 in the afternoon when air-conditioning requirements are high in Silicon Valley right now, turn it on at 8:00 at night or 2:00 a.m.

And so, in fact, it actually wants the individualized data and if it has the individualized data then it can certainly share it with law enforcement under court order.

The security by design is often in the internet of things, securing the data on the device and securing the transmission of the data elsewhere. The issue in the Apple phone is the data stays on the device and that's the conflict that we're having. For the internet of things, it's most useful if the data goes off the device to somewhere elsewhere, where it can be used in a certain way.

DELBENE:
And, Mr. Sewell, could companies open themselves up to liability if vulnerabilities for law enforcement end up being exploited by a bad actor?

SEWELL:
I think that's absolutely true. Somewhat ironically I suppose we have the FTC at this point actively policing the way in which technology companies deal with these issues and we can be liable under the section 5 or under the authority of the FTC if we fail to close a known vulnerability.

DELBENE:
And, Ms. Landau, you talked about the question of security versus -- or the issue of security versus security. And that this really is a debate about security versus security. Could you explain a little bit more why...

LANDAU:
Sure.

DELBENE:
... our national security and cybersecurity incompatible in your opinion?

LANDAU:

So, what we really have here over the last 20 years as I mentioned earlier is you see the NSA and Snowden revelations aside, we don't have time for me to describe all of the subtle points there, but you really see the NSA working to secure private sector telecommunications infrastructure, many, many examples.

We have moved to a world of electronic devices, you talk about the internet of things, that leak all sorts of data. And in order to protect ourselves, whether ourselves, our health data or our bank data, the locations of our children and so on, we need -- we need encryption and so on. But if you think more broadly about the risks that our nation faces and the risks of people coming in and attacking the power grid, people coming in and stealing data from whatever company and stealing patented information and so on, you see a massive national security risk. And you've been hearing it from General Keith Alexander, we've been hearing it from Hayden, we've been hearing it from Mike McConnell, we've been hearing it from Chertoff, all the people who have been involved on the DHS and NSA side.

The only thing that can secure that is security everywhere and the move that Apple makes to secure the phones is one of the many steps we need in that direction.

DELBENE:
Thank you. My time's expired. I yield back, Mr. Chair.

GOODLATTE:
Thank you. I'm going to recognize myself for some questioning, so welcome in.

I'm sorry, Mr. Sewell, pronouncing that name correctly?

SEWELL:
You are.

GOODLATTE:
All right. I have some questions for you concerning China.

In 2014, you moved your -- what's referred to as your Chinese Cloud to China, is that correct?

SEWELL:

That is correct.

GOODLATTE:
Okay. And can you -- can you tell me who's data is stored in that Chinese Cloud? Is it just people in China? Is my data stored in that Cloud as well?

SEWELL:
Your data is not stored in that Cloud.

GOODLATTE:
Is it strictly limited to Chinese people?

SEWELL:
There are a number of things that in the cloud, so I should probably be clear about what's there.

GOODLATTE:
Okay.

SEWELL:
With respect to personal data, no personal data is there unless the individual's data -- the individual himself has registered as having a Chinese address and having a Chinese access point. In addition, we have other data which has to do with film content, movies, books, iTunes, music. The reason we do that is because of something called latency. If you're streaming across the internet and you have to bring the data from the United States to China, there's a live time, there's a latency piece, whereas if we move that data closer to China either Hong Kong or Mainland China, then we can provide a much better service to our customers.

MARINO:
OK. Can you tell me, what was the cost in the ballpark figure in the time to make the move to -- from the United States to move Chinese information over to China and their Cloud?

SEWELL:
I'm sorry, did you say in time?

MARINO:
Cost in time.

SEWELL:
So, the time -- the cost is building the facilities. I don't have a number for that. It's certainly not something that I'm aware of, although, of course, the company has that information. In terms of the time, once the server exists, once there is a receptacle for the data in theory it's instantaneous.

MARINO:
OK. You may or may not know but I was a prosecutor for a while both at the state and federal level and we prosecutors are focused on the case and the crime concerned and we want to get our hands on anything we can to see that justice is served. But on the other side of this, too, we're talking about privacy issues. And I'm very concerned about to what extent if for some reason you were to change your mind about working with the FBI or the court ordered that, what does that mean to our privacy?

SEWELL:
I think it means that we have put our privacy at risk. The tool that we're being asked to prepare is something which could be used to defeat both the safety and the privacy aspects of the...

MARINO:
Let me get this clear, because there are many rumors flying around, and you probably into his couple times, and I apologize, I had to run and do something else. Are you saying that there is no method that exists now that you could unlock that phone and let the FBI know what is in there?

SEWELL:
Short of creating the tool that they have asked us...

MARINO:
Right.

SEWELL:
We are not aware of such a method, you know.

MARINO:
Now, you talk about the cost is an unreasonable burden and the time involved, that's why I asked you what did it cost to move the Cloud, what was the time, and you're the expert. I'm not.

SEWELL:
Congressman (ph), to be fair, we haven't claimed that the time that it would take to create the tool is the undue burden. Our claim is that the undue burden is to compromise the safety and security of all of our customers.

MARINO:
So, it's your position that if you do what the FBI wants to one phone, could you elaborate on that in the 33 seconds I have left as to why that would be an undue burden, keeping in mind that, I'm very critical about our privacy.

SEWELL:
Congressman, the answer is very simple. We don't believe this is a one-phone issue. We don't believe it can be contained to one phone or that it would be contained to one phone.

MARINO:
OK. I see that my time is just about run out, so I'm going to yield back and who's next? Mr. Jeffries, Congressman Jeffries, is next.

JEFFRIES:
Thank my good friend from Pennsylvania for yielding.

I want to thank all the witnesses for your presence here today. It's been very informative discussion. In particular I want to thank D.A. Vance for your presence and certainly for the many progressive and innovative programs that you have in Manhattan, proving that you can be both tough and fair as a prosecutor and that has not gone unnoticed.

Let me start with Mr. Sewell, there's an extensive record of cooperation that Apple has with law enforcement in this San Bernardino case, isn't that fair to say?

SEWELL:
That's correct. For over 75 days we've been working with the FBI to try to get more information and try to help solve this crime.

JEFFRIES:
I think it's useful to put some of this on the record. On December 5th, the Apple emergency 24/7 call center received a call concerning the San Bernardino shooting, is that right?

SEWELL:
That's right. In fact, the call came in to us at 2:47 a.m. on a Saturday morning. We have a hotline that exists. We have people that are manning that hotline.

JEFFRIES:
And you responded with two document productions, is that correct?

SEWELL:
By 2:48 that morning, we were working on the case and we responded by giving the FBI all of the information that we could immediately pull from our sources and then we continued to respond to subpoenas and to work directly with the FBI on a daily basis.

JEFFRIES:
Right. In fact, the next day I think Apple received a search warrant for information relating to at least three e-mail accounts, is that right?

SEWELL:
That's correct.

JEFFRIES:
And you complied with that request?

SEWELL:
We did comply with that and subsequent requests.

JEFFRIES:
And so I think also on January 22nd, you received another search warrant for iCloud information related to the iPhone that was in position of the male terrorist, is that right?

SEWELL:
That's right and it's important that in the intervening stage, we had actually sent engineers to work directly with FBI technicians in Washington, D.C. and Cupertino. And we provided a set of alternatives or options that we thought should be tried by the FBI to see if there might be some possibility that we could get into this phone without having to do the tool that we're now being asked to create.

JEFFRIES:
So the issue here is not really about cooperation as I understand it. Apple has clearly cooperated in an extensive fashion as it relates to all of the information that you possess. The question I think that we all on the judiciary committee and beyond have to consider is the notion of you being asked as a private company to create anti-encryption technology that currently does not exist and could jeopardize the privacy and security of presumably hundreds of millions of iPhone users throughout the country and the world, is that right?

SEWELL:
We're being asked to create a method to hack our own phones.

JEFFRIES:
Now, Mr. Vance, are you familiar with the Arizona v. Hicks Supreme Court case from the late '80s.

VANCE:
If you give me the facts, I'm sure I will have read it.

JEFFRIES:
OK. Well, the Supreme Court held that the police conducted an unconstitutional search of evidence that was not in plain view. It was a decision that was written by Justice Antonin Scalia and the most important point that I want you to reflect upon is he stated, "In authoring the majority opinion, that there is nothing new about the realization that the constitution sometimes insulates the criminality of the few in order to protect the privacy of us all."

Do you agree that embedded in the fabric of our constitution, the Fourth Amendment and beyond, is the notion that we value the privacy rights of Americans so deeply that at times it is something that will trump law

enforcement convenience?

VANCE:
Congressman, I do sincerely believe that. What concerns me about the picture we are seeing from the state perspective is that Apple has decided that it's going to strike that balance now with no access by law enforcement for full disk encrypted devices even with a warrant. So, they have created their own balance. They now have decided what the rules are. And that changes radically, the balance that existed previously. And it was done unilaterally so this could be...

JEFFRIES:
Well, I think -- if I can just interject. I mean I think that that's a balance that ultimately the Congress is going to have to work out and also the article three court systems certainly beyond an individual magistrate who is not even appointed for lifetime tenure is going to have to work itself through the court system. A district court judge and maybe the ninth circuit, ultimately the Supreme Court.

And so, the company exercising its right in an adversarial system to have all facts being aired on both sides of the debate is very consistent in my view with American democracy and jurisprudence. Just one last question that I wanted to ask as my time is expiring. Because you raised an interesting point earlier in your testimony about an individual who is a suspected criminal who claimed that the encryption technology was a gift from God. But I also noted, I think, in your testimony that this individual communicated that, in an intercepted phone conversation that presumably your office or others were wiretapping. Is that right?

VANCE:
No. It's not right. All phone calls from prison, out of Rikers, are recorded.

JEFFRIES:
Right.

VANCE:
And there's a sign when you pick up the phone, if you are in Rikers Island that this is happening. So, there's a tape. And ultimately that tape was subpoenaed, and it's from that tape that that conversation was transcribed.

JEFFRIES:
And if I could just -- in conclusion, I appreciate the chair's indulgence. I mean I think that illustrates the point. Presumably that it's fair to say that in most instances bad actors will make a mistake. And at the same time that he's heralding the availability of encryption technology to shield his activity from law enforcement, surveillance and engagement, he's ignoring a plain view sign that these conversations are being recorded and subjecting himself to unfettered government surveillance.

And I think that I have faith in your ability and the FBI's ability ultimately to outsmart the criminals and the bad actors without jeopardizing the privacy and security of the American people.

VANCE:
And in that case, our challenge is because of our inability to access the phone, our inability to investigate further any evidence of sex trafficking, is not made available to us. So yes, he did something that was not smart. But the greater harm is the inability, in my opinion, of being able to get to the true facts which in fact are extremely important as matter of public safety to get access to.

JEFFRIES:
My time is expired. I thank you.

GOODLATTE:
I thank the gentleman from New York and the chair recognized now the gentleman from Rhode Island, Congressman Cicilline.

CICILLINE:
Thank you Mr. Chairman. Thank you to our witnesses for your testimony. These are very important discussion.

I think we all recognize there are few be absolute in the law and so balancing, you know, occurs all the time. There are risks in developing the software that have been articulated very well during this hearing and indeed there are risks associated with inability to access critical information. So that, I think we are living in a world with our risks in both ways forward.

And I guess my first question is, many people who agree that Apple or any other company should not be required, and there's no authorization to require them, to produce a product that doesn't exist or to develop an intellectual property that doesn't exist. Many people who think that that's

correct wonder whether Apple has considered in limited circumstances and maybe a standard you would set internally, if it in fact is a situation that would prevent immediate death or serious bodily injury coupled with a consent of the person or lack of objection.

In this case, this person is deceased, where there is no privacy claim asserted, in some very narrow category, whether there's a set of protocols you might voluntarily adopt to provide that information or that software within instructions that it be immediately destroyed if they done in a skip in a security. I mean is that practical, something like that? Should that be part of this discussion that we keep hoping that the industry and the justice department will have and trying to develop something or is that fraught with so many problems that's...

SEWELL:
Thank you for the question Congressman.

We have, and spend a lot of time thinking about, how we can assist our customers in the event that they have a problem, if they've lost a phone, if they are in a situation where they are trying to recover data. We have a number of mechanisms to do that and we will continue to improve those mechanisms as we move forward. It's very important to us that we try to think about the consequences of the devices that we create.

In this particular case, the pass code unlock is not something that we think lends itself to a small usage. The problem with this particular issue is that once you take that step, once you create the mechanism to unlock the phone, then you have created a back door and we cannot think of a way to create a back door that can only be used beneficially and not be used by that thing.

CICILLINE:
So you have in fact already contemplated other ways in which you could make this information available in this case that would not have those sorts of broader implications.

SEWELL:
And we have provided information in this case. We have provided logs. We have provided iCloud backup. We've provided all the things that at our disposal.

CICILLINE:

Thank you. (inaudible), you say in your written testimony, the point is that solutions to accessing the data already exist with the forensic analysis community. We did ask Director Comey and we probably limit our question too narrowly because we ask about the intelligence communities of the United States. It sounds like you're suggesting that there may be capabilities outside the United States government that the justice department or the FBI could contract with that are capable of doing what it is they are asking a court to order Apple to do.

LANDAU:
That's right. So I noticed when Director Comey answered the question, he said, we talk to everyone who will talk with us and as I mentioned earlier, I don't know if you were here at that point, I had a conversation with some senior DOJ people a few years ago about using NSA tools in law enforcement cases and they said, NSA is very low to share because of course when you share a tool, it can get into a court case and then the tool is exposed.

And so I don't know in the -- we talked with everyone who will talk with us, how much NSA revealed about what they know and what they can do. So that's the first place I would ask. Now, I phrased let me correct it. That's the first place that I suspect have some tools for exactly this problem.

But yes, there were discussions last week in Silicon Valley. There's been discussions I've had with colleagues, where people believe as Congressman Issa put various potential solutions that there are ways to break in to the phone. There is of course a risk that data might be destroyed. But I have described both in my written and verbal testimony, the FBI has not tried to develop this level of expertise, and it should.

CICILLINE:
It seems that you know, we are contemplating whether or not Congress should take some action to either grant this authority and then figure out what is the appropriate standard and test et cetera. It sounds as if you think that is problematic and that in fact the real answer is a substantial increase investment in the intelligence capability, the law enforcement capability that sort of keeps pace with the advances that come is like Apple are making. But that's really the best protection in terms of both law enforcement and the long-term security in the United States.

LANDAU:

That's right. I don't think actually there needs to be more authority but there needs to be a completely different view of how it's done. There's probably needs to be some authority in terms of how do you handle it for state and local because state and local will not have the resources. And so there have to be some sort of sharing of tools and not as jurisdictional issue and also, you know, an issue between bureaucracies that we'll have to work out and that we'll be have to work out for law and policy.

But in terms of creating new authority, the FBI already has that authority. But if users that at a much lower level and it should expanded in a much lower level, they need to move from the situation they're in to dealing with the 21st century technologies in the appropriate way.

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

GOODLATTE:
You bet. Chair recognizes Lofgren California.

LOFGREN:
Could I ask just one quick question, Mr. Sewell. I forgot when it was my turn. And we had asked Mr. Comey, somebody asked Mr. Comey about the changing of the password of apparently the county did at the request of the FBI. What did that do? Can you explain what happened?

SEWELL:
Certainly, one of the methods that we might enable the phone in San Bernardino, to do what's called the auto back up, that issue that the FBI is struggling with, is to find data between a certain time frame, the time of the last backup and the time of the horrific incident in San Bernardino. If the phone would back up, that evidence, that information would become available to the FBI.

The way that we can back these phones up in an automatic way is we connect them to a known Wi-Fi source. A source that the phone has already connected to before and recognizes. If you plug the phone in and you connect it to a known Wi-Fi source, it will, in certain circumstances, auto backup.

And so the very information that the FBI is seeking would have been available and we could have pulled it down from the Cloud. By changing the password, this is different from the pass code, but by changing the pass

word, it was no longer possible for that phone to auto backup.

LOFGREN:
Thank you. And thank you Mr. Chairman, for letting me get that information out.

MARINO:
Mr. Sewell, I have one more question for you. Does the Chinese government have access to the Cloud or is there any indication that they've tried to hack the Cloud in China to get information on the Chinese people?

SEWELL:
Let me be clear about the question. The Chinese undoubtedly have the ability to access their own Cloud.

MARINO:
Yes.

SEWELL:
But with respect to the U.S. Cloud, we believe that -- again, I'm struggling because of the words. The Cloud is a synonym for the Internet. So of course Chinese people have access to the Internet. Are we aware of a Chinese hack through Apple? No.

MARINO:
OK.

SEWELL:
But beyond that, I can't say.

MARINO:
You answered my question. Thank you.

GOODLATTE:
This concludes today's hearing. I want to thank the panel very much for being here. Without objection, all members, we have five legislative days to submit additional questions for the witnesses or additional materials for the record.

The hearing is adjourned.

CQ Transcriptions, March 1, 2016

List of Panel Members and Witnesses

PANEL MEMBERS:
REP. ROBERT W. GOODLATTE, R-VA. CHAIRMAN

REP. LAMAR SMITH, R-TEXAS

REP. JIM SENSENBRENNER, R-WIS.

REP. DARRELL ISSA, R-CALIF.

REP. J. RANDY FORBES, R-VA.

REP. STEVE KING, R-IOWA

REP. TRENT FRANKS, R-ARIZ.

REP. LOUIE GOHMERT, R-TEXAS

REP. JIM JORDAN, R-OHIO

REP. TED POE, R-TEXAS

REP. JASON CHAFFETZ, R-UTAH

REP. STEVE CHABOT, R-OHIO

REP. TOM MARINO, R-PA.

REP. TREY GOWDY, R-S.C.

REP. RAUL R. LABRADOR, R-IDAHO

REP. BLAKE FARENTHOLD, R-TEXAS

REP. DOUG COLLINS, R-GA.

REP. RON DESANTIS, R-FLA.

REP. MIKE BISHOP, R-MICH.

REP. KEN BUCK, R-COLO.

REP. JOHN RATCLIFFE, R-TEXAS

REP. DAVE TROTT, R-MICH.

REP. MIMI WALTERS, R-CALIF.

REP. JOHN CONYERS JR., D-MICH. RANKING MEMBER

REP. JERROLD NADLER, D-N.Y.

REP. ZOE LOFGREN, D-CALIF.

REP. SHEILA JACKSON LEE, D-TEXAS

REP. STEVE COHEN, D-TENN.

REP. HANK JOHNSON, D-GA.

RES. CMMSR. PEDRO R. PIERLUISI, D-P.R.

REP. JUDY CHU, D-CALIF.

REP. TED DEUTCH, D-FLA.

REP. LUIS V. GUTIERREZ, D-ILL.

REP. KAREN BASS, D-CALIF.

REP. CEDRIC L. RICHMOND, D-LA.

REP. SUZAN DELBENE, D-WASH.

REP. HAKEEM JEFFRIES, D-N.Y.

REP. DAVID CICILLINE, D-R.I.

REP. SCOTT PETERS, D-CALIF.

WITNESSES:
BRUCE SEWELL, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, APPLE, INC.

SUSAN LANDAU, PROFESSOR, WORCESTER POLYTECHNIC INSTITUTE

CYRUS R. VANCE JR., DISTRICT ATTORNEY, NEW YORK COUNTY
