Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

TESTIMONY ON CYBERSECURITY
AND U.S. NATIONAL SECURITY

Thursday, July 14, 2016

Washington, D.C.

ALDERSON COURT REPORTING
1155 CONNECTICUT AVENUE, N.W.
SUITE 200
WASHINGTON, D.C. 20036
(202) 289-2260
www.aldersonreporting.com

TESTIMONY ON CYBERSECURITY AND U.S. NATIONAL SECURITY

Thursday, July 14, 2016

U.S. Senate

Committee on Armed Services

Washington, D.C.

The committee met, pursuant to notice, at 9:33 a.m. in Room SD-G50, Dirksen Senate Office Building, Hon. John McCain, chairman of the committee, presiding.

Committee Members Present: Senators McCain, Ayotte, Fischer, Cotton, Ernst, Sullivan, Reed, Nelson, McCaskill, Gillibrand, Blumenthal, Donnelly, Hirono, Kaine, and King.

OPENING STATEMENT OF HON. JOHN McCAIN, U.S. SENATOR FROM ARIZONA

Chairman McCain: Good morning to all of our witnesses. We are pleased to have with us a distinguished panel of expert witnesses who each bring a unique perspective to this important issue of cybersecurity, encryption, and U.S. national security: Cyrus Vance, Jr., who currently serves as Manhattan district attorney; Chris Inglis, former deputy director of the National Security Agency and a professor cybersecurity studies at the U.S. Naval Academy; and Kenneth Wainstein, a former homeland security adviser and assistant attorney general for national security at the Department of Justice during the Bush administration and now partner at Cadwalader.

I am sure it is a great organization.

[Laughter.]

Chairman McCain: I thank each of our witnesses for appearing before the committee today.

I must note for the record that these were not our only invited guests. This committee extended an invitation to Apple CEO Tim Cook to offer his perspective on these important issues. He declined.

I hope he will reconsider in the future so that this committee can benefit from the widest possible variety of perspectives.

End-to-end encryption allows communications and data shared across devices and platforms to be seen only by the individuals holding the device. The information on the device cannot be accessed in most cases by the company and in nearly all cases by the government, even with a lawful court order backed by probable cause.

Major American tech companies have made this level of encryption the default setting on their devices, meaning that even the least sophisticated lone wolves can operate in digital secrecy.

Terrorist groups like ISIL have taken notice. ISIL's backward ideology and brutal tactics may be a throwback to medieval times, but these terrorists are also effectively using modern technological tools. Indeed, encryption is now ubiquitous across the counterterrorism fight, providing an avenue for recruitment and radicalization, as well as the planning and coordination of attacks that pose an increasingly difficult challenge to intelligence collection, military operations, and law enforcement.

Put simply, encryption is eroding the digital advantage our national security and intelligence officials once enjoyed. That is why the topic of encryption concerns the Senate Armed Services Committee.

But we must also recognize that encryption is not just a national security issue concerning terrorists in distant

lands. Encryption is being used to shield criminals that terrorize communities across the Nation every day.

As Mr. Vance will testify, there are thousands of lawfully seized iPhones and other devices in the hands of law enforcement today that are completely inaccessible because their manufacturers refuse to comply with court-issued search warrants. The result is that thousands of murder, child sex abuse, and human trafficking cases are not being fully investigated.

Let there be no doubt the job of our national security agencies and our local, State, and Federal law enforcement is getting harder and the threat is growing. However, this is a complex problem with no easy solutions.

Encryption technology protects our most common and essential day-to-day Internet activities and safeguards our Nation's secrets from sophisticated cyber adversaries. We must carefully balance our national security needs and the rights of our citizens.

While we must recognize that authoritarian regimes are eager to gain keys to encrypted software so they can further their own abusive policies, we must also resist slipping into a false moral equivalence. Not all governments are the same. Not all surveillance is the same. Complying with valid search warrants in countries that uphold the rule of law does not create an obligation for tech companies to

assist repressive regimes that undermine the rule of law in suppressing dissent or violating basic human rights.

Yes, this is a difficult problem. But ignoring this issue is not an option, nor is meeting all efforts to reach a middle ground with absolute resistance as too many tech companies have done.

An all-or-nothing approach to encryption that is making it difficult and sometimes impossible to prosecute murderers, pedophiles, human traffickers, and terrorists is simply unacceptable.

I believe there is a growing recognition that the threat posed by the status quo is unacceptable and that we need the public and private sectors to come together to eliminate cyber safe havens for terrorists and criminals.

The struggle between security and privacy, or between public and private goods, is not new. These struggles are as old as our republic. We have not always gotten it right, but when we found that balance, it has always been through open and honest dialogue. That is what we need right now.

Beyond encryption, I remain concerned by the administration's failure to provide the Department of Defense, the National Security Agency, and others with the necessary policy guidance to effectively defend, deter, and respond to our adversaries in cyberspace.

To be sure, there has been important progress,

including the willingness of the administration to carry out and more openly discuss offensive cyber operations against ISIL. Still, policy deficiencies from deterrence to rules of engagement to arbitrary limitations on geographic areas of operations, and cyber collateral damage, all must be addressed.

Rather than answering these hard policy questions, it seems the White House continues to micromanage every cyber issue on a case-by-case basis.

Finally, as the role of Cyber Command continues to mature, some have suggested that we should reevaluate the "dual-hack" relationship between Cyber Command and NSA. Whether in the context of possibly elevating Cyber Command to a unified command or in its current role, we must be careful not to prematurely sever this important relationship.

I welcome the views of our witnesses, especially Mr. Inglis, as to whether, at some point in the future, it may make sense for Cyber Command to stand independent of NSA.

Once again, I thank our witnesses for their appearance before the committee today. I look forward to their testimony.

Senator Reed?

STATEMENT OF HON. JACK REED, U.S. SENATOR FROM RHODE ISLAND

Senator Reed: Thank you very much, Mr. Chairman, for having this second hearing on encryption. I, too, want to welcome our trio of very distinguished witnesses and thank them for their many years of service to the Nation.

Mr. Vance, your leadership on this issue is commendable and your statement eloquently articulates your position. I also want to note that District Attorney Vance is advocating for legislation on only one element of the overall encryption debate which he considers most critical for law enforcement, the ability to access data stored on the most modern versions of the leading smart phones in the custody of the courts or the police.

Mr. Wainstein had a distinguished career in the FBI before being appointed the first assistant attorney general for national security and then as homeland security adviser to President Bush. He has seen this issue evolve over time.

Thank you, Mr. Wainstein.

Mr. Chris Inglis is a graduate of the Air Force Academy with decades of experience at NSA, including over 7 years as deputy director. He has taught at both West Point and the Naval Academy, to try to make up for his previous situation.

You now occupy the chair of cybersecurity at the Naval Academy.

Thank you, Mr. Inglis.

Cyber is an issue that touches many committees in Congress. To the extent that it advances commercial encryption technology, and the ease with which effective commercial encryption is applied adversely impacts foreign intelligence collection and counterterrorism, this committee has a strong and vital role to play and needs to be informed.

Law enforcement, in contrast, is not directly in our jurisdiction. But as the FBI's dispute with Apple in the San Bernardino terrorist case shows, the inability of law enforcement agents to physically unlock smart phones and retrieve unencrypted data can directly impact national security.

I look forward to further exploring these types of issues with our witnesses.

I also want to note that there are other distinguished national security experts who provide competing advice on this complex issue. National experts such as Admiral Mike McConnell, former Director of National Intelligence, director of NSA; General Mike Hayden, former deputy director of NSA and CIA; and former Deputy Secretary of Defense Bill Lynn; and also former Secretary of Homeland Security Michael Chertoff, all oppose government mandates on commercial industry to enable access to unencrypted content.

This is an issue I would love to discuss with the panel when we get to your questioning.

They argue that cyber vulnerabilities are the greater threats to the public and national security, that previous predictions of disastrous consequence from commercial encryption technology failed to materialize, that U.S. Government access mandates will harm U.S. companies and provide cover for repressive regimes to suppress dissent, and that previous attempts to control encryption technologies for legislation did not succeed.

These experts have written an article explaining their views. Mr. Chairman, I would like to these articles part of the record.

Chairman McCain: Without objection.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator Reed: Thank you very much, Mr. Chairman.

I believe one of the most important functions of our hearing is to illuminate and explain complex issues, and I hope our hearing today will make such a contribution.

Indeed, the series of hearings that the chairman has set up is absolutely critical, I think, to our consideration going forward, so I thank him for that.

Thank you, gentlemen. I look forward to your testimony.

Chairman McCain: I thank the witnesses.

Mr. Vance?

STATEMENT OF CYRUS R. VANCE, JR., MANHATTAN DISTRICT ATTORNEY

Mr. Vance: Thank you. Good morning, Chairman McCain, Ranking Member Reed, and members of the Senate Committee on Armed Services.

On behalf of our office in New York City, on behalf of State and local law enforcement around the country, I am very grateful that you are willing to hear our testimony this morning.

The basic facts, Senators, underlying this debate, in my view, are really not that much in dispute.

First, just talking about Tim Cook's own statements that he made to the public and his customers in February of this year, it is absolutely true, as he said, that smart phones led by the iPhone have become an essential part of our lives. They certainly are an essential part of my life. As a citizen, I certainly appreciate the many benefits of the technological age and the Internet.

But these devices are also essential to criminals. Our office investigates and prosecutes a range of cases from homicide to sex crimes, from international financial crime to crimes of terrorism. In all those crimes, and others, it is undisputed that criminals use smart phones to share digital information, to plan and commit crimes, whether through iMessages, photos, or videos.

Third, criminals know iPhones now enable them to communicate with impunity about those crimes. Let me tell you that the criminals are thrilled with this development.

Now, that is not hyperbole. In a real example from a case in my office, an incarcerated defendant on a pending sex crimes charge tells a friend that we overhear on a lawfully recorded landline out of Rikers Island jail, and I am quoting from the call, "Apple and Google came out with software that can no longer be unencrypted by the police. If our phones are running on iOS 8 software, they cannot open my phone. This may be another gift from God."

Senators, it is clear this is not a gift from God. It is a gift, perhaps unintended, from the two largest technology companies in the world.

Fourth, Apple's and Google's decision to limit law enforcement access, even with a court warrant, to critical information is, I believe, made under a questionable claim of increased privacy.

The encryption Apple provided on its mobile devices before iOS 8, that is, before the end of September 2014, was both secure for its customers and amenable to court-authorized searches.

Apple itself characterized the iOS 7 operating system as the ultimate in privacy, touting its proven encryption methods and ensuring users that iOS 7 could be used with

confidence in any personal or corporate environment.

Now, given Apple's own statements about iOS 7, shortly after Apple's reengineering of its phones to prevent search warrant access by law enforcement, I asked Apple in a letter dated March 2015 whether there was a bona fide security reason to make its new operating system, iOS 8, warrant-proof. Now, Apple chose not to answer me.

But in March of this year, the House Judiciary Committee compelled Apple to answer the same question. That committee asked Apple the following question in writing, and I am quoting from the committee, "Was the technology you possess to decrypt these phones," the reference is to iOS 7 and their predecessors, "ever compromised?" That was the question to Apple.

Apple's written response was, and I am quoting the response, "The process Apple used to extract data from locked iPhones running iOS 7 or earlier operating systems was not, to our knowledge, compromised."

Now Apple's answer to this crucial question shows what we have long suspected, that Apple's method of data extraction under iOS 7 posed no documented security problems.

That being so, I believe there should be no unreasonable security risk in a going-forward solution, if court-ordered warrants can be honored by extracting

responsive data off the smart phones.

Now we know, I believe now, the risk of loss of security, on the one hand, may have been exaggerated. But I know, on the other hand, speaking on behalf of law enforcement, that I can document the impact of warrant-proof devices on the security of the residents in my community.

So let me give you, if I may, an impact of this new encryption protocol introduced by Apple.

In my office alone, we now have more than 310 lawfully seized iPhones running iOS 8 or 9 that are completely inaccessible, despite court-ordered search warrants having been issued for them. These devices represent hundreds of real crimes against New Yorkers that we cannot fully investigate, including cases of homicide, child abuse, human trafficking, assault, cybercrime, and identity theft.

Now, that is just my office. But the data from across the country tell a similar story.

In California, the Los Angeles County Sherriff's Department has amassed more than 150 inaccessible devices. The L.A. Police Department has more than 300. And the Roseville Police Department has more than 200. Riverside County, California, has 12 inaccessible devices connected just to murder cases alone. The Charlotte-Mecklenburg Police Department in North Carolina has 160 inaccessible devices. In Texas, the Harris County DAs office collected

more than 100 inaccessible devices in 2015 and have encountered 8 to 10 inaccessible devices per month so far this year. In Massachusetts, the Suffolk County DA representing Boston has 129 inaccessible devices.

Now this brief list shows the problem from the perspective of some members of State and local law enforcement.

But even this small sampling represents more than 1,000 cases in which local prosecutors lacked the evidence that we need, and that juries demand, to hold criminals accountable, in some cases exonerate the innocent, and deliver justice for victims and safety in our streets.

Now it is, respectfully, in my view, no answer to suggest, as some have, that government should develop the capacity to hack into these devices. In my opinion, a technological arms race between the Federal Government and Silicon Valley is not in our collective interest.

The enormous cost and energy of such a conflict are better directed, in my opinion, against our common enemies, the criminals.

Furthermore, local law enforcement agencies do not have the resources to access each lawfully seized device and would be required to send each device to costly third-party companies for analysis and data extraction.

According to the reports, the FBI paid in the

neighborhood of $1 million to bypass the terrorist passcode in the San Bernardino case. I can assure you that amount represents more than the budgets for all law enforcement in many counties across the country.

Despite the large number of experts in the field of digital forensics and cryptology, such experts are still several models behind Apple's iPhones. The method employed to open Syed Farook's iPhone in the San Bernardino case reportedly works only on that particular iPhone, and only until Apple finds and patches the flaw the FBI was able to exploit.

Senators, surely the solution to the encryption problem is not a technological arms race. It is, in my opinion, Federal legislation.

But I appreciate that some are skeptical of Federal regulation. But Federal regulation of consumer products that impact public safety has been a part of our legal landscape for more than 100 years. And numerous industries, especially in financial services, are required by Federal regulators to retain data expressly for the purpose of helping to combat fraud and other wrongdoing.

Federal regulation is already important in the communications industry. When telephone companies went from using copper wires to using fiber optics and digital signals, the police could no longer use their old techniques

of executing wiretap orders, so Congress passed CALEA, mandating that telecom providers build into their systems mechanisms for law enforcement to install court-ordered wiretaps.

Many of these regulations initially faced resistance, and the affected industries argued that the regulations were imposing upon individuals' privacy interests. But over time, the regulations have been accepted. And it is clear that they play an important part in our society, especially in keeping people safe from harm.

Now our office's proposed solution, which was proposed in a white paper that we published in September 2014, is to enact a Federal statute providing that data on any smart phone made or sold in the United States needs to be accessible, not by law enforcement, but by the designer of the phone's operating system when the company is served with a valid search warrant issued by a court.

And if a person or entity such as Apple offers encryption software, it has to have the ability to provide data, also in response to judicial order.

The solution, as I say is spelled out in our 2015 report, does not require new technology or any government backdoor. Under this solution, Apple would be able to comply with judicial warrants and offer the same strong encryption that it employed without, to our knowledge, a

single documented breach before it adopted the default device encryption under iOS 8.

The focus of the proposed legislation, we believe, is appropriate because, since September 2014, our primary obstacle in local law enforcement has involved getting access to data at rest on the smart phones in our possession. But that would be no small achievement, because it is local law enforcement that prosecutes more than 95 percent of the criminal cases in this country.

As it stands today, Apple and Google, not a court, not Congress, decide who has access to key evidence in criminal investigations and trials. I cannot and I do not believe it is right that two private companies should decide which victims can achieve justice in our country.

There has been discussion about convening task forces to examine the science and policy implications of default device encryption. That may well be a good step, but I urge Congress to act quickly. Twelve months of taking testimony resulting in nonbinding recommendations in a report will not adequately address the urgency of the problem that local law enforcement faces.

Time is simply not a luxury that local law enforcement, crime victims, or communities can afford. Our laws require speedy trials. Victims are waiting for justice. And criminals must be held accountable before they can reoffend.

Centuries of jurisprudence hold that no item -- not a home, not a file cabinet, and not a smart phone -- is beyond the reach of a court order. Our access to data today is grounded in and limited by the Fourth Amendment, which authorizes only reasonable searches based on probable cause, supported by a particularized search warrant, issued by a neutral judge.

Senators, that burden, not warrant-proof encryption, I believe, is the strongest safeguard we have in balancing privacy and public safety.

Thank you very much.

[The prepared statement of Mr. Vance follows:]

Chairman McCain: Thank you.

Mr. Inglis?

STATEMENT OF JOHN C. INGLIS, ROBERT AND MARY M. LOOKER PROFESSOR IN CYBER SECURITY STUDIES, UNITED STATES NAVAL ACADEMY, AND FORMER DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Mr. Inglis: Thank you, Chairman McCain, Ranking Member Reed, and members of the committee. I am pleased to appear before you to talk today about cyber and encryption issues.

In my opening remarks, I would like to cover three areas.

First, I think it is important to lay out a framework of interests that can guide choices about desired or unwanted outcomes that transcend the technology discussions that so often dominate this debate.

Second, I would like to offer my view, in the context of encryption within the system of systems we once referred to as the telecommunications sector and now variously refer to as the Internet or cyberspace. There are, of course, surgical applications of encryption that can be considered in isolation, but these tend to be the exception rather than the rule, even if they are considerably more tractable.

Finally, I will suggest some implications of this discussion in the context of an increasingly interconnected world, one where it is unlikely that purely national solutions will either be acceptable or widely adopted.

First, framing the issues. In trying to simplify and

untangle the various threads of this discussion, it is tempting to focus first and foremost on technology and, more particularly, encryption. One of the perils of that approach is that it fails to first establish a foundation of principles and objectives that can drive the attributes of technology and other systems intended to serve the interests of society.

There are, arguably, at least four interests converging here. The first is the desire by individuals for security of the communications and data that they transmit or store on digital devices and networks.

This interest is often oversimplified as a desire to protect confidentiality of data, sometimes shorthanded as protecting privacy. But the services of integrity and availability are often just as important, delivering needed confidence to the integrity and resilience of financial transactions, personal preferences, and the flow of critical resources ranging from energy to airplanes, and the like. Encryption technology can and does make a contribution to all three.

The second interest in play here is the goal of protecting society from the actions of those who would use Internet-based communications to plan, coordinate, and deliver harm to its collective security interests. This is not an idle threat and not a future prospect. These threats

include, but are not limited to, the use of Internet-based communications to conduct illicit activities such as child pornography, terrorism, or the delivery of cyberthreats.

Indeed, it is the demonstrated potential for encryption to provide anonymity and cover to those who threaten our collective interests that underpins law enforcement and the intelligence community's desire to gain access to the content of individual communications.

The third interest in play is the desire of individuals or companies to freely innovate, create, share, and sell products in the marketplace without undue interference from government. The ability to do so, of course, is a vital component of U.S. freedoms and its economic and national security.

And building upon the third interest, a fourth interest emerges, namely the need for U.S. companies to remain competitive in what has become a global marketplace, a desire that is particularly acute for companies doing business across differing legal regimes where the balance struck between individual and collective security is uneven.

Solutions that arbitrarily deliver a unique advantage to one society above others will falter and fail in that world, risking not only a company's viability in foreign markets but the economic vitality and prosperity of the U.S. itself.

Taken individually, each of these aims can be viewed as a laudable goal. Taken in sum, an unqualified commitment to one of the aims necessarily makes it more challenging to achieve one or more of the others. Further, the dynamic nature of technology and its creative application to the myriad tasks by millions of users, hundreds of millions of users, greatly increases the difficulty of striking and sustaining a particular balance over time.

In any event, unless and until we determine which of these interests we want to support, we will be unable to judge the efficacy and suitability of any particular system, technology, or protocol.

My bottom-line point would be the following. Some would argue that these four interests constitute a choice. I believe this is shortsighted. The U.S. Constitution, as already noted by the Senators leading the hearing, provides useful guidance here in the use of the word "and," not "or," as the conjunction joining the preamble's enumeration of goals motivating the formation of a more perfect union.

I am firmly convinced that the innovation, creativity, and industry exist to align and support all four of the interests I have outlined here.

Whatever the choice may be, the premise of our union is that we must establish the overarching goal before devising laws, procedures, and technologies that advance those stated

interests.

There are two common misperceptions that often the cloud this debate vis-a-vis encryption. The first is that encryption stands on its own as a security tool. In practice, across the vast majority of security systems, encryption is just one of several mechanisms used in combination to deliver the desired mix of confidentiality, availability, and integrity. To be sure, it is an essential component of a globally deployed system protecting both data and motion and data at rest, but it is hardly sufficient in and of itself. Physical security, personnel security, user behaviors, hardware, software, security are all equally essential.

I do not point this out to detract from the necessary focus on the resilience of encryption schemes, but to say that we should not fool ourselves that a strong right arm on an otherwise undeveloped frame is enough to protect our interests. This will be ever true as technology continues to advance.

Second, and more important, is the misconception about encryption that it is a monolithic thing, that it is either on or that it is off. A quick look at the diversity of user expectations and vendor choices reveals that it is far more nuanced and complicated. Some users want their data encrypted so that they can be the only ones who can recover

it -- no vendor backups, no emergency recovery service, no possibility of third-party access or government surveillance.

Other users want a safety net, the ability to recover a lost key, retrieve lost data, backup data on some mediums, say the cloud, that is recoverable under a variety of circumstances.

Adding to that, vendor choices regarding their service offerings cater to this broad array of user preferences while adding an overlay of vendor-preferred attributes. Some vendors deliver encryption systems that cannot be penetrated by even the vendor himself or herself, either for their purposes or on behalf of others. Other vendors build and deliver systems that contain exceptional access mechanisms, built-in means to remove the overlay of encryption at various points in the transport or storage of that piece of data.

The commercial reasons for this exceptional access run the gamut from creating safety nets for users seeking to recover data to enabling access to data by a party other than the data owner -- in some cases, the vendor himself or herself -- because they want to actually access that content for purposes of their business proposition.

The result is an architectural landscape where some vendors place security controls wholly in the hands of users

while others deliver systems that allow vendor or third parties to access user data because that access is essential to the vendor's business model.

The point is that these differing approaches are not generally portrayed as weak versus strong encryption. They are more properly differentiated by their choice of how and when the protected materials may be revealed.

This diversity of choices reflects, of course, the reality of a free market economy and the rights of individuals, including companies, to pursue features of their own preference. As such, these choices are neither good nor bad. They are just choices.

This diversity suggests there is no one design principle driving the use of encryption. But if we assume that these same market forces will deliver a principled reconciliation, if not an alignment, of societal goals that will endure over time, we should only look at the diverse user expectations, the diverse technologies in the marketplaces, and remember the excesses periodically delivered by markets to come to a different conclusion that that is not the solution.

In the face of this natural diversity and architectural choices, the use of terms like backdoors and secret keys must be seen as pejorative and unhelpful. It is ultimately determined by a system designer that it is appropriate to

provide a means for exceptional access through some party other than the data owner.

Generally, they ask three questions. Is there a legitimate purpose being served? Does the data owner understand the nature if not the details of the potential access? And are the controls on the access sufficient to ensure that such access is constrained to the identified purpose?

In summarizing, I would like to actually tease out some implications enumerated or perhaps surfaced by those two broad topics of discussion.

First, the use of strong encryption is an essential component of security for our Nation and our citizens. The fundamental question is not whether to choose one purpose or another, but to determine how access to stored or transmitted data is controlled by the application of strong encryption that is technically feasible to do then.

Second, a framework to reconcile the various interests arguing for potentially different technical solutions will be best served by first reconciling if not aligning our societal goals.

Third, if our goal is to deliver security to individuals, and security for the American people writ large, and continued economic vitality in a global marketplace, then we must deliver these goals in a global

context, neither surrendering nor wholly favoring U.S. security to the detriment of like-minded nations.

Along those lines, fourth, it is considerably more likely that law enforcement interests can be parsed into international norms than can national security interests. A bias, therefore, toward law enforcement interests in this area may be appropriate to deliver the framework that we seek and the attendant solutions that then work within that framework.

Fifth, as I have said before, market forces alone have seldom shown themselves able to deliver consistent alignment of societal outcomes across diverse products and services and typically have never done that across time.

Finally, inasmuch as I describe a mandate for government action in this space, I think government action is both required and must be fully informed by various interests government is formed to represent; focused on ensuring the various freedoms and rights of individuals while also maintaining collective security -- we can do both; and mindful that the engine of innovation and delivery is almost exclusively found in the private sector.

To be clear, I do see a role for government in both facilitating the creation of an enduring values-based framework that will drive technology and attendant procedures and in reconciling that framework to like-minded

nations across the world.

Conversely, I believe government's failure to serve in this role will effectively defer leadership to a combination of market forces and the preference of other nation-states, which will drive unopposed solutions that we are likely to find far less acceptable.

In spirit, I applaud the initiative of this committee and the further work that it undertakes today, and I look forward to your questions.

[The prepared statement of Mr. Inglis follows:]

Chairman McCain: Thank you.

Mr. Wainstein?

STATEMENT OF HON. KENNETH L. WAINSTEIN, FORMER ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, DEPARTMENT OF JUSTICE

Mr. Wainstein: Chairman McCain, Ranking Member Reed, members of the committee, thank you very much for the invitation to appear before you today.

As my colleagues have made clear, we are in the midst of a national debate over the implications of default encryption. This is a debate that has been going on for the better part of 2 years, and we now find ourselves at really what is a complete impasse. It is time, I urge, for Congress to step in and break through that impasse.

Congress has played a pivotal role over the years in striking a balance between individual and societal privacy interests on one hand, and our government's law enforcement and national security interests on the other.

That is what it did when it passed Title III and FISA, which mandated a judicial process for issuing warrants and orders for criminal and national security wiretaps. That is what it did when it passed the Communications Assistance for Law Enforcement Act, CALEA, that my colleague referenced, requiring telecommunications carriers to equip themselves to ensure the government can conduct lawfully authorized surveillance on their systems.

But despite these laws, gaps started to appear in our

surveillance capabilities in the last decade, and government officials started to worry that they were going dark. This going dark issue has become exponentially more problematic with the recent advent of the default encryption, as a result of which providers and manufacturers are now often completely unable to satisfy lawful court surveillance orders.

This dilemma is now clear for all to see, and the lines of the debate have been drawn with government officials arguing that default encryption can endanger our country by creating safe places for criminals and terrorists to operate outside the reach of law enforcement and national security officials, and with representatives of the tech and civil liberties communities countering with a variety of arguments, including that any accommodation for government surveillance would undermine the security of encryption, that any accommodation would cause U.S. tech companies to lose customers who might be skeptical of a company that cooperates with the U.S. Government, and that any accommodation would simply cause wrongdoers to start using foreign encrypted services as opposed to services here in the U.S. that are subject to that accommodation.

Citing these and other arguments, some of the tech and civil liberties communities have taken an absolutist position that there should be no government accommodation at

all.

Now, while I fully appreciate the tremendous societal value of strong encryption, and I appreciate the validity of the tech industry's concerns, I do not believe that that is the end of the discussion. Our surveillance capabilities are just too important to our national security. It is due in large part to those capabilities that we have had success in protecting our country against large-scale terrorism since 9/11.

That record of success, however, is now being tested by the rise of ISIS, which clearly recognizes the operational value of encrypted communications, as it has issued its members guidance on encryption and it intentionally uses encrypted apps in its recruiting efforts.

With this gathering threat on the horizon, now is the time for Congress to mobilize and embark on a legislative process that calls on both sides of this debate to fully lay out the basis for their views.

For the government, this means completely explaining how significantly their different investigative efforts are or are not handicapped by the use of default encryption technologies. And for the tech industry and civil liberties groups, this means providing hard data that demonstrates exactly how and how much each possible type of potential accommodation would impact their encryption system.

It is only when Congress receives this data that it can knowledgeably balance the potential cyber dangers posed by any government accommodation against the national security and law enforcement benefits of having one in place.

Congress can undertake this effort either through a traditional legislative process or through the establishment of a commission like that that has been proposed by Senator Warner and Chairman McCaul. Either of these options would be a significant step forward from where we are now.

The option that is not a step forward is the option of inaction and continued impasse. We have seen the consequences of that option before, as that was the option the government effectively pursued in the late 1990s and early 2000s when debating the wisdom of the wall, which was the regulatory barrier that prevented coordination and information-sharing between law enforcement and intelligence community personnel.

That inaction had tragic consequences when the existence of the wall contributed to our inability to identify the 9/11 hijackers and to prevent them from launching their attacks. Congress dismantled the wall when it passed the PATRIOT Act 6 weeks after 9/11, but that was too late for the 3,000 murdered Americans.

We made the mistake of inaction once before. We must not make it again.

I applaud the committee for holding today's hearing and showing leadership on this issue. It gives me hope that we can, in fact, move beyond the current impasse and reach a workable solution to this critical problem.

My thanks again for inviting be here today, and I look forward to answering your questions.

[The prepared statement of Mr. Wainstein follows:]

Chairman McCain: I thank you. And I want to emphasize to you, sir, that I view this issue as one of the most compelling for a whole variety of reasons, and I intend for this committee to, if necessary, take up separate legislation to try to address an issue that has clearly not been resolved.

Mr. Vance, we, Republicans and Democrats, liberals and conservatives, disagree on a lot of issues. One issue we do not disagree on is the horrible crimes that are committed by child pornographers and human traffickers. I know of no one that does not condemn this terrible, terrible exploitation of the innocent in our lives and our society.

So what we are doing here, if you would mention again, we are basically protecting child pornographers and human traffickers. We are protecting them by giving them access to encrypted mechanisms so that they can carry on their disgraceful, odious conduct.

I guess I say that because we talk about encryption and freedom of speech and government intervention and all that, but I thought one of the fundamental requirements of any government is to protect the defenseless. Now, de facto, by this encryption and failure for us to allow law enforcement people such as yourselves to have access to this information, we are furthering the cause of child pornographers and human traffickers.

Your comments, Mr. Vance?

Mr. Vance: Senator, I absolutely agree that the consequence of this device default encryption, which was a purposeful reengineering of the devices to make them inaccessible and to be unlocked even with court order, the consequence of that is a loss of, speaking for local law enforcement, local law enforcement's ability to do the job that each of us was sworn to protect.

And the cases that we outlined in our white paper from November 2015 described to the committee some of the absolutely horrific fact patterns that in the past we have been able to solve those issues because of access to devices. And, as I say, in our office alone, there are 314 cases ranging from murder to child sex abuse that we can now not access those devices.

So the answer is yes. But I think, from my perspective, Senator, the reason I think this is so important, that the legislature deal with this, and why I am so grateful that you are giving further visibility to this, is that it seems to me that there are some in the technology community who have come to the conclusion that the inability to find a path toward justice for victims in the cases that I described is simply collateral damage and acceptable collateral damage in the service of their privacy position.

I, for one, have a hard time understanding how I can

explain that to the victims of crime in my community.

Chairman McCain: Even though the United States Supreme Court, if I recollect, stated that child pornography was unique in itself and its criminal activities. "I know it when I see it" is one of the phrases that was used.

Twitter barred a data miner, a company specializing in searching across millions of tweets to identify unfolding terror attacks and unrest, from accessing its real-time stream of tweets because of its work for U.S. intelligence agencies.

What are your thoughts, all three witnesses, on Twitter's decision to ban this valuable counterterrorism tool from being used by the intelligence community, even though Twitter continues to sell the information used about consumers for a profit?

Mr. Inglis?

Mr. Inglis: Sir, if I might, I will answer that question, and first go back to the previous question.

I fully support the comments made by Mr. Vance about the nature of the choices being made with respect to the use of default encryption. The idea that the private sector believes that they are the arbiter of that choice is both inappropriate and I think unnecessary because I do not think we have to choose. I think that are systems that we can develop that essentially deliver appropriate security for

those systems.

He gave a great example between operating versions seven and eight, and that at the same time can deliver appropriate access for the government when and where it needs it.

Chairman McCain: Is that a second key idea?

Mr. Inglis: Pardon, sir?

Chairman McCain: A second key?

Mr. Inglis: There are any number of schemes that you can bring to bear. That might be one of them. I think the government is taking great pains, and I think appropriately so, to not specify an implementation because I would defer to the innovation of the private sector which has shown --

Chairman McCain: But if they want to, they could.

Mr. Inglis: They could. They could.

There are any number of ways that you can do this and that you could provide appropriate protection for that, without giving the government the keys to the store or, for that matter, rogue governments that might want to have access to the same thing.

To your question about the data miner, I think it is inappropriate and hypocritical for a data miner to retain that information for use for commercial purposes, but not to provide that such that society, writ large, might be protected.

Chairman McCain: But that is Twitter's fault, right, because Twitter stopped doing business with them? It was kept from accessing their real-time stream of tweets.

Mr. Inglis: Senator, I do not disagree. The shame of the larger proposition is that, increasingly, entities within the private sector stand in as the arbiter of how you align these societal values. I think that is not appropriate.

Chairman McCain: I see.

Mr. Wainstein?

Mr. Wainstein: Thank you, Mr. Chairman. I agree with Mr. Inglis on this issue.

I would like to point out the broader question or the broader concern that I have, which is just generally about cooperation by private industry with our efforts to protect the country. As a prosecutor for 15 years or so, I enjoyed great cooperation from most of the telecommunications providers and others in the industry. When we were running down terrorists or criminals, they were very helpful.

I think there has been a change since the disclosures by Snowden, and I think there are now business reasons for some companies to not only scale back on their cooperation with the government, but to be seen by customers and potential customers as scaling back because they think there is a business disincentive for them to be seen as

cooperative. There are some customers who will go to other companies if they think that your company is being too cozy with the U.S. Government.

That is terribly unfortunate. I think part of what I would like to see come out of this legislative process, which you just discussed embarking on, is the clear signal that we expect cooperation and we should have a cooperative relationship.

This is not to say there isn't. I was briefed recently by a major tech company that is doing a lot of really good stuff for the intelligence community, so there is cooperation going on. I just think it is very unfortunate that some companies are resorting to these public measures to show how they are distancing themselves from the U.S. Government.

Chairman McCain: Well, I am reminded when the tech companies say that, well, other countries will not do business because of the fact that there is a possibility of compromise, I am reminded of when, after the scandals of the 1970s, we enacted antibribery laws and everybody said, oh, no, you cannot do that because then these countries will not do business with our defense companies and corporations. That obviously did not happen.

My time has long expired, but I do think it is important to point out, and maybe we can get a comment later

on, there is a Wall Street Journal article that says, "How Islamic State Teaches Tech Savvy to Avoid Detection." It is a well-known fact that Mr. Baghdadi is sending people into the refugee flow with encrypted phones in order to carry out acts of terror. That is well-known. It is not classified information. And yet our tech companies seem to be ignoring that direct threat to the security of the United States.

Senator Reed?

Senator Reed: Thank you very much, Mr. Chairman. Again, thank you for holding these hearings. This is the second. There will be many more, because this issue is extraordinarily complex.

I do not want to oversimplify it, but let me suggest, at least to begin, that there are two perhaps distinct issues here, among many. One is a phone that law enforcement authorities physically have in their custody. And the question is, should there be a statute that gives the right, or demands the company gives you access to that phone? That seems to me more straightforward than the second issue, which is how you access encrypted communication before a crime or with probable cause that a crime has been committed, but you do not yet have a complete case.

Mr. Vance, are there technological ways to do that that the companies could provide? That is the first issue here,

too, in terms of getting into that encrypted --

Mr. Vance: On the phone itself?

Senator Reed: No, I am talking about one of the challenges we have, particularly to anticipate criminal activity, to investigate it, the old wiretap, where you had probable cause to suspect a crime was being planned, went to a court. In the old days, you just put the electrodes, the wires on the phones, and you were listening in and you got information. Can we physically do that now, technologically?

Mr. Vance: Senator, in our office, we have historically used Title III to access data in transit, cell phone to cell phone, text to text. So it historically has been doable.

Obviously, the developments of encryption software, purposefully, in some cases, directed to be used by outside terrorism actors, affects that. Director Comey, I think, has been the most powerful spokesperson on that interest.

So going forward, the answer to your question is, can you create an environment in which law enforcement, pursuant to a court order, can access communications and others cannot? That is the technological question that I think all of us are struggling with.

I would suggest that, and, respectfully, the answer has to be yes. We are an enormously creative and innovative

country with geniuses in the tech community, as well as in the security industry, particularly at the Federal level. I find it not a solution for industry to fold its arms and say we are not going to provide any way forward for this debate. I think that is not helpful. And I believe that, surely, with all the other technological advances we have achieved, this is not impossible. It is just not being -- there is no direction or requirement that this be addressed by the tech industries and the government in a coordinated manner.

Senator Reed: Again, my knowledge is not as extensive as yours. That will require not only the makers of the phones but the Internet providers to be able to, pursuant to court order, have the means of getting into the phone surreptitiously, because you do not want to disclose your activities, and extracting information.

Mr. Vance: I think that is accurate. But again, though I am not the smartest technological person in the room, I think that does not mean that it is not achievable.

Senator Reed: No, I think the technology could be there. I just want to make sure we are focused on what has to be done, and then let people to it. But that is the issue of end-to-end encryption.

I second Mr. Wainstein's comment, too. I think after Snowden, there is a whole different attitude in the industry about this, and there are business considerations about who

is the most secure, et cetera. So I think it was a very interesting and important point to make, Mr. Wainstein. That is something we have to face going forward.

Just to the whole panel, I mentioned in my opening remarks Secretary Chertoff, Admiral McConnell, very distinguished, thoughtful people who spend their lives dedicated to national security, have taken a very different position, saying several factors.

First of all, these are real problems but there is a greater issue, and that is protecting legitimate information from cyber intrusion. That is one aspect.

The second aspect is that, and the chairman alluded to this, that if we do it, and the rest of the world does not do it, we are at a disadvantage.

And third, we tried efforts to control encryption technology through legislation before, and they have not worked.

So quickly, my time is expired, but I will start with Mr. Wainstein, your comments?

And rebuttal, Mr. Vance and Mr. Inglis?

Thank you.

Mr. Wainstein: Thank you, Senator Reed.

First, that list that you just read off of people are some of the finest public servants this country has ever had, and they are close friends and colleagues of mine, and

I have tremendous respect for their opinions. They raise good points.

As I said in my remarks, there are strong arguments on the tech industry side of this. There are real concerns, and they have raised them.

I guess my response would be this. Those concerns have been raised, and there have been arguments as to why this might end up unduly compromising encryption, which really is an important thing for society.

But the only way you are going to be able to do your job and balance the need for an accommodation against the impact it might have on encryption is for them to show exactly, specifically, technically, how that damage would come about.

So this potential, whether it is escrow key accommodation or another one, look at that and have them lay out exactly what that will do to encryption that causes them concern.

We have not heard that yet. Until we hear that, you cannot do your job and come up with a solution.

Senator Reed: Thank you very much.

Mr. Vance: Senator, I could not agree more with what Mr. Wainstein has said. In fact, I think it has been one of our frustrations that there has not been the ability or the willingness to quantify the increased loss of security.

Now, as I indicated, we just learned recently that it appears that there had been no data compromises by virtue of phones running on iOS 7 being open pursuant to court order. I think we all, listening to the tech community, thought that this was happening all the time. But the fact of the matter is, it turns out it was actually extremely secure.

So I think there is reality and then there is argument and advocacy.

As to the international disadvantage, I certainly think we need to take that seriously, but I think it is safe to say that the world has found a way to address the individual requirements of each country in the world to respect their sovereignty.

If Volkswagen or any company wants to sell a car in the United States, they have to meet certain security standards -- in some way, or at least -- really, really meet them.

Chairman McCain: Bad example.

Mr. Vance: So that is not a strange concept in the world of international commerce. If governments want to move money in and out of treasury departments around the world, there are certain standards that are required in each country before money is accessed and moved.

This has happened before. It is not a foreign concept to the world.

Senator Reed: Thank you, Mr. Vance.

Mr. Inglis, please?

Mr. Inglis: First, I support the remarks of the prior two speakers. I absolutely have an enormous and abiding respect for the individuals that you cited who made that comment.

I would say the following. First, if the choice is to weaken security, such that the government or others might have access to it, or to leave it strong, of course, the right choice is to leave it strong. I do not think that is the choice. I think that is a false choice.

Second, I would observe that there are a variety of circumstances under which, as a desired feature, we cut a third party into a conversation, maybe for a teleconference purpose or because you want to blind courtesy copy somebody on an email. For a variety of purposes, we essentially do software upgrades because we want to patch a system, and we have the means by which, from the vendor to the devices at the edge, we can have a sweeping application of software.

We do not call the former a backdoor, and we do not call the latter a secret method to denigrate the quality of the software. We call them features. So I think the technology exists such that we might do this.

To the comment that if we set this up, other foreign governments might then misappropriate it, that is a real issue. I think that we need to think our way through that.

But if we do not drive the rules, they will.

There are thoughtful nations, like the United Kingdom United Kingdom, that are thinking their way through this, and they have come up with something in the investigatory powers bill, which I think is likely to be passed this fall, which is going to strike an alignment, not a compromise, but an alignment of these great goods. There are other nations that will not be as thoughtful as that.

If the United States stands by, we defer to the wishes, to the values set, of others. If we lead, we might just perhaps drive that to the place we want it to go.

Senator Reed: Thank you very much.

Thank you, Mr. Chairman.

Chairman McCain: Senator Cotton?

Senator Cotton: Thank you, gentlemen, for being here on this important topic.

I speak today as a friend of encryption, someone who recognizes its vital role in protecting some of the most important data that we all have, whether it is our email, text messages, phone calls, health information, financial information. But also someone who wants to protect the American people, to protect them from mass casualty terrorist attacks, to prevent them from being shot in nightclubs or in community centers, or blown up in malls, something that is as important if not more important than

protecting that data.

I also recognize the great contribution that companies like Apple and Twitter and Facebook have made to our society and the way that we live today.

I hope that there is some way that we can all find some compromise or alignment, as Mr. Inglis called it, to address all of these threats to the American people.

Mr. Inglis, I want to touch on a point you just made. In this debate, we often hear a lot about backdoors. But as you said, many companies employ software update mechanisms that could be thought of as a backdoor because they change or update the functionality of the device periodically, and sometimes without even notice.

These require additional keys or pathways to enter a device, so could you elaborate a little bit on, if a company can build a safeguard or additional key for updates and patches, why they could not do so for safeguards or keys for emergency purposes like terrorism, like kidnappings, like child pornography and so forth?

Mr. Inglis: I think your point is well-made, sir. I think that they can.

The question is not whether that capability exists or not. It certainly does exist, that you can upgrade software, that you can add other parties, legitimate parties, at the behest of the user to conversations, whether

it is retraction to pull stored data, or whether it is a conversation in motion.

The question is, is there a legitimate purpose that we understand and say that is sufficiently noble, we are going to engineer the solution. And do we have the controls on that, such that we are confident it will be used for that purpose and no other.

It is the bookends, not the capability, that then should be the focus of our conversation.

So I think the technology does exist. The question is whether we can engineer that and have confidence about its efficacy.

Senator Cotton: So let's put this question in a bit of a broader societal and legal context, Mr. Vance. We all have an expectation of privacy in our bank accounts, of course. However, you, I would assume, regularly obtain lawful subpoenas from a court to obtain the bank records of someone suspected of engaging in criminal activity. Is that correct?

Mr. Vance: Correct.

Senator Cotton: We also have reasonable expectation of privacy in our telephone conversations, the actual content of those conversations. However, I would assume that you often seek court-ordered wiretaps from telecom providers when there is a reasonable suspicion of criminal activity?

Mr. Vance: Correct.

Senator Cotton: Is there any reason why tech and data companies should be treated differently from banks or telephone companies in our society?

Mr. Vance: Senator, I believe there is no legitimate objective reason. I think what is interesting about the state of affairs we find ourselves in today is, sticking with Apple for a second, they reengineered the phones so they can no longer be opened by the company. That was a conscious choice.

But having done that, they have now argued that they have created a right to privacy that previously did not exist because of their engineering decisions to block access by law enforcement.

I think that is ironic, but that is where we are today. But I find no logical, reasonable reason why the technology companies should not be subject to the same sorts of rights and obligations that other industries have come to adapt and have worked through over the decades. I think that is something that is fair to look at going forward.

Senator Cotton: Mr. Wainstein, do you have any perspective on whether there should be some special set of rules for technology and data companies, as opposed to banks or telephone companies?

Mr. Wainstein: No, Senator Cotton. Look, I agree with

Mr. Vance on this, that as a sort of our compact with our government, we all, individuals, industry, companies, we have to submit to lawful court orders.

And despite this encryption, as Mr. Vance said, they did not create a new zone of privacy. They cannot do that. The privacy is as dictated in the Constitution and by the decisions of our courts.

And they have an obligation to provide that information. They have tried to litigate it. At the end of the day, I think they are going to lose on the fundamental issue. I am quite confident they will. I think that it is really up to Congress to make the point legislatively that unless you voluntarily accept the solution to this, it is of such paramount importance to the national security and to enforcement of our laws that we are going to legislate it.

Senator Cotton: We all have certain rights to privacy under our Constitution, but we also have a duty to provide information when subjected to a lawful court order, and that would be a duty not to our government, but to our fellow citizens.

Thank you.

Chairman McCain: Senator King?

Senator King: I think it is important to clarify, because there is a lot of confusion in this discussion, even in this hearing.

Encryption, the encryption horse is way out of the barn. We are not talking about encryption. We are not talking about WhatsApp or Telegram. That is done. It cannot be broken.

And we could say WhatsApp, you are owned by Google, you have to open it up. But somebody goes and buys Telegram, which is from Germany, and the Internet as a free exchange across borders.

I mean, if NSA can break it, that is one thing. But I do not think any of you are suggesting, or are you, that somehow we can deal with the encryption of apps that al-Baghdadi is using.

I think we need to clarify this discussion. We are really talking about the Apple case and compelling tech companies to provide access to their devices.

Am I not correct? Encryption, that is a done deal, isn't it?

Mr. Inglis: I think it is, sir. It is a done deal. And it is a good thing that encryption is in wide and almost ubiquitous use.

Senator King: So that is not really the question before the house. The real question are issues like the Apple case.

I think one of the problems we have to think anew here is, is that this is an international phenomenon. It is not

neat borders, sovereignty. It is very difficult to make those things stick where you have something that moves invisibly through the air and can be built anywhere in the world. It seems to me that is one of the problems.

We could pass a law here that forced Apple in some way, shape, or form to provide the key to open their iPhones. But whether or not that law would apply to an iPhone made in Turkey or Germany or Russia -- and I guess we could try to pick them up at the border, but it is like squeezing Jell-O. I mean, it is going to be a very difficult technological -- the international aspect of this makes it incredibly more difficult.

Mr. Inglis, don't you agree?

Mr. Inglis: I do agree, sir. I think that, then, this government has a dual obligation. One, to figure out what our values are such that we would drive choices to be biased toward an alignment of these, as I described it, four interests. It could be that it is three interests. But at the same time, work with like-minded governments to create an international regime where it is more likely that these products will win in that marketplace and put our vendors in the right position.

Senator King: I agree with that. This is a very difficult issue to grapple with, because basically we are balancing two provisions of the Constitution, provide for

the common defense and ensure domestic tranquility, and the First, Fourth, and Fifth Amendments. I mean, that is what we are trying to do here.

I do not like commissions, but I signed on to Senator Warner's bill to set up a commission to really look in depth at this issue involving the tech community, the law enforcement community, and the intelligence community, and come back to us with some really good thinking. I like your term of alignment.

As I say, I do not generally -- I think commissions often are a copout. But I think in this case -- and I totally agree that this should be a legislative solution. It should not be case-by-case in various Federal district courts. It should be a legislative solution. It is a policy issue.

But I think we need more information, frankly. I commend the chair for setting up this hearing, but I think this really needs some deep thought by a lot of people because it is really, in many ways, new territory.

Mr. Vance, hypothetical, and I know we were all taught in law school to never ask a question you do not know the answer to, and I do not know the answer to this.

If a locksmith makes a safe, and it is set up in such a way that the customer can set the combination and the locksmith does not know the combination, cannot open it,

could you get a subpoena or a warrant to force that locksmith to somehow break into that safe?

Mr. Vance: We would, Senator, likely get a warrant permitting us to, through physical force, open that safe with court directive.

Senator King: But that is my point. The FBI found a way to get into the Apple iPhone. They did not make Apple do it. In your answer, you just conceded that you would not make the locksmith do it. You would figure out how to do it.

One of the things, frankly, that really bothered me about the Apple case was that we had all this excitement and publicity about a great American company that went on for months and months, and then the FBI said never mind, we figured out how to do it. That bothered me.

They should have exhausted all of those remedies before they went to that magistrate in California and said we need something under a 200-year-old All Writs Act.

So you couldn't enforce that locksmith to come in and somehow break into that safe.

Mr. Vance: Senator, I think that legislation could be passed which would require that locksmith to have the ability to open that safe, if we reached a level of volume, such as we are reaching right now with the probability of a problem getting into encrypted devices that are relevant to

law enforcement investigations.

Senator King: You have 300 cases pending, so this isn't about one iPhone in San Bernardino. You have 300. And where does it stop? Is this for an OUI in Poughkeepsie that you are going to be able to open the iPhone? Is there any limit? Once we say law enforcement can get a warrant to force Apple or Google or whoever it is to open their phone, is there any limit on that?

Mr. Vance: I am not sure why there would be any other limit than the constitutionally recognized requirements of a court-ordered, specific warrant based on probable cause. So, yes, if that standard was met in Poughkeepsie or New York City or California, that warrant should be able, in my opinion, to be affected.

Senator King: I think that is a very important point, because a lot of the publicity and discussion and testimony at the time of the original San Bernardino case was we only want this for one phone. We are not talking about one phone. We are talking about thousands of phones.

Mr. Vance: I am certainly not talking about one phone, Senator, absolutely. And I believe it is because we are talking about thousands of phones that represent criminal investigations involving thousands of victims and investigations that may relate to security beyond the individual victims, that is why it is so important that this

committee has taken this issue up and is looking at it with an eye toward potential Federal legislation.

Senator King: One quick question, Mr. Chairman.

Do you fellows have any few on the Warner bill on the commission idea?

Mr. Vance: Senator, my view is that a commission sounds like a very sensible, thoughtful thing. But, as I said before, there is a sense of real urgency, particularly in State and local law enforcement, that we reach a resolution that could permit us to go forward.

So it is 1,000 cases. Maybe it is 5,000 cases around the country. Each of our cases in State court have statute of limitations, once filed, that we are operating under. We have victims of real crimes that are waiting for justice all around the country.

So if a commission was a commission that went on for 18 months and that issued a nonbinding recommendation at the end of that 18 months, from this one prosecutor's perspective, I am not sure that addresses the urgency with which State and local law enforcement need to deal with this problem.

Senator King: Mr. Inglis?

Mr. Inglis: So I largely agree with all of that.

It might well be that the government's best play is to say that it intends to act to create a stalking horse with a

sense of urgency, but, at the same time, it intends to do so in the most thoughtful way and the most well-informed way possible, such that then the commission creates an opportunity to establish a venue at which a very diverse array of disciplines, functions, perspectives, then can come together, but to encourage collaboration in advance of what ultimately will be a government action.

But there is an urgent need to get on with that, and thus far we have not seen the kind of collaboration required to bring the diversity that America has been so well-known for to the table to pull that off.

If I might go back to your earlier question, I think you are quite right to raise the context of the All Writs Act. Leaving aside, which I think you are right about the precedent of one versus a thousand, I would say that I think we are likely to find that the All Writs Act is insufficient, that it was not imagined it could be used in this situation, and, therefore, Congress needs to act to actually update that and bring that into the modern age.

Two, with respect to the San Bernardino case, the idea that in the absence of an All Writs Act, the absence of an ability to compel the vendor to assist, that you then turn to the FBI and say you are just going to have to hack the civilian infrastructure, I think that puts the government in exactly the wrong place. You do not want government hacking

civilian infrastructure, the private sector's infrastructure. You want government aiding and abetting the increased resilience of that infrastructure.

You, therefore, need to figure out how upfront do I attend to all of government's responsibilities to provide for collective security, which is what Jim Comey is pursuing. That is his lawful charge. But at the same time, have deference and support for the individual privacy and security that is attendant to the Constitution's promise.

Senator King: Thank you. Thank you for your thoughtful testimony on a very tough issue. I appreciate it.

Chairman McCain: If we did a commission, it would be at least a year, at best. But the point is this issue is not so complicated.

We have banking laws in the United States that are not respected by every country in the world, but we enforce them because anybody who wants to do business with the United States of America has to abide by those laws. We have other rules and regulations that we enforce -- antibribery -- that other nations engage in.

But we set the pace, and we are the ones who dictate the terms because we happen to be the largest market in the world.

And so I have heard this song before about, well, other

people are going to do it. So, therefore, we should not do it. I do not accept that argument.

When we have child pornographers who are operating freely -- freely -- and human traffickers who are operating freely, there is an urgency to this issue, which is why this committee has taken up, and is going to have more hearings on it, including hearing from the tech companies, even if they do not want to come here. This committee has subpoena power.

But for them to blatantly say that they will not give us information or give us the ability to acquire information as we have, as you pointed out, Mr. Vance, on banking financial records, all kinds of other ways that we have of pursuing criminal activity, but somehow this new technology should be exempt from all of that is something that I do not buy. Nor do I think the families of those young girls who are being human trafficked right now, nor those children who are now the victims of child pornography, which is being protected by the way that these companies are doing business now. I find it unacceptable.

Senator Blumenthal?

Senator Blumenthal: Thanks, Mr. Chairman.

I want to thank you for those comments. I share those concerns about the power of our private sector, financial and communication companies, that have immense financial and

market power, and the ability to do good and cooperate and protect victims of human trafficking, as well as of terror, extremism, and violence.

The United States is home to some of the world's leading social media, advertising, film, communications companies. One of ISIL's most powerful tools for recruitment is its social media campaign. The group releases absolutely horrifying but expertly done videos inspiring young people to join its ranks.

On the one hand, our modern, interconnected world gives ISIS the ability to reach the United States, no matter how robust the physical barriers or boundaries may be. On the other hand, their hatred for us is absolutely inescapable and open, and we need to intensify our efforts against those malicious messages, including forging solidarity with the Muslim world, which has as much to lose as we do. And the messages of intolerance and persecution and extremist violence I think can bring us together, even as our adversaries and enemies seek to divide us.

I want to thank all of you for being here today on this supremely important topic, particularly District Attorney Vance.

Thank you for your good work. I know of all of your distinguished service.

District Attorney Vance happens to work in a venue

close to my State of Connecticut in an area where I used to work as well, both as a Federal prosecutor and as State Attorney General.

So I think your work is supremely important in this area, and your leadership and advocacy.

I want to ask a question that is directed to the private sector.

How can we bring the private sector to cooperate more closely and be a better partner of law enforcement in this area?

Mr. Vance: I am not expert in these matters, but I do think, as I was saying, Senator, that whether the private sector is willing to acknowledge it or not, this is an urgent issue. And it is urgent because it is affecting national security, about which I am not an expert, but local security, about which I have some knowledge.

Now I guess the commission, a presidential commission or congressional commission, is one sure way to start the process. One of the Senators has suggested that.

But I think it needs the active involvement of the administration. I think the President and his administration needs to grab ahold of the collar of local law enforcement and the enforcement communities, grab ahold of the collar of the private sector, pull them into a room, work at an accelerated speed with an eye toward getting a

resolution to this or some recommendations on how to go forward between now and the end of the year.

That may be totally unrealistic from a calendar standpoint with the way we are in America right now, but unless the administration is going to come in and assist the Congress, local law enforcement and others, I think it is not going happen.

Senator Blumenthal: Yes, sir?

Mr. Inglis: Sir, I would add to that that I think the government first and foremost, Mr. Vance's point, needs to indicate its desire to lead, its intent to lead, as opposed to observe.

Then second, the framing will be profoundly important. If the government were to approach this by saying we intend to impose a requirement on the private sector, to satisfy Mr. Vance's or perhaps Jim Comey's need for exceptional access, that is one way of framing it.

Another way to frame it would be to say that we intend to guarantee or to align the kind of collective distinguished interests that are on the table here, kind of individual pursuit of security to include companies' abilities to innovate and succeed in national, international marketplaces, and the ability of governments when necessary under exceptional access to access communication for purposes of what Mr. Vance and Jim Comey are pursuing under

their lawful mandate. That is a very different framing.

That might then encourage people to say I am coming to the table because that is the way we are essentially going to make a contribution against the interests I am charged to represent.

Senator Blumenthal: What I see, from Connecticut's standpoint, and we have very able Federal prosecutors, our United States attorney, Deirdre Daly, whom you no doubt know, Mr. Vance, as well as our State prosecutors, increasingly tell and show me that our local and State security are inseparable from our national security, and that the bad guys have seamless ways of accessing information and communicating with each other, and we remain separated in terms of our law enforcement jurisdiction and our inability to access the very means of communication that they use so seamlessly.

So I share the chairman's and your sense of urgency, not that I oppose a commission. Who could oppose a commission focused on this issue? But I feel a much greater sense of urgency and immediacy about the need to address these concerns.

Thank you very much, Senator Reed, Mr. Chairman.

And thank you to our panel.

Senator Reed: [Presiding] On behalf of Chairman McCain, let me recognize Senator King for a very quick

question, because we have floor activity.

Senator King: We have to go vote.

I just want to again sort of clarify. You can tap phones now, right, Apple iPhones, if you get subpoenas, Mr. Vance? You can get the verbal conversation?

Mr. Vance: Some, unless the communications, for example, are encrypted.

Senator King: Okay. Okay, but encryption, we talked about encryption. Encryption is not the issue here. Encryption is encryption, and you can either can get it or you cannot.

You can get messages. You can get the content of messages, unless they are encrypted. You can get where people called under the 215 program under the metadata.

I just want to be clear what it is you can already get without asking companies to unlock their phones, because you are really talking about something other than phone calls, messages, and metadata. You are talking about maybe the geographic -- anyway, I just think it is important.

And that shows the complexity of this issue. You have to really do it in a granular way.

Mr. Vance: Senator, I understand what you are saying. Let's just talk about data at rest, which is of the most interest to law enforcement of what is on the phones. Interestingly, many criminals do not encrypt, and that was

one reason why we were able to get so much information about rape, robbery, murder, and other state law crimes.

Why they do not encrypt is a question I cannot answer. But the fact of the matter is that even when there has been encryption technology, it is not used by the vast majority of people committing crimes.

Therefore, there is an absolutely direct consequence because of now our inability to access those phones, with a court-ordered warrant, information that is on the phone likely not to be encrypted relevant to the criminal investigation is inaccessible.

Senator King: I understand. I would appreciate, to the extent you guys can give us suggested language or proposals or outlines of legislation, that is what we are looking for. Thank you very much.

Thank you, Mr. Chairman.

Senator Reed: Thank you, Senator King.

Gentlemen, thank you for your extraordinarily thoughtful testimony. I can assure you that as the days go forward, and you made it quite clear this is not something that can take forever, we will be reaching out for your advice and your assistance.

I second Senator King's point. Any proactive legislative proposals or ideas, please forward them.

On behalf of Chairman McCain, I also want to explain

that this is a busy day, lots of floor activity. Your testimony was extraordinarily important, the most important issue that we are coming to grips with, which is cybersecurity and protecting the Nation. My colleagues were, I think, deflected to the floor, so I apologize.

But let me thank you all for your extraordinary testimony. On behalf of the chairman, Chairman McCain, let me adjourn the hearing. Thank you.

[The information referred to follows:]

[COMMITTEE INSERT]

[Whereupon, at 10:55 a.m., the hearing was adjourned.]