ENCRYPTION TECHNOLOGY AND POTENTIAL U.S. POLICY RESPONSES

HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

APRIL 29, 2015

Serial No. 114–143

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

25–879 PDF WASHINGTON : 2017

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK, MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

SEAN MCLAUGHLIN, *Chief of Staff*
DAVID RAPALLO, *Minority Chief of Staff*
TROY STOCK, *Staff Director, Subcommittee on Information Technology*
SARAH VANCE, *Staff Assistant*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, *Vice Chair*
MARK WALKER, North Carolina
ROD BLUM, Iowa
PAUL A. GOSAR, Arizona

ROBIN L. KELLY, Illinois, *Ranking Member*
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
TED LIEU, California

CONTENTS

ENCRYPTION TECHNOLOGY AND POTENTIAL U.S. POLICY RESPONSES

Wednesday, April 29, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:32 p.m., in Room 2154, Rayburn House Office Building, Hon. Blake Farenthold [chairman of the subcommittee] presiding.

Present: Representatives Hurd, Farenthold, Walker, Blum, Chaffetz, Kelly, Connolly, and Lieu.

Mr. HURD. The Subcommittee on Information Technology will come to order. Without objection, the chair is authorized to declare a recess at any time.

Good afternoon, everyone. And thanks for attending today's hearing. And I appreciate your flexibility with time. Votes always come at the inopportune moment.

In September of last year, Apple and Google, the largest mobile device manufacturers in the United States, announced that they would implement increased security measures on their products in an attempt to strengthen privacy and data security.

These developments were met with concern from some law enforcement entities, such as the FBI, who were worried that this increased level of encryption would lead to an inability to access data on specific devices and that, despite obtaining a warrant, investigatory efforts could be hindered by this.

As a former CIA officer, I understand and appreciate the need and desire for law enforcement to access digital information in a timely manner. However, I also understand the protections afforded to Americans provided by the Constitution, and I have taken an oath two times to protect and defend these rights.

I firmly believe that law enforcement officials must gain the trust of the very people they are trying to protect in order to be successful, and I remain concerned that a government-mandated back or front door on U.S.-based mobile device manufacturers might undermine that trust.

Today's hearing will involve testimony from a variety of experts and stakeholders and representatives on ways to balance law enforcement needs with privacy and security concerns. The hearing will also explore the impact of this debate on domestic privacy, American consumers, and U.S. technology manufacturers.

As technology continues to evolve and encryption capabilities become a part of everyday life for all Americans, this debate will only

grow larger. I believe we can find a way to protect the privacy of law-abiding citizens and ensure that law enforcement have the tools they need to catch the bad guys.

I welcome the witnesses and look forward to today's discussion.

Mr. HURD. I would like to now recognize my friend and the ranking member of the subcommittee, Ms. Kelly of Illinois, for 5 minutes for an opening statement.

Ms. KELLY. Thank you, Mr. Chairman.

And thank you to our witnesses for appearing on today's panel.

Recently companies like Apple and Google have announced plans to incorporate automatic encryption for their mobile devices. Encryption will become the default privacy feature on their mobile devices, making their content unreadable and inaccessible without the user's selected pass code.

As a society, we rely on mobile devices to manage and protect many aspects of our lives, personal, professional, and financial. Privacy on our smartphones is critically important. Hackers are concerned, as is unrestricted government surveillance.

According to a May 2014 study on trends in U.S. smartphone industry, Android and Apple control 52.1 and 41.9 percent share of the market. Their move towards automatic encryption will have a significant effect on the industry standard for privacy protections.

The move towards automatic encryption has been criticized as seriously hindering law enforcement operations. Criminals, like noncriminals, use mobile devices to manage the many aspects of their lives, some of which can provide evidence of a crime.

Today many criminal cases have a digital component and law enforcement entities increasingly rely on the content of mobile devices to further an investigation or prosecution of serious crimes of national security threats. The FBI, local law enforcement departments, and prosecutors have all expressed concern with automatic encryption.

They envision a number of scenarios in which the inability to assess data kept on mobile devices will seriously hinder a criminal investigation. They do not want to be in a position to tell a victim of a crime or the family of a victim that they cannot save someone or prosecute someone because they cannot access the content of a mobile device. There is a balance to be struck here.

It is important that the Government's policies approach ensures privacy protections and it is important that law enforcement, under tightly controlled circumstances, have the ability to investigate and prosecute crimes. I look forward to today's hearing and your testimony.

Thank you, Mr. Chairman. I look forward to continue working with you to examine policy issues related to advancement and information technology.

I yield back.

Mr. HURD. Thank you.

I am now pleased to recognize Mr. Chaffetz of Utah, the chairman of the full committee, for an opening statement.

Mr. CHAFFETZ. I thank the chairman.

And I appreciate your passion on this topic. It affects literally every American. It affects people all across the world.

I think one of the great questions that needs to be posed to our society and certainly our country as a whole is how to find the right balance between personal privacy and national security. And I, for one, am not willing to give up every bit of privacy in the name of security. So how do we find that right balance? It is not easy to find.

In response to recent moves by Apple and Google mentioned by Chairman Hurd, the FBI Director Comey recommended, quote,"a regulatory or legislative fix," end quote, which would force companies to manufacture their mobile devices in such a way that law enforcement can access the data on those devices without a warrant or court order.

I have three general concerns about Director Comey's proposal:

First, it is impossible to build just a back door for just the good guys, you know, just the good guys can get this. If somebody at the genius bar can figure it out, so can the nefarious folks in a van down by the river.

As Alex Stamos, Yahoo's chief information security officer, recently explained, all of the best public cryptographers in the world would agree that you can't really build back doors in crypto. That is like drilling a hole in a windshield."

The Commerce Department's National Institute of Standards and Technology's chief cybersecurity adviser agreed, saying, quote, "There is no way to do this where you don't have an unintentional vulnerability," end quote. And I worry about those unintentional vulnerabilities.

We have a wide variety of experts on the panel today to help us examine some of the potential economic, privacy, security, and geopolitical consequences of introducing a vulnerability into the system.

Second, we already live in what some experts have referred to as the, quote, "golden age of surveillance," end quote, for law enforcement. Federal, State, and local law enforcement never had more tools at their disposal to help detect, prevent, and prosecute crime. It seems that we hear every day there is new, often-startling stories about the United States Government's ability to track its own citizens.

I recognize technology can be a double-edged sword and many pose challenges for law enforcement as well, but we are certainly not going to go dark, and in many ways we have never been brighter.

Third, strong encryption prevents crime and is a part of the economy. People keep their lives in their mobile phones. A typical mobile phone might hold a person's pictures, contacts, communications, finance schedule, and much more personal information, in addition to my Words with Friends, which is critical to my daily sanity.

If your phone is lost or stolen, you want to know your information is protected, and encryption does that. There is a reason the world's largest technology companies are increasingly developing stronger and more frequently used encryption technology. It is not because they are anti-law enforcement. On the contrary. It is because sophisticated cyber hacks are nearly daily events.

No one is immune from digital snooping, from the White House, to corporate America, to private citizens. The opportunity brought to us by the modern technologies are near limitless, but not if the system is compromised. Strong encryption helps ensure data is secure and allows companies and individuals to operate with confidence and trust.

I look forward to hearing from our witnesses today. But we have choices to make. Do we allow the 99 percent of Americans who are good, honest, decent, hard-working, patriotic people to have encrypted phones or do we need to leave a back door open and create vulnerability for all of them?

Because vulnerability is—it is all or none, folks. It is not just a little bit, not just for the good guys. And that is why we are having this hearing today. I appreciate Chairman Hurd and what he is doing. And I appreciate and thank you all for being here as witnesses today.

I yield back.

Mr. HURD. Thank you.

I am going to hold the record open for 5 legislative days for any members who would like to submit a written statement.

We will now recognize our panel of witnesses.

I am pleased to welcome Ms. Amy Hess, Executive Assistant Director of the Science and Technology Branch at the Federal Bureau of Investigation; Mr. Daniel Conley, District Attorney of Suffolk County, Massachusetts; Mr. Kevin Bankston, Policy Director at New America's Open Technology Institute; Mr. John Potter, President of the Application Developers Alliance; and Dr. Matthew Blaze, Associate Professor of Computer and Information Science of the School of Engineering and Applied Science at the University of Pennsylvania. Welcome to all.

Pursuant to committee rules, all witnesses will be sworn in before they testify. So please rise and raise your right hands.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Mr. HURD. Let the record reflect that all witnesses answered in the affirmative. Thank you.

In order to allow time for discussion, please limit your testimony to 5 minutes. Your entire written statement will be made part of the record.

And, Ms. Hess, we will start with you. You are recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF AMY S. HESS

Ms. HESS. Thank you. Good afternoon, Chairman Chaffetz, Chairman Hurd, Ranking Member Kelly, and members of the subcommittee. Thank you for the opportunity to appear here today and for your continued support of the men and women of the FBI.

The Bureau has undergone an unprecedented transformation in recent years to address and prevent threats to our national security and our public safety. But as those threats continue to evolve, the FBI must evolve as well. Today's FBI is a threat-focused, intel-

ligence-driven organization, and we must continuously challenge ourselves to stay ahead of changing threats and changing circumstances.

As you know, technology has forever changed the world we live in. Our phones and computers have become reflections of our personalities, interests, and our identities. And with that comes the need to protect our privacy and our data.

But technology can be used by some very dangerous people, and the FBI has a sworn duty to keep every American safe from harm while simultaneously protecting their constitutional rights and preserving their civil liberties.

Moreover, we recognize our national interests in promoting innovation and the competitiveness of U.S. companies in the global marketplace, as well as freedom of expression around the world.

But the evolution of technology creates new challenges for law enforcement. It impacts our ability to access communications pursuant to court orders, which means those of us charged with protecting the American people aren't always able to access the information we need to prosecute criminals and prevent terrorism, even though we have the lawful authority to do so.

To be clear, we obtain the proper legal authority to intercept and access communications and information, but we increasingly lack the technical ability to do so. This problem, which we refer to as "going dark," is broader and more extensive than just encryption, but for the purposes of today's testimony, I will focus on the challenges of the evolving use of encryption.

We encounter encryption in two overlapping contexts. The first is legally authorized realtime interception of what we call data in motion, such as phone calls, emails, and text messages in transit. The second concerns legally authorized access to data stored on our devices or what we call data at rest.

First let me address court-ordered interception of data in motion. In the past, there were a limited number of communication carriers conducting electronic surveillance and it was more straightforward. We developed probable cause to believe a suspected criminal was using a target phone to commit a felony. We then obtained a court order for a wiretap on that phone. And under the supervision of a judge, we collected the evidence we needed for prosecution.

Today there are countless providers, networks, and means of communicating. We have laptops, smartphones, and tablets. We use multiple networks and any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, target victims, and concoct alibis. Thousands of companies now provide some form of communication service, but most do not have the ability to isolate and deliver particular information when urged to do so by a court.

Turning to court-ordered access to data at rest, we know that encryption of stored data is not new, but it has become increasingly prevalent and sophisticated. And the challenge to law enforcement and national security officials has been heightened with the advent of default encryption settings and stronger encryption standards.

In the past, the consumer had to decide whether to encrypt data stored on his or her device and take action. But with today's new operating systems, a device and all of the user's information on the

device can be encrypted by default. Further, companies have developed encryption technology which makes it impossible for them to decrypt data on devices they manufacture, even when lawfully ordered to do so.

Although there are certainly good reasons to support these new uses of encryption, such decisions regarding system design have a tremendous impact on our ability to fight crime and bring perpetrators to justice. Like the general population, criminals are increasingly storing such information on electronic devices and, if these devices are encrypted, the information they contain may be unreadable to anyone other than the user. The process of obtaining a search warrant authorized by a court of law to seek evidence of a crime could be an exercise in futility.

To be clear, we in the FBI support and encourage the use of secure networks and sophisticated encryption to prevent cyber threats. We know that adversaries will exploit any vulnerability they find, but we believe that security risks associated with the implementation of lawfully authorized access are better addressed by developing solutions during the design phase rather than resorting to a patchwork solution after the product or service has been deployed.

Just as we have an obligation to address threats to national security and public safety, we likewise have an obligation to consider the potential impact of our investigations on civil liberties, including the right to privacy. We must always act within the confines of the rule of law and the safeguards guaranteed by the Constitution.

We also believe that no one in this country should be beyond the law. The notion that a suspected criminal's closet could never be opened or his phone could never be unlocked, even with properly obtained legal authority, is troubling.

We will, of course, use every lawfully authorized technique we have to protect the citizens we serve, but having to rely on those other tools could delay criminal investigations, preclude us from identifying victims and coconspirators, risk prematurely alerting suspects to our investigative interests, and potentially put lives in danger.

Thank you again for this opportunity to discuss the FBI's priorities and the challenges of "going dark." The work we do would not be possible without the support of Congress and the American people. I look forward to your questions.

[Prepared statement of Ms. Hess follows:]

Department of Justice

STATEMENT OF

AMY HESS
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON INFORMATION TECHNOLOGY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

CONCERNING

ENCRYPTION AND CYBERSECURITY FOR
MOBILE ELECTRONIC COMMUNICATION DEVICES

PRESENTED

APRIL 29, 2015

Statement of
Amy Hess
Executive Assistant Director
Federal Bureau of Investigation

Before the
Subcommittee on Information Technology
Oversight and Government Reform
U.S. House of Representatives

Concerning
Encryption and Cybersecurity for
Mobile Electronic Communication Devices

Presented
April 29, 2015

Good morning/afternoon, Chairman Hurd, Ranking Member Kelly, and members of the Subcommittee. Thank you for the opportunity to appear before the Committee today, and for your continued support of the men and women of the FBI.

Today's FBI

As you know, the Bureau has undergone unprecedented transformation in recent years to address and prevent threats to our national security and our public safety, from terrorism, state-sponsored espionage, and cyber security to violent gangs, transnational organized crime, and crimes against children.

As national security and criminal threats continue to evolve, so too must the FBI evolve to stay ahead of changing threats and changing technology. Today's FBI is a threat-focused, intelligence-driven organization. We must continually ask ourselves whether we are able to meet the challenges of the day, whatever they may be.

Online technology has forever changed the world we live in. We're online, in one form or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. With this online presence comes the need to protect our privacy and the security of our data.

But, as with any technology, it can be used by some very dangerous people, and the FBI has a sworn duty to keep every American safe from crime and terrorism while simultaneously protecting their constitutional rights and preserving their civil liberties. Moreover, we recognize

our national interests in promoting innovation and the competiveness of U.S. companies in the global marketplace, as well as freedom of expression around the world.

The evolution of technology is creating new challenges for law enforcement and our ability to access communications. We call it "Going Dark," and it means that those charged with protecting the American people aren't always able to access the information necessary to prosecute criminals and prevent terrorism even though we have lawful authority to do so. To be clear, we obtain the proper legal authority to intercept and access communications and information, but we increasingly lack the technical ability to do so. This problem is broader and more extensive than just encryption. But, for purposes of my testimony today, I will focus on the challenges we face based on the evolving use of encryption.

The issues law enforcement encounters with encryption occur in two overlapping contexts. The first concerns legally authorized real-time interception of what we call "data in motion," such as phone calls, email, text messages and chat sessions in transit. The second challenge concerns legally authorized access to data stored on devices, such as email, text messages, photos, and videos – or what we call "data at rest." Both data in motion and data at rest are increasingly encrypted.

Court-Ordered Interception of Encrypted Data in Motion

In the past, there were a limited number of communications carriers. As a result, conducting electronic surveillance was more straightforward. We identified a target phone being used by a suspected criminal, obtained a court order for a wiretap, and, under the supervision of a judge, collected the evidence we needed for prosecution.

Today, communications occur across countless providers, networks, and devices. We take our laptops, smart phones, and tablets to work and to school, from the soccer field to the coffee shop, traversing many networks, using any number of applications. And so, too, do those conspiring to harm us. They use the same devices, the same networks, and the same applications to make plans, to target victims, and to concoct cover-up stories.

Law enforcement and national security investigators need to be able to access communications and information to obtain the evidence necessary to prevent crime and bring criminals to justice in a court of law. We do so pursuant to the rule of law, with clear guidance and strict judicial oversight. But increasingly, even armed with a court order based on probable cause, we are too often unable to access potential evidence.

The Communications Assistance for Law Enforcement Act (CALEA) requires telecommunication carriers to be able to implement court orders for the purpose of intercepting

communications. But that law wasn't designed to cover many of the new means of communication that exist today. Currently, thousands of companies provide some form of communication service, but most do not have the ability to isolate and deliver particular information when ordered to do so by a court. Some have argued that access to metadata about these communications – which is not encrypted – should be sufficient for law enforcement. But metadata is incomplete information, and can be is difficult to analyze when time is of the essence. It can take days to parse metadata into readable form, and additional time to correlate and analyze the data to obtain meaningful and actionable information.

Court-Ordered Access to Stored Encrypted Data

Encryption of stored data is not new, but it has become increasingly prevalent and sophisticated. The challenge to law enforcement and national security officials has intensified with the advent of default encryption settings and stronger encryption standards on both devices and networks.

In the past, a consumer had to decide whether to encrypt data stored on his or her device and take some action to implement that encryption. With today's new operating systems, however, a device and all of a user's information on that device can be encrypted by default – without any affirmative action by the consumer. In the past, companies had the ability to decrypt devices when the Government obtained a search warrant and a court order. Today, companies have developed encryption technology which makes it impossible for them to decrypt data on devices they manufacture and sell, even when lawfully ordered to do so. Although there are strong and appropriate cybersecurity and other reasons to support these new uses of encryption, such decisions regarding system design have a tremendous impact on law enforcement's ability to fight crime and bring perpetrators to justice.

Evidence of criminal activity used to be found in written ledgers, boxes, drawers, and file cabinets, all of which could be searched pursuant to a warrant. But like the general population, criminal actors are increasingly storing such information on electronic devices. If these devices are automatically encrypted, the information they contain may be unreadable to anyone other than the user of the device. Obtaining a search warrant for photos, videos, email, text messages, and documents can be an exercise in futility. Terrorists and other criminals know this and will increasingly count on these means of evading detection.

Additional Considerations

Some assert that although more and more devices are encrypted, users back-up and store much of their data in "the cloud," and law enforcement agencies can access this data pursuant to court order. For several reasons, however, the data may not be there. First, aside from the technical requirements and settings needed to successfully back up data to the cloud, many

companies impose fees to store information there – fees which consumers may be unwilling to pay. Second, criminals can easily avoid putting information where it may be accessible to law enforcement. Third, data backed up to the cloud typically includes only a portion of the data stored on a device, so key pieces of evidence may reside only on a criminal's or terrorist's phone, for example. And if criminals do not back up their phones routinely, or if they opt out of uploading to the cloud altogether, the data may only be found on the devices themselves – devices which are increasingly encrypted.

Facing the Challenge

The reality is that cyber adversaries will exploit any vulnerability they find. But security risks are better addressed by developing solutions during the design phase of a specific product or service, rather than resorting to a patchwork solution when law enforcement presents the company with a court order after the product or service has been deployed.

To be clear, we in the FBI support and encourage the use of secure networks and sophisticated encryption to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data. We have been on the front lines of the fight against cybercrime and economic espionage and we recognize that absolute security does not exist in either the physical or digital world. Any lawful intercept or access solution should be designed to minimize its impact upon the overall security. But without a solution that enables law enforcement to access critical evidence, many investigations could be at a dead end. The same is true for cyber security investigations; if there is no way to access encrypted systems and data, we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets.

A common misperception is that we can simply break into a device using a "brute force" attack – the idea that with enough computing resources devoted to the task, we can defeat any encryption. But the reality is that even a supercomputer would have difficulty with today's high-level encryption standards. And some devices have a setting that erases the encryption key if someone makes too many attempts to break the password, effectively closing all access to that data.

Finally, a reasonable person might also ask, "Can't you just compel the owner of the device to produce the information in a readable form?" Even if we could compel an individual to provide this information, a suspected criminal would more likely choose to defy the court's order and accept a punishment for contempt rather than risk a 30-year sentence for, say, production and distribution of child pornography.

Without access to the right evidence, we fear we may not be able to identify and stop child predators hiding in the shadows of the Internet, violent criminals who are targeting our

neighborhoods, and terrorists who may be using social media to recruit, plan, and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who can't provide us with the password, especially when time is of the essence.

Examples

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that evidence that was once found in filing cabinets, letters, and photo albums will now be available only in electronic storage. We have seen case after case – from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation – where critical evidence came from smart phones, computers, and online communications.

Each of the following examples demonstrates how important information stored on electronic devices can be to prosecuting criminals and stopping crime. As encryption solutions become increasingly inaccessible for law enforcement, it is cases like these that could go unsolved, and criminals like these that could go free.

As an example of the importance of lawful access to smart phones, consider the case involving a long-haul trucker who kidnapped his girlfriend, imprisoned her within his truck, drove her from State to State, and physically and sexually assaulted her along the way. The victim eventually leapt from the truck and escaped to nearby civilians, and later the police. The trucker refuted the charges and claimed the sexual activity was consensual. In this case, law enforcement obtained a search warrant for the trucker's smart phone, as well as a court order requiring the phone manufacturer's assistance to extract that data. Through this court-authorized process, law enforcement recovered video and images of the abuse stored on the smart phone, which were integral to corroborating the victim's testimony at trial. The trucker was convicted of kidnapping and interstate domestic violence at trial, and sentenced to life in prison.

Additionally, in a case investigated by a small Midwest police department, a woman reported that an unknown stranger forcibly raped her while she was out walking. She sought treatment at a local hospital where a sexual assault examination was performed. However, the investigator noted peculiarities in the woman's responses during the interview and requested access to her phone. She consented and, using forensic tools, the investigator uncovered evidence indicating the woman had sought out a stranger via an Internet advertisement with the intent to get pregnant. To cover her infidelity, she fabricated the story that a stranger had raped her. When confronted with the communications recovered from her phone, the woman admitted the rape report was false. Without the digital evidence, an innocent man may well have been accused of a violent sexual assault.

Another investigation in Clark County, Nevada, centered on allegations that a woman and her boyfriend conspired together to kill the woman's father who died after being stabbed

approximately 30 times. Text messages which had been deleted from the phone and recovered by investigators revealed the couple's plans in detail, clearly showing premeditation. Additionally, the communications around the time of the killing proved that both of them were involved throughout the process and during the entire event, resulting in both being charged with murder and conspiracy to commit murder.

Following a joint investigation conducted by the FBI and Indiana State Police, a pastor pleaded guilty in Federal court to transporting a minor across state lines with intent to engage in illicit sexual conduct in connection with his sexual relationship with an underage girl who was a student at the church's high school. During this investigation, information recovered from the pastor's smart phone proved to be crucial in showing the actions taken by the pastor in the commission of his crimes. Using forensic software, investigators identified Wi-Fi locations, dates, and times when the pastor traveled out of state to be with the victim. The analysis uncovered Internet searches including, "What is the legal age of consent in Indiana", "What is the legal age of consent in Michigan", and "Penalty for sexting Indiana." In addition, image files were located which depicted him in compromising positions with the victim.

These are examples of how important evidence that resides on smart phones and other devices can be to law enforcement – evidence that might not have been available to us had strong encryption been in place on those devices and the user's consent not granted.

The above examples serve to show how critical electronic evidence has become in the course of our investigations and how timely, reliable access to it is imperative to ensuring public safety. Today's encryption methods are increasingly more sophisticated, and pose an even greater challenge to law enforcement. We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop – evidence that may be the difference between an offender being convicted or acquitted – but we cannot access it.

Previously, a company that manufactured a communications device could assist law enforcement in unlocking the device. Today, however, upon receipt of a lawful court order, the company might only be able to provide information that was backed up in the cloud – and there is no guarantee such a backup exists, that the data is current, or that it would be relevant to the investigation. If this becomes the norm, it will be increasingly difficult for us to investigate and prevent crime and terrorist threats.

Civil Liberties and the Rule of Law

Just as we have an obligation to address threats to our national security and our public safety, we also have an obligation to consider the potential impact of our investigations on civil liberties, including the right to privacy.

Intelligence and technology are key tools we use to stay ahead of those who would do us harm. Yet, as we evolve and adapt our investigative techniques and our use of technology to keep pace with today's complex threat environment, we must always act within the confines of the rule of law and the safeguards guaranteed by the Constitution.

The people of the FBI are sworn to protect both security and liberty. We care deeply about protecting liberty – including an individual's right to privacy through due process of law – while simultaneously protecting this country and safeguarding the citizens we serve.

The rule of law is our true north; it is the guiding principle for all that we do. The world around us continues to change, but within the FBI, our values must never change. Every FBI employee takes an oath promising to uphold the United States Constitution. It is not enough to catch the criminals; we must do so while upholding civil rights. It is not enough to stop the terrorists; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights are not burdens. They are what make all of us safer and stronger. In the end, we in the FBI will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

And with the rule of law as our guiding principle, we also believe that no one in this country should be beyond the law. We must follow the letter of the law, whether examining the contents of a suspected individual's closet or the contents of her smart phone. But the notion that the closet could never be opened – or that the phone could never be unlocked or unencrypted – even with a properly obtained court order, is troubling.

Are we as a society comfortable knowing that certain information is no longer available to law enforcement under any circumstances? Is there no way to reconcile personal privacy and public safety? It is time to have open and honest debates about these issues.

Where Do We Go From Here?

The FBI confronts serious threats to public safety every day. So in discussing developments that thwart the court-authorized tools we use to investigate suspected criminals, we must be sure to understand what society gains, and what we all stand to lose. What is law enforcement's recourse when we are not able to access stored data and real-time communications, despite having a court order? What happens when we cannot decipher the passcode? What happens if there are no other means to access the digital evidence we need to find a victim or prosecute a criminal? We will use every lawfully authorized investigative tool

we have to protect the citizens we serve, but having to rely on those other tools could delay criminal investigations, preclude us from identifying victims and co-conspirators, risk prematurely alerting suspects to our investigative interests, and potentially put lives in danger.

We will continue to work with our Federal, State, tribal, and local partners to identify a path forward. We are thankful for Congress' support in funding the National Domestic Communications Assistance Center, which will enable law enforcement to share tools, train one another in available intercept solutions, and reach out to the communications industry with one voice.

Companies must continue to provide strong encryption for their customers and make every effort to protect their privacy, but so too does law enforcement have a real need to obtain certain communications data when ordered by a court of law. We care about the same things – safety, security, and prosperity. And from the FBI's perspective, we know an adversarial posture won't help any of us in achieving those things. We must challenge both government and industry to develop innovative solutions to secure networks and devices, yet still yield information needed to protect our society against threats and ensure public safety.

Perhaps most importantly, we need to make sure the American public understands the issues and what is at stake.

I believe we can come to a consensus, through a reasoned and practical approach. And we must get there together. It is only by working together – within the law enforcement and intelligence communities, with the private sector, and with our elected officials – that we will find a long-term solution to this growing problem.

We in the FBI want to continue the discussion about how to solve these serious problems. We want to work with Congress, with our colleagues in the private sector, with our law enforcement and national security partners, and with the people we serve, to find the right balance for our country.

Conclusion

Chairman Hurd, Ranking Member Kelly, and members of the committee, I thank you for this opportunity to discuss the FBI's priorities and the challenges of Going Dark. The work we do would not be possible without the support of Congress and the American people. I would be happy to answer any questions that you may have.

# # #

Mr. HURD. Thank you, Ms. Hess.
Now we recognize Mr. Conley for 5 minutes.

STATEMENT OF DANIEL F. CONLEY

Mr. CONLEY. Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, my name is Dan Conley, and I'm the District Attorney in Boston and a member of the National District Attorneys Association, the largest association of prosecutors in America. Thank you for the invitation to testify today here today on this critical issue.

Last year, when Apple and Google announced their new operating system, they touted that the technology would not allow law enforcement, even with a court order, to access information on its mobile devices.

In America, we often say that none of us is above the law. But when corporate interests place crucial evidence beyond the legitimate reach of our courts, they are, in fact, granting those who rape, defraud, assault, or even kill a profound legal advantage over victims in society. So I'm here today to ask Congress to intervene.

As a prosecutor, my most important duty is to ensure that evidence we present in court is gathered fairly, ethically, and legally. If it's not, if a search is improper, a court will suppress that evidence and exclude it.

We, as Americans, enjoy a presumptive right to privacy that may only be abridged under clearly defined circumstances, such as when there are specific articulable facts that would lead a judge to believe that the place to be searched will yield evidence of a crime. In decades past, these places were car trunks and safety deposit boxes. Today they are mobile devices.

We undertake those searches to solve crimes. We don't wander to Web sites where people visit or aggregate data about people's personal health, wealth, or shopping habits. That, frankly, is the purview of companies like Apple and Google.

Their nominal commitment to privacy rights would be far more credible if they were forbidding themselves access to their customers' interests, search terms, and consumer habits. But, as we all know, they are taking full advantage of their customers' private data for commercial purposes while building an impenetrable barrier around evidence in legitimate court-authorized investigations.

For over 200 years of American jurisprudence, our courts have balanced the rights of individuals against society. But, in this case, in one fell swoop, Apple and Google have upended it. They have created hiding places not merely beyond the reach of law enforcement, but beyond the laws that define our Nation.

Let me give you an idea of what this means in practical terms. In every big city, there's a mass transit system and a disgraceful practice of snapping photographs up women's skirts has taken place. If the offender's phone cannot be searched pursuant to a warrant, then the evidence won't be recovered and this practice will be an unchargeable crime. This isn't even the worst of it.

Three years ago we were investigating a child pornography case. We just thought a teacher was trading child pornography. Turns out, after we got a warrant and examined his mobile devices, he was not only collecting photographs, he was actually abusing chil-

dren. After a multijurisdictional investigation, he's serving 45 years in prison. If those devices were encrypted today, he would be free to continue what he's doing on our streets.

Human trafficking and commercial sexual exploitation of children is also aided and abetted by the same technology with victims, including children, advertised for sale on Web sites accessed through handheld devices. With these operating systems, those devices would become warrant-proof and the evidence they contain unreachable by investigators.

Now, I don't believe Apple or Google set out to design an encryption system to protect human traffickers, but this is the result. When we talk about warrant-proof encryption, it is the perpetrators of every violent sexual or financial crime in which handheld technology is used who benefit. This isn't rhetoric. This is reality.

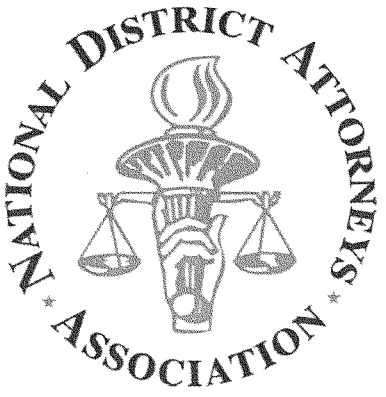
Like most Americans, I am a customer of these companies and I hold my privacy interest dear, and I understand and I strongly encourage the use of secure encryption technology to prevent hacking, theft, and fraud. And I think most people recognize that there must be a balance struck between individual's privacy rights and the legitimate interests of our society to bring dangerous criminals to account. Apple and Google need to recognize this as well.

I will conclude today by pointing out that, for the past several weeks, in Boston and around the country, individuals have all been following the trial of one of the individuals who was a terrorist in Boston 2 years ago and, through his actions, left four people dead and hundreds more grievously injured. Cell phone evidence, much of it volunteered by people, but some of it obtained by warrant, was critical to understanding what happened, how it happened, and who did it.

Were law enforcement blocked from obtaining that evidence, the apprehension of those responsible for the Boston Marathon bombings might have been very much in doubt. So, again, I don't think Apple or Google intended to create a safe space for terrorists to do their deeds. But make no mistake. This is the result and those are the stakes.

I therefore respectfully urge Congress to help us find a reasonable, balanced solution that protects privacy while also ensuring that there are reasonable means to gain lawful access to crucial evidence. I thank you for your time and attention, and I look forward to your questions. Thank you.

[Prepared statement of Mr. Conley follows:]



Testimony of
Daniel F. Conley
Suffolk County District Attorney
Massachusetts

Encryption Technology and Potential U.S. Policy Responses

Committee on Oversight and Government Reform

Subcommittee on Information Technology

Wednesday, April 29, 2015

Chairman Hurd, Ranking Member Kelly, members of the subcommittee, my name is Dan Conley and I am the elected District Attorney of Suffolk County, Massachusetts, which includes the city of Boston. I am also currently a board member of the National District Attorneys Association (NDAA), the largest association representing the voice of prosecutors across the country. I appreciate the invitation to testify before you today on a critical issue facing state and local law enforcement from around the country.

Last year, when Apple announced its new iOS 8 operating system, it touted the fact that this technology would not allow law enforcement, even with a court order, to access information on its mobile phones, computers, iPads and other devices. Google also stated that its new operating system would make its mobile devices inaccessible to law enforcement officials, even with a warrant signed by a judge. What's more, this inaccessibility has been presented not as a bug to be fixed but as a selling point to be featured.

In America, we often say that none of us is above the law. But when unaccountable corporate interests place crucial evidence beyond the legitimate reach of our courts, they are in fact placing those who rape, defraud, assault and even kill in a position of profound advantage over victims and society. One of my colleagues, Cy Vance, the District Attorney for New York County, has been a leading voice on this issue. He's met directly with representatives from Google and Apple to listen to their concerns, express our own, lay out the facts, and find a solution, but has been unable to move them from their position. So I am here today to ask Congress to help us find a solution because what Apple and Google are doing is dangerous and should not be allowed to continue.

As a prosecutor, one of my most important duties is to ensure that the evidence we present in court is gathered fairly, ethically, and legally. There is a very good reason for this: the penalty for overreach is suppression of the evidence. If a search is illegal, if a warrant is flawed, then the evidence it yields is excluded and we cannot use it. Under the Fourth Amendment to the Constitution, we as Americans enjoy a presumptive right to privacy that may only be violated under certain, clearly-defined circumstances. Among those circumstances is when there are

specific, articulable facts that would lead a reasonable person – and a judge – to believe that the place to be searched will yield evidence of a crime.

In short, the Fourth Amendment allows law enforcement access to the places where criminals hide evidence of their crimes, once the legal threshold has been met. In decades past, these places were car trunks and safety deposit boxes; today they are computers and smart phones.

Law enforcement agencies like mine undertake these lawful searches to solve crimes that have occurred and prevent further crimes from taking place. We don't monitor what web sites people visit, or aggregate data about people's personal health, wealth, or shopping habits. That, frankly, is the purview of companies like Apple and Google. Their nominal commitment to privacy rights would be far more credible if they were forbidding themselves access to their customers' interests, search terms, and consumer habits, but as we all know, that's not a step they're willing to take. Instead, they're taking full advantage of their customers' private data for commercial purposes while building an impenetrable barrier around evidence in legitimate, court-authorized criminal investigations.

Apple and Google are using an unreasonable, hypothetical narrative of government intrusion as the rationale for the new encryption software, ignoring altogether the facts as I've just explained them. And taking it to a dangerous extreme in these new operating systems, they've made legitimate evidence stored on handheld devices inaccessible to anyone, even with a warrant issued by an impartial judge. For over 200 years, American jurisprudence has refined the balancing test that weighs the individual's rights against those of society, and with one fell swoop Apple and Google has upended it. They have created spaces not merely beyond the reach of law enforcement agencies, but beyond the reach of our courts and our laws, and therefore our society.

Let me give you an idea what this means in practical terms. In every major city with mass transit, prosecutors have been confronted with a rising number of men who use their phones to take pictures and videos up female passengers' skirts. The practice is called "upskirting," and it violates the right that every person has to privacy beneath our own clothes. If the offender's

phone can't be searched pursuant to a warrant, then the evidence won't be recovered and this practice will become absolutely un-chargeable as a criminal offense. But this isn't nearly the worst of it.

Three years ago, we were investigating a child pornography case that led us to a Boston-area teacher. These cases, which re-victimize child rape victims every time an image or video clip is shared, have skyrocketed in the past decade with the advent of faster, more powerful technology. Early on in this particular case, we believed the teacher was merely trading child pornography, but after obtaining and executing search warrants on his electronic devices we recovered evidence that he was actually abusing children and recording his crimes. After a multi-jurisdictional investigation, he was indicted and sentenced to a 45-year federal prison sentence. But if his phone had been encrypted with the technology at issue today, that evidence would have been beyond our reach and he would have been above the law.

Human trafficking and commercial sexual exploitation of children is also on the rise in America and globally, aided and abetted by the same technology. It's moved off the street corner and into motels with Wi-Fi access, with victims, including children, advertised for sale on web sites accessed through handheld devices. With these operating systems, those devices would become warrant-proof and the evidence they contain unreachable by investigators. I don't believe that Apple or Google set out to design a system to enable human trafficking, but that's precisely what these new systems do.

So when we talk about warrant-proof encryption, let's be very clear about who will benefit from it: perpetrators of every violent, sexual, or financial crime in which handheld technology is used. I would be hard pressed to think of any homicide solved in recent years where significant, critical evidence wasn't recovered from a cell phone. We've uncovered massive economic and financial fraud schemes and disrupted vast drug trafficking rings, none of which could have been stopped, let alone solved, had law enforcement – with the blessing of the courts - been blocked from exercising the legal and legitimate means to do so. This isn't rhetoric. It's reality.

Apple and Google operating systems run a combined 96.4% of smartphones worldwide, and as of March, 78% of all Apple devices are running iOS 8. This means law enforcement is unable to access data on 78% of all pin-locked Apple devices, and that number is growing every day. It is a myth that law enforcement has some secret means to decrypt these devices. It is also patently false to claim that this same data can be downloaded from the cloud when most of it is never uploaded to begin with.

This is not an issue of mass data collection. Whatever some advocates might claim about the search warrants granted each year to federal, state and local law enforcement, those warrants are authorized by independent judges, they are based upon an established legal principle, and they affect only the tiny, tiny percentage of the population against whom there is specific, articulable evidence of criminal activity. Let's remember, the vast majority of people are leading honest, upstanding lives every day. We're not interested in what's on their phones. Even Apple's own estimates show that only 0.00571% of customers had information disclosed due to government information requests.

And while some might point to overreach and intrusion by the NSA as justification for designing phones that block out entirely the government's ability to gain access to them, I think the vast majority of Americans recognize that over-reacting and shutting off access to these phones under and any and all circumstances will not only make it monumentally harder to solve crimes and hold criminals accountable in the digital age, but will also make it infinitely more difficult to detect and prevent terrorist threats.

It is ironic that what Google and Apple are doing is, in many ways, a response to what occurred at the NSA, but it is state and local law enforcement and the tens of millions of Americans we protect and victims we serve who are now bearing the brunt of it. We recognize that Google and Apple are global companies with a worldwide customer base, but whatever goodwill or support they believe they will earn with these dangerous operating systems will erode rapidly as victims of physical and economic predation find their paths to justice blocked while those who hurt and exploit them are protected.

Let's also be clear about another unintended consequence of these operating systems: by cutting off law enforcement and society's legitimate interests in obtaining evidence to hold the guilty accountable, it also cuts us off from crucial evidence that speaks to factual innocence. While the evidence obtained from a smart phone will often place an individual at the scene of a crime or provide other evidence of guilt, that same information eliminates other people from the realm of possible suspects. In the past decade, the technology driving exonerations of wrongly convicted defendants has been DNA science. But the day is not far off when a piece of digital evidence obtained from a cell phone will prove to be the key that frees an innocent man.

What these companies are doing is unprecedented, and for good reason: they are substituting their own interests for 200 years of jurisprudence and the independent judgment of our courts, our legislatures, and our Congress as to how the Fourth Amendment to the Constitution should be balanced and applied.

In addition, I can think of no other example of a tool or technology that is specifically designed and allowed to exist completely beyond the legitimate reach of law enforcement, our courts, our Congress, and thus, the people. Not safe deposit boxes, not telephones, not automobiles, not homes. Even if the technology existed, would we allow architects to design buildings that would keep police and firefighters out under any and all circumstances? The inherent risk of such a thing is obvious so the answer is no. So too are the inherent risks of what Apple and Google have devised with these operating systems that will provide no means of access to anyone, anywhere, anytime, under any circumstance.

Like most Americans, I too am a customer of these companies and I hold my privacy rights dear. As the head of one of the largest District Attorney's Offices in the country, I also understand the value of, and strongly encourage the use of, secure encryption technology to prevent hacking, theft, and fraud. I think most people recognize however, that balance must be struck between an individual's privacy rights and the legitimate interests of society to protect itself and bring dangerous criminals to justice. Apple and Google need to recognize this, too.

I will conclude today by pointing out that for weeks now in Boston and all across the country, we have been following the trial of one of the terrorists whose actions at the Boston Marathon two years ago left four people dead and hundreds more grievously injured. Cell phone evidence – much of it volunteered but some obtained only through a warrant - was critical to understanding what happened, how it happened, and who did it. Were law enforcement blocked from obtaining that evidence, or if other companies were allowed to make their own determinations as to what video or other evidence law enforcement was and was not permitted to see, the apprehension of those responsible for the Boston Marathon bombings would have been very much in doubt. Again, I don't believe that Apple or Google intend to create "safe space for terrorists", but make no mistake, that would be the result and those are the stakes.

Therefore, I respectfully urge Congress to prohibit the sale of digital devices that cannot be accessed pursuant to court orders. I would further urge Congress to update the Communications for Law Enforcement Assistance Act, or CALEA, to cover smartphones and ensure that there is a reasonable solutions for law enforcement to gain legal access to crucial evidence. Thank you for your time and attention and I am happy to take any questions you might have.

Mr. HURD. Thank you, Mr. Conley.

Now I would like to recognize Mr. Bankston for 5 minutes.

STATEMENT OF KEVIN S. BANKSTON

Mr. BANKSTON. Thank you, Chairman, Ranking Member Kelly, members of the subcommittee.

District Attorney Conley is absolutely right that encryption is one of the most critical law-and-order issues of our time. However—and with respect and thanks for his and the FBI's work to keep us all safer—he has got it exactly backward. Strong encryption is absolutely critical to the preservation of law and order in the digital age much more than it is a threat to it.

Some have framed this debate as a choice between safety and privacy, but that is a false choice. The debate over whether to allow strong encryption without back doors is really a choice between safety and safety, a little more safety against some isolated crimes or much more safety for many more people against countless other concrete criminal and national security threats, be they street criminals looking to steal our phones and laptops, ID thieves and fraudsters and Russian hackers and corporate spies trying to steal our most valuable data, or foreign intelligence agencies trying to compromise our most sensitive national security secrets.

The ultimate question isn't what will make law enforcement's job easier in some investigations. The ultimate question is what will prevent more crime, which will make law enforcement's job easier overall and will keep us all safer. The answer to that question is more strong encryption, not less.

I won't deny that encrypted devices or end-to-end encrypted communications will, in some cases, inconvenience law enforcement. Notably, however, the Government has yet to provide a single specific example where such encryption has posed an insurmountable problem. That's likely because there are often a variety of other ways for law enforcement to get the evidence that it needs.

The FBI is concerned that it's "going dark." But, all in all, the digital revolution has been an enormous boon to law enforcement, what some have called a golden age of surveillance.

More and more of our interactions with others and with the world are moving into the digital realm, being quantified and recorded, an unprecedented and exponentially growing cache of sensitive data about all of us, and most of it available to law enforcement.

Think about the massive archives of private email and instant messages and text messages and photos and videos and the vast public records of our social network activities, most of which didn't exist or weren't available just 15 years ago, most of which are stored in the Internet cloud and are easily accessible to law enforcement, and much of which is backed up from the very same encrypted phones that the Government is concerned about.

Think of all the new metadata revealing when and with whom all those messages were exchanged, where and when those photos and videos were taken. And think especially about all that new location data generated by our cell phones and by our mobile apps, creating extensive records of our movements regardless of whether those phones are encrypted or not.

Think about all of that when law enforcement says it is going dark. I would counter that, by most measures, they are going bright. And in those few cases where they are in the dark and they truly need the data on an encrypted device, even then there are options.

They can in many cases ask the Court to compel the owner to decrypt the device under threat of contempt or even remotely hack into the device over the Internet, a technique that is somewhat worrisomely being used more and more often.

Admittedly, I have some serious constitutional concerns about both of those law enforcement techniques, but I am much more concerned that, in order to address those rare cases, law enforcement seems to want Congress to take steps that would undermine everyone's security rather than targeting an individual suspect.

Make no mistake. Attempting to mandate encryption back doors will undermine everyone's security, as Professor Blaze will testify. That is the unanimous conclusion of every technical expert that has spoken publicly on this issue.

And, as Mr. Potter will make clear, surveillance backdoor mandates would also undermine our economic security and prompt international customers and many American consumers and even many of the bad guys that we're trying to stop to turn away from the compromised products and services offered by U.S. companies.

It's true now, just as it was true during the so-called crypto wars of the 1990s, weakening encryption is a bad idea. That is why a majority of the House of Representatives at the time, including four current members of this Oversight Committee, including Ranking Member Cummings, co-sponsored Chairman Goodlatte's Security and Freedom Through Encryption Act, which would have reaffirmed Americans' right to make, use, and distribute strong encryption products without back doors.

That is why a majority of the House just last year voted for the Sensenbrenner-Massie-Lofgren Amendment that would have prohibited the NSA from demanding or even asking that companies weakenthe security of their products. And that is why this Congress should similarly reject any short-sighted backdoor proposals in favor of preserving our long-term national and economic security.

Thank you very much. And I look forward to your questions, in particular, any questions about the 10 specific arguments laid out in my written testimony. Thank you.

[Prepared statement of Mr. Bankston follows:]

Statement of Kevin S. Bankston
Policy Director of New America's Open Technology Institute
& Co-Director of New America's Cybersecurity Initiative

Before the U.S. House of Representatives
Subcommittee on Information Technology
of the Committee on Oversight and Government Reform

Hearing on "Encryption Technology and Possible U.S. Policy Responses"

April 29, 2015

Chairman Hurd, Ranking Member Kelly and Members of the Subcommittee:

Thank you for giving me the opportunity to testify today on the importance of strong encryption technology to Americans' continued security and prosperity, and allowing me to articulate the arguments against recent suggestions that Congress should legislate to limit the availability of strongly encrypted products and services. I represent New America's Open Technology Institute (OTI), where I am Policy Director of the OTI program and also Co-Director of New America's cross-programmatic Cybersecurity Initiative. New America is a nonprofit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences. OTI is New America's program dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open and secure communications networks.

In September, Apple and Google enhanced the security of all smartphone users by modifying the operating system software of iPhones and Android smartphones, respectively, to ensure that the contents of those phones are encrypted by default such that only the user can decrypt them.[1] However, instead of praising those companies for taking a step that would help prevent countless crimes and data breaches, a variety of high-level law enforcement and intelligence officials instead quickly raised concerns that such unbreakable encryption—whether in the context of smartphones or in the context of end-to-end encrypted Internet communications—may pose a challenge to law enforcement and intelligence investigations.[2] Several officials have even gone

[1] Craig Timberg, "Apple will no longer unlock most iPhones, iPads for police, even with search warrants," *The Washington Post*, September 18, 2014, *available at* http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html; Craig Timberg, "Newest Androids will join iPhones in offering default encryption, blocking police," *The Washington Post*, September 18, 2014, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

[2] For a summary of the controversy as it stood in November 2014, along with a bibliography of relevant announcements, speeches, op-eds, analyses and other resources that had been published up to that point, see

so far as to urge Congress to pass legislation to address the issue,[3] presumably by requiring companies to build their systems such that even when their users' data is encrypted, the government can still obtain the plain text of that data when necessary to a lawful investigation. Put more colloquially, they seem to be suggesting that companies build "backdoors" into their encrypted products and services in order to allow surreptitious access by the government.

With all due respect for the many legitimate needs of our law enforcement and intelligence agencies, I am here today to give you ten reasons why Congress should reject any such proposal. First and most obviously…

1. It was already rejected as a policy approach two decades ago, including by Congress. American policymakers were faced with just this issue in the 90s as part of a policy debate often referred to as the "Crypto Wars," where the Clinton Administration battled against privacy advocates and the technology industry on a variety of fronts to limit the spread of strong encryption in order to address law enforcement and intelligence concerns.[4] One conflict was over the U.S. government's attempts to promote so-called "key escrow" technologies—such as the much-maligned "Clipper Chip"[5]—whereby the government or a trusted third party would hold master keys that could decode any encrypted communications. The other conflict was over the U.S. government's attempts to restrict the proliferation of strong encryption products overseas by treating them as munitions subject to export controls. Ultimately, after many years of debate and widespread opposition from the public as well as from Congress, the Administration withdrew its key escrow proposals and relaxed export restrictions on encryption. It did so in response to many of the same arguments that I will make today: that strong encryption is vital to our information security, to our economic security, and to our privacy and free speech, and that attempts to limit

---

Danielle Kehl & Kevin Bankston, "The #CryptoDebate is Coming: Are You Prepared?", *New America's Open Technology Institute,* November 14, 2014, *available at* https://www.newamerica.org/oti/the-cryptodebate-is-coming-are-you-prepared/. For a basic introduction to encryption technology and the role that it plays in our lives, see Danielle Kehl, "Encryption 101," *Slate*, February 24, 2015, *available at* http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html.

[3] Spencer Ackerman, "FBI director attacks tech companies for embracing new modes of encryption," *The Guardian*, October 16, 2014, *available at* http://www.theguardian.com/us-news/2014/oct/16/fbi-director-attacks-tech-companies-encryption; "FBI Director Continues Crusade Against Encryption, Calls on Congress to Act," *The District Sentinel*, March 25, 2015, *available at* https://www.districtsentinel.com/fbi-director-continues-crusade-against-encryption-calls-on-congress-to-act/; Andrew Weissmann, "Apple, Boyd, and Going Dark," *Just Security*, October 20, 2014, *available at* http://justsecurity.org/16592/apple-boyd-dark/; Cyrus Vance Jr., "Apple and Google threaten public safety with default smartphone encryption," *The Washington Post*, September 26, 2014, *available at* http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html ("Absent remedial action by the companies, Congress should act appropriately.").

[4] For a brief but well-documented summary of the Crypto Wars and their lessons for today's policymakers, see Danielle Kehl, Kevin Bankston & Andi Wilson, "Comments to the UN Special Rapporteur on Freedom of Expression and Opinion Regarding the Relationship Between Free Expression and the Use of Encryption," *New America's Open Technology Institute*, February 10, 2015, *available at* https://static.newamerica.org/attachments/1866-oti-urges-un-human-rights-council-to-promote-the-benefits-of-strong-encryption/OTI_Crypto_Comments_UN.pdf. For a more detailed history, see Steven Levy, *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age* (New York: Viking, 2001).

[5] See Steven Levy, "Battle of the Clipper Chip," *The New York Times*, June 12, 1994, *available at* http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

the distribution or use of strong encryption that is free of government backdoors will not only undermine those priorities but will be ineffective and ultimately unnecessary.

The eventual consensus on these points was summed up at the time by Representative Bob Goodlatte, who concluded that "[o]nly by allowing the use of strong encryption, not only domestically but internationally as well, can we hope to make the Internet a safe and secure environment."[6] That consensus was reflected by Congressman Goodlatte's Security and Freedom Through Encryption or "SAFE" Act, a bill that sought to reaffirm Americans' right to distribute and use strong encryption, bar the government from mandating the use of key escrow technologies, and allow for the export of strong encryption.[7] By 1999, that bill was cosponsored by a majority of House members—258 of them, including current members of this oversight committee, Ranking Member Elijah Cummings (D-MD), Rep. John "Jimmy" Duncan Jr. (R-TN), Rep. John Mica (R-FL), and Del. Eleanor Norton (D-DC).[8]

That bill was also in line with the recommendations of the National Academies, which after extensive study issued a 700-plus page report on the policy challenges posed by encryption. Its primary recommendation was:

> **Recommendation 1**—No law should bar the manufacture, sale, or use of any form of encryption within the United States. Specifically, a legislative ban on the use of unescrowed encryption would raise both technical and legal or constitutional issues. Technically, many methods are available to circumvent such a ban; legally, constitutional issues, especially those related to free speech, would be almost certain to arise, issues that are not trivial to resolve.[9]

As Professor Peter Swire, the White House's privacy czar at the time that it announced its newly liberalized encryption export policies, recently summed up the conclusion of the Crypto Wars: "If there is modest harm and enormous gain to be derived from using certain technology, societies should logically adopt that technology. In 1999, the U.S. government concluded that strong encryption was precisely that type of valuable technology—it was worth going at least slightly "dark" in order to reap the many benefits of effective encryption."[10] One of the most obvious benefits of encryption—then as now—is that it ensures the security of the private communications and data of Americans and American companies against all attackers. And if the government were to mandate backdoors into encrypted products and services…

2. It would seriously undermine our nation's cybersecurity, at a time when that security is already in crisis as demonstrated by the endless string of high profile data breaches in the past

---

[6] "Statement of Rep. Bob Goodlatte (R-VA) on re-introduction of the Security and Freedom Through Encryption (SAFE) Act," *The Library of Congress*, February 25, 1999, *available at* http://www.techlawjournal.com/cong106/encrypt/19990225bg.htm.

[7] *See* H.R. 850, 106th Cong. (1999).

[8] *See id.*

[9] Kenneth W. Dam and Herbert S. Lin, Editors, Committee to Study National Cryptography Policy, National Research Council, "Cryptography's Role in Securing the Information Society," *National Academies Press* (1996), *available at* http://www.nap.edu/catalog/5131/cryptographys-role-in-securing-the-information-society.

[10] Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 8 Colum. Sci & Tech. L. Rev. 437 (2013), *available at* http://ssrn.com/abstract=1960602.

year.[11] Every technical expert that has spoken publicly on this controversy since it began last September—both experts from the generation that fought in the original Crypto Wars,[12] as well as experts from the next generation[13]—has concluded that it is impossible to devise a system that provides government access to data on encrypted devices, or to end-to-end encrypted communications, while also ensuring that it remains secure against other attackers, be they computer criminals, industrial spies, Chinese intelligence, or anyone else.[14] Whether you want to call it a front door or a back door, mandating guaranteed government access to encrypted data would open us up to a variety of new cyber-threats. In fact, it would be an open invitation for attackers to focus on hacking into U.S. products and services because they would be easier targets than products and services that are not subject to such mandated vulnerabilities.

As the Chief Information Security Officer of Yahoo put it when debating the issue with the Director of the NSA at New America's cybersecurity conference in February, "all of the best public cryptographers in the world would agree that you can't really build [secure] backdoors in

---

[11] A wide variety of commentators have labeled 2014 "the year of the hack" after an unprecedented string of major security breaches. Arjun Kharpal, "Year of the Hack? A Billion Records Compromised in 2014," *NBC News*, February 12, 2015, *available at* http://www.nbcnews.com/tech/security/year-hack-billion-records-compromised-2014-n305001; Bridget Carey, "2014: Year of the Hack," *CNET Magazine*, December 18, 2014, *available at* http://www.cnet.com/news/2014-the-year-of-the-hack/; Andrew Lumby, "2014: The Year of the Hack," *Fiscal Times*, December 30, 2014, *available at* http://www.thefiscaltimes.com/2014/12/30/2014-Year-Hack; Jennifer LeClaire, "2014: The Year of the Hacker, More to Come in 2015," *CIO Today*, December 31, 2014, *available at* http://www.cio-today.com/article/index.php?story_id=00100015QE3Q.

[12] *See, e.g.*, Jeffrey Vagle and Matt Blaze, "Security 'Front Doors' vs. 'Back Doors': A Distinction Without a Difference," *Just Security*, October 17, 2014, *available at* http://justsecurity.org/16503/security-front-doors-vs-back-doors-distinction-difference/ ("Security engineers, cryptographers, and computer scientists are in almost universal agreement that any technology that provides a government backdoor also carries a significant risk of weakening security in unexpected ways."); Bruce Schneier, "Stop the hysteria over Apple encryption," *CNN.com*, October 31, 2014, *available at* http://www.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/index.html ("You can't build a backdoor that only the good guys can walk through. Encryption protects against cybercriminals, industrial competitors, the Chinese secret police and the FBI. You're either vulnerable to eavesdropping by any of them, or you're secure from eavesdropping from all of them."); Steven M. Bellovin, "Apple's 'Warrant-Proof' Encryption," *SMBlog*, September 23, 2014, *available at* https://www.cs.columbia.edu/~smb/blog/control/ ("[T]he existence of the code to implement [a] back door is itself a danger. Code is often buggy and insecure; the more code a system has, the less likely it is to be secure. This is an argument that has been made many times in this very context, [including in] debates over the Clipper Chip and key escrow in the 1990s…."); Tim Greene, "RSA: Panel calls NSA access to encryption keys a bad idea," *Network World*, April 22, 2015, *available at* http://www.networkworld.com/article/2913280/security0/rsa-panel-calls-nsa-access-to-encryption-keys-a-bad-idea.html (Quoting esteemed cryptologists and Crypto War veterans Ron Rivest, co-founder of RSA, and Whitfield Diffie, one of the inventors of public key cryptography, raising doubts about any new key escrow scheme. "'This is going to be a house of many doors and many parties and it's just not going to work,' Rivest says.").

[13] *See, e.g.*, Matthew Green, "How do we build encryption backdoors?", *A Few Thoughts on Cryptographic Engineering*, April 16, 2015, *available at* http://blog.cryptographyengineering.com/2015/04/how-do-we-build-encryption-backdors.html; Joseph Lorenzo Hall, "The NSA's Split-Key Encryption Proposal is Not Serious," *Center for Democracy & Technology*, April 20, 2015, *available at* https://cdt.org/blog/the-nsas-split-key-encryption-proposal-is-not-serious/.

[14] *See* Schneier, *supra* note12, for a concise summary of known instances of surveillance backdoors being exploited for purposes other than lawful surveillance: "Back-door access built for the good guys is routinely used by the bad guys. In 2005, some unknown group surreptitiously used the lawful-intercept capabilities built into the Greek cell phone system. The same thing happened in Italy in 2006. In 2010, Chinese hackers subverted an intercept system Google had put into Gmail to comply with U.S. government surveillance requests. Back doors in our cell phone system are currently being exploited by the FBI and unknown others."

crypto… That it's like drilling a hole in the windshield."[15] Indeed, when the White House cybersecurity coordinator was asked last week if he could name a single respected technical expert who believed it was possible, he had no answer.[16] Even one of the government's own top experts, the chief cybersecurity adviser to the Commerce Department's National Institute of Standards and Technologies, has publicly concluded that when it comes to designing a secure 'key escrow' system where the government has access to a master decryption key that can't be subverted by other attackers, "[t]here's no way to do this where you don't have unintentional vulnerabilities."[17] Put another way, there is no way to build a "secure golden key" that can only be used by the government, like that which was suggested in a recent *Washington Post* editorial that was immediately and roundly criticized by the Internet community.[18] This fact was conclusively demonstrated in the 90s,[19] and it is equally true today.[20] However, even assuming such a "golden key" system were feasible…

---

[15] Andrea Peterson, "Here's how the clash between the NSA Director and a senior Yahoo executive went down," *The Washington Post*, February 23, 2015, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/23/heres-how-the-clash-between-the-nsa-director-and-a-senior-yahoo-executive-went-down/; *see also* John Reed, "Transcript: NSA Director Mike Rogers vs. Yahoo! on Encryption Back Doors," *Just Security*, February 23, 2014, *available at* http://justsecurity.org/20304/transcript-nsa-director-mike-rogers-vs-yahoo-encryption-doors/.

[16] Joseph Menn, "White House seeks Silicon Valley help on strong yet breakable encryption," *Reuters*, April 21, 2015, *available at* http://www.reuters.com/article/2015/04/21/us-cybersecurity-rsa-encryption-idUSKBN0NC2LT20150421?irpc=932.

[17] Ellen Nakashima and Barton Gellman, "As encryption spreads, U.S. grapples with clash between privacy, security," *The Washington Post*, April 10, 2015, *available at* http://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

[18] *See* Washington Post Editorial Board, "Compromise needed on smartphone encryption," *The Washington Post*, October 3, 2014, *available at* http://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html, *but see, e.g.*, Vagle and Blaze, *supra* note 12 ("The problem with the "golden key" approach is that it just doesn't work."); Jeremy Gillula, "Even a Golden Key Can Be Stolen By Thieves," *Electronic Frontier Foundation*, October 10, 2014, *available at* https://www.eff.org/deeplinks/2014/10/even-golden-key-can-be-stolen-thieves-simple-facts-apples-encryption-decision; Mike Masnick, "Washington Post's Clueless Editorial On Phone Encryption: No Backdoors, But How About A Magical 'Golden Key'?" *Techdirt*, October 6, 2014, *available at* https://www.techdirt.com/articles/20141006/01082128740/washington-posts-braindead-editorial-phone-encryption-no-backdoors-how-about-magical-golden-key.shtml; Julian Sanchez, "What NSA Director Mike Rogers Doesn't Get About Encryption," *Cato Institute*, February 24, 2015, *available at* http://www.cato.org/blog/what-nsa-director-mike-rogers-doesnt-get-about-encryption ("When [FBI Director James] Comey or [NSA Director Michael] Rogers get a ten minute briefing from their experts about the plausibility of designing 'golden' key backdoors, they are probably getting the technically accurate answer that yes, on paper, it is possible.… The trouble… is that real world systems are rarely as tidy as the theories, and the history of cryptography is littered with robust-looking cryptographic algorithms that proved vulnerable under extended scrutiny or were ultimately impossible to implement securely under real-world conditions."). *See also* Video: Surveillance in Cyberspace by Government Actors at the 2015 Idaho Law Review Symposium (Idaho Law Review), *available at* https://vimeo.com/album/3349185/video/124869982 (Professor Ed Felten explaining difficult questions and serious risks associated with key recovery proposals).

[19] The definitive work on this subject from the 90s is a technical report coordinated by the Center for Democracy & Technology and authored by nearly a dozen of the top cryptographers and computer scientists of the era. *See* Hal Abelson *et al*, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," May 27, 1997, *available at* https://www.cdt.org/files/pdfs/paper-key-escrow.pdf.

[20] Several examples from this decade have further demonstrated the security risk of maintaining central databases of encryption keys. *See, e.g.*, Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed," *The New York Times*, June 3, 2011, *available at* http://www.nytimes.com/2011/06/04/technology/04security.html (theft of data about "SecurID" cryptographic tokens from security vendor RSA enabled hackers to breach the network of

3. It would cost the American economy untold billions of dollars. Experts estimated during the original Crypto Wars that building and operating the kind of key escrow infrastructure desired by the government would have cost the government and industry many billions of dollars.[21] Since then, the number of computer and Internet users, and computer and Internet devices, has grown exponentially; so too has the complexity and cost of such a scheme to give the government the universal decryption capability it apparently desires.[22]

That's not even counting the many more billions of dollars that would be lost as consumers worldwide lost confidence in the security of American computing products and online services. American technology companies, which currently dominate the global market, have already been wrestling with diminished consumer trust in the wake of revelations about the scope of the National Security Agency's programs, a loss of trust already predicted to cost our economy billions of dollars.[23] Any new requirement that those companies guarantee that the U.S. government have the technical capability to decrypt their users' data would give foreign users—including major institutional clients such as foreign corporations and governments that especially rely on the security of those products and services—even more incentive to avoid American products and turn to foreign competitors. It would also likely diminish trust in the security of digital technology and the Internet overall, which would slow future growth of the Internet and Internet-enabled commerce and threaten the primary economic engine of the 21st century.

To put it bluntly, foreign customers will not want to buy or use online services, hardware products, software products or any other information systems that have been explicitly designed to facilitate backdoor access for the FBI or the NSA.[24] Nor will many American users, for that

---

Lockheed, the United States' largest defense contractor, and put at risk the security of RSA's 25,000 customers, including Fortune 500 companies and government agencies around the world); Dominic Rushe, "Sim card database hack gave US and UK spies access to billions of cellphones," *The Guardian*, February 19, 2015, *available at* http://www.theguardian.com/us-news/2015/feb/19/nsa-gchq-sim-card-billions-cellphones-hacking (British intelligence agency GCHQ hacked into Gemalto, the world's largest SIM card manufacturer, stealing encryption keys giving it the capability to decrypt telephone and Internet communications made by the billions of cellphones using Gemalto cards).

[21] *See* Abelson et al., *supra* note 19 at 13–16 (describing potentially billions of dollars of direct and indirect costs to "deploy a global key recovery infrastructure").

[22] High costs associated with creating and maintaining such a complex key escrow system - overhead of operating the system; product design and testing costs, which must be rigorous and extensive to assure the highest level of security consistent with key escrow; and costs for all users who are required by law to comply with key escrow requirements. This also includes the potentially irreparable costs to users in the likely event that their communications are compromised. Swire and Ahmad, *supra* note 10.

[23] *See, e.g.*, Danielle Kehl, Kevin Bankston, Robyn Greene, & Robert Morgus, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity* (2014), http://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf; Daniel Castro, Information Technology and Innovation Foundation, *How Much Will PRISM Cost the US Cloud Computing Industry?* (2013), http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry (estimating that the revelations about the NSA's PRISM program could cost the American cloud computing industry $22 to $35 billion over the next three years); James Staten, Forrester Research, *The Cost of PRISM Will Be Larger Than ITIF Projects* (2013), http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects (arguing that ITIF's estimates were low, suggesting that the actual figure could be as high as $180 billion over three years).

[24] Vagle and Blaze, *supra* note 12 ("As Apple, Google, and other similarly situated companies point out, why would customers pay for and use such a system? Companies are now awakening to the fact that, in a post-Snowden world, customers are becoming more savvy about security issues, and will discern between products on this basis.").

matter. Instead, they will turn to more secure products that are available for purchase or for free download from sources outside of the United States, which is a major reason why…

4. It would not succeed at keeping bad actors from using unbreakable encryption. Encryption technology and the ability to create it was already becoming widespread during the original Crypto Wars,[25] and at this point is nearly ubiquitous. And, as was true then, much of that technology is free and open source. For example, there are the open source versions of PGP encryption software that are still the most popular end-to-end email encryption solution, the OpenSSL software library that has long been used to encrypt vast amounts of every-day web traffic, open source disk encryption programs like TrueCrypt, the open source Off-The-Record instant messaging encryption protocol used by a wide variety of IM clients, and the TOR onion routing software originally developed by the Naval Research Laboratory that is now widely used to circumvent oppressive governments' censorship regimes and allow for anonymous online browsing.[26] A government mandate prohibiting U.S. companies from offering products or services with unbreakable encryption is of little use when foreign companies can and will offer more secure products and services, and when an independent coder anywhere on the planet has the resources to create and distribute free tools for encrypting your communications or the data stored on your mobile devices. As former Homeland Security Secretary Michael Chertoff recently put it, "[T]hat genie is not going back in the bottle."[27]

The result is that a U.S. government-mandated backdoor into the encrypted products and services of U.S. companies, while undermining the information security of millions of ordinary Americans and the economic security of the American tech industry, would do little to prevent bad actors from taking advantage of strong encryption. Or, as PGP's inventor Phil Zimmerman famously said in the 90s: "If privacy is outlawed, only outlaws will have privacy."[28] Not only is such a mandate likely to be ineffective, but also…

5. It's unnecessary in order to keep us safe from criminals—but strong encryption is. So far, the opponents of strong device encryption have failed to offer any compelling examples where such encryption seriously hindered a criminal investigation or prosecution. FBI Director Comey did offer, in his October speech on the subject, four examples of cases where cellphone-derived evidence was supposedly critical to a solving a crime, but those examples were quickly debunked by the press.[29] During the same event, Director Comey came up empty when asked for

---

[25] A comprehensive report from the Cyberspace Policy Institute at George Washington University in June 1999 noted that there were over 500 foreign companies manufacturing or distributing foreign cryptographic products in nearly 70 countries outside the United States. Lance J. Hoffman et al., "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations," Cyberspace Policy Institute at the George Washington School of Engineering and Applied Science, June 10, 1999, *available at* http://cryptome.org/cpi-survey.htm

[26] *See* The OpenPGP Alliance at http://www.openpgp.org/, the OpenSSL Project at https://www.openssl.org/, TrueCrypt (once popular but now discontinued due to security concerns) at http://truecrypt.sourceforge.net/, Off-The-Record Messaging at https://otr.cypherpunks.ca/, and the Tor Project at https://www.torproject.org/.

[27] Jason Koebler, "The Man Who Crafted the Patriot Act Now Supports Your Right to Encrypt Data," *Motherboard*, February 27, 2015, *available at* http://motherboard.vice.com/read/the-man-who-crafted-the-patriot-act-now-supports-your-right-to-encrypt-data.

[28] Philip Zimmerman, "Why I wrote PGP," June 1991, *available at* https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

[29] *See* Dan Froomkin and Natasha Vargas-Cooper, "The FBI Director's Evidence Against Encryption is Pathetic," *The Intercept*, October 17, 2014, *available at* https://firstlook.org/theintercept/2014/10/17/draft-two-cases-cited-fbi-dude-dumb-dumb/ ("In the three cases *The Intercept* was able to examine, cell-phone evidence had nothing to do

a real-world example where encryption actually stymied an investigation.[30] And in March he admitted to the House Appropriations Committee in March that he wasn't in a position to offer "a percentage or number" of cases affected by encrypted devices.[31] Meanwhile, in the realm of law enforcement wiretaps of phone and Internet communications, where numbers are available via annual reports by the Administrative Office of the U.S. Courts, the number of cases where encryption has posed a problem is miniscule. Specifically, according to the report issued in 2014, of the over 3,576 wiretaps conducted by federal and state law enforcement in 2013, encryption was encountered in only 41 cases, and the police were able to obtain the plain text of the encrypted communications in 32 of those 41 cases. [32] So, strong encryption posed a problem in only nine of 3,500 wiretaps, and that was a record high.

Indeed, rather than "going dark," there's good reason to believe that thanks to the growing role played by digital technology in nearly all aspects of our lives—and especially thanks to the prevalence of smartphones—law enforcement is in the midst of a "golden age of surveillance" where they can access more data about what we say, where we go, what we do, and with whom we associate and communicate than ever before.[33] Indeed, as a number of law enforcement and intelligence officials have acknowledged, metadata about private communications can be just as revealing if not more revealing than the contents of those messages themselves.[34] This golden

---

with the identification or capture of the culprits, and encryption would not remotely have been a factor."); Jack Gillum and Eric Tucker, "Do FBI's Examples Support Encryption Worries?", *Associated Press*, October 17, 2014, *available at* http://bigstory.ap.org/article/e03177df2c9a4e0ebe5b584c909218bf/do-cases-fbi-cites-support-encryption-worries (noting that although in one case, text messages on a phone helped secure a plea deal, "three other examples the FBI director has cited are not so cut and dry. They are cases in which the authorities were tipped off — or even solved the crime — through means other than examining data they took from victims or suspects."). Another example offered in an op-ed by a former FBI official, of a case where encryption would have purportedly prevented the rescue of a kidnapping victim, had to be corrected when it proved to be false. *See* Ronald T. Hosko, "Apple and Google's new encryption rules will make law enforcement's job much harder," *The Washington Post*, September 23, 2014, *available at* http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/ ("Editors note: This story incorrectly stated that Apple and Google's new encryption rules would have hindered law enforcement's ability to rescue the kidnap victim in Wake Forest, N.C. This is not the case. The piece has been corrected.").

[30] *See* C-SPAN, "Comey Flustered When Asked For Actual Real-Live Examples," October 16, 2014, *available at* http://www.c-span.org/video/?c4511673/comey-flustered-asked-actual-real-live-examples.

[31] "FBI Director Continues Crusade Against Encryption, Calls on Congress to Act," *The District Sentinel*, March 25, 2015, *available at* https://www.districtsentinel.com/fbi-director-continues-crusade-against-encryption-calls-on-congress-to-act/.

[32] *See* The Adminstrative Office of the U.S. Courts, "Wiretap Report 2013," *available at* http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx#sa9; *see also* Andy Greenberg, "Rising Use of Encryption Foiled the Cops a Record 9 Times in 2013," *Wired*, July 2, 2014, *available at* http://www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013/ ("So the cryptapocalypse they warned us about in the 90's has come to pass, University of Pennsylvania computer science professor Matt Blaze noted drily on twitter. 'Strong crypto used in a whopping 0.25% of wiretaps last year.'").

[33] "Consider three areas where law enforcement has far greater capabilities than ever before: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create 'digital dossiers' about individuals' lives." Peter Swire, "'Going Dark' Versus a 'Golden Age for Surveillance," *Center for Democracy & Technology*, November 28, 2011, *available at* https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/; *see also* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. 335 (2014), *available at* http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones (describing the rapidly declining cost of location tracking by law enforcement).

[34] As former NSA general counsel Stewart Baker put it, "Metadata absolutely tells you everything about somebody's life.... If you have enough metadata you don't really need content.... [It's] sort of embarrassing how predictable we

age of surveillance promises to get even brighter for law enforcement with the rise of the so-called "Internet of Things", where fine-grained data about everything from our electricity consumption to the contents of our refrigerators to the behavior of our medical implants will be available to prosecutors.[35]

Meanwhile, much of the data stored on the encrypted Apple and Android cellphones that have caused so much concern are also backed up to Apple and Google servers in the Internet "cloud" and available via legal process served on those companies.[36] That which is not available via the cloud will in many cases be obtainable simply by having a court compel the suspect to hand over the data or else face jail time for contempt.[37] And for cases where notice to the suspect is not desirable, encrypted data or communications that cannot be obtained from the cloud might even be obtained by government investigators secretly hacking into suspects' devices from afar over the Internet, a law enforcement technique that is worrisomely on the rise despite constitutional concerns.[38]

With few examples of encryption posing a serious challenge for law enforcement, and a wide variety of other ways for law enforcement to obtain a wide variety of information from or about suspects, the necessity of encryption backdoors to better combat crime is unclear at best. What is absolutely clear, however, is a fact that Representative Bob Goodlatte attested to back in 1997:

> Strong encryption *prevents* crime. Just as dead-bolt locks and alarm systems help people protect their homes against intruders, thereby assisting law enforcement in preventing crime, strong encryption allows people to protect their digital communications and computer systems against criminal hackers and computer thieves. The blue-ribbon National Research Council said it best, concluding that strong encryption supports both law enforcement efforts and our national security, while protecting the proprietary information of U.S. businesses.[39]

---

are as human beings." Alan Rusbridger, "The Snowden Leaks and the Public," *New York Review of Books*, November 21, 2013, *available at* http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/. Former NSA director Michael Hayden agrees: "[Baker's comment was] absolutely correct… We kill people based on metadata." David Cole, "We Kill People Based on Metadata," *New York Review of Books*, May 10, 2014, *available at* http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/.

[35] Bruce Schneier, "Will giving the Internet eyes and ears mean the end of privacy?" *The Guardian*, May 16, 2013, *available at* http://www.theguardian.com/technology/2013/may/16/internet-of-things-privacy-google; Mike Wheatley, "Big Brother's Big Data: Why We Must Fear the Internet of Things," *Silicon Angle*, January 10, 2013, *available at* http://siliconangle.com/blog/2013/01/10/big-brothers-big-data-why-we-must-fear-the-internet-of-things/.

[36] Micah Lee, "Apple Still Has Plenty of Your Data for the Feds," *The Intercept*, February 22, 2014, *available at* https://firstlook.org/theintercept/2014/09/22/apple-data/.

[37] Andy Greenberg, "Google and Apple Won't Unlock Your Phone, But a Court Can Make You Do It," *Wired*, September 22, 2014, *available at* http://www.wired.com/2014/09/google-apple-wont-unlock-phone-court-can-make/.

[38] Fed. Jud. Center, *Public Hearing on Proposed Amendments to the Federal Rules of Criminal Procedure* 34–40 (Nov. 5, 2014) (testimony of Kevin S. Bankston), available at http://www.newamerica.org/downloads/OTI_Rule_41_Testimony_11-05-14_final.pdf (summarizing constitutional concerns).

[39] Bob Goodlatte, "Let's Open Up Encryption," *The Washington Post*, June 12, 1997, *available at* http://www.washingtonpost.com/wp-srv/politics/special/encryption/stories/ocr061297.htm (emphasis added), citing Dam and Lin, *supra* note 9.

It is even more true now than it was nearly twenty years ago: encryption makes us all safer,[40] and default encryption on smartphones especially so. There is a growing epidemic of smartphone theft, with 3.1 million stolen in the U.S. in 2013, nearly double the number of smartphones stolen in 2012.[41] The vast amount of personal information on those devices makes them especially attractive targets for criminals aiming to commit identify theft or other crimes of fraud, or even to commit violent crimes or further acts of theft against the phone's owner.Yet over a third of consumers fail to activate even the simplest security mechanisms on their mobile devices.[42] That is why the FBI itself used to advise consumers with smartphones to turn their encryption on—until abruptly changing course and deleting that advice from its website last month.[43] By taking this step for their customers and turning on encryption by default, mobile operating system vendors have completely eliminated the risk of those crimes occurring, significantly discouraged thieves from bothering to steal smartphones in the first place, and ensured that those phones' contents will remain secure even if they are stolen. A necessary consequence, of course, is that the contents will also remain secure if the phone is seized by law enforcement.

6. It would undermine and turn on its head the Fourth Amendment right to be secure in our papers and effects.

The Fourth Amendment gives individuals the right to be secure in their papers and effects, prohibiting unreasonable searches and seizures and requiring that any warrant authorizing such a government invasion be issued by a court based on a showing of probable cause.[44] As indicated by recent Supreme Court cases, the need for vigorous enforcement of that right has become even more acute in the context of powerful digital technologies. Most recently, a unanimous Supreme Court in the case of *Riley v. California* decided to require warrants for the search of a cellphone in the possession of an arrestee, based on the unprecedented amount of private data that may be stored on such devices even though such searches incident to arrest have traditionally been allowed without a warrant.[45] As the Court explained, many cell phones "are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries,

[40] Nuala O'Connor, "Encryption Makes Us All Safer" *Center for Democracy & Technology*, October 8, 2014, *available at* https://cdt.org/blog/encryption-makes-us-all-safer/.

[41] "Smart phone thefts rose to 3.1 million last year, Consumer Reports finds," *ConsumerReports.org*, May 28, 2014, *available at* http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

[42] *Id.*

[43] The FBI previously included the following recommendation in a consumer safety guide on its website: "Depending on the type of phone, the operating system may have encryption available. This can be used to protect the user's personal data in the case of loss or theft." *See* Mike Masnick, "FBI Quietly Removes Recommendation To Encrypt Your Phone... As FBI Director Warns How Encryption Will Lead To Tears," Techdirt, March 26, 2015, *available at* https://www.techdirt.com/articles/20150325/17430330432/fbi-quietly-removes-recommendation-to-encrypt-your-phone-as-fbi-director-warns-how-encryption-will-lead-to-tears.shtml. However, the same advice is still available via a separate FBI press release, "Smartphone Users Should be Aware of Malware Targeting Mobile Devices and the Safety Measures to Help Avoid Compromise," October 22, 2012, *available at* http://www.fbi.gov/sandiego/press-releases/2012/smartphone-users-should-be-aware-of-malware-targeting-mobile-devices-and-the-safety-measures-to-help-avoid-compromise.

[44] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

[45] *Riley v. California*, 134 S. Ct. 2473, 2485 (U.S. 2014).

albums, televisions, maps, or newspapers."[46] These devices, with "immense storage capacity," can hold "every picture [their users] have taken, or every book or article they have read," and "even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on."[47] Ultimately, as the Supreme Court explicitly held, the search of a modern electronic device such as a smartphone or a computer is more privacy invasive than even "the most exhaustive search of a house."[48]

As the Court concluded in *Riley*, "We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost."[49] The court did not pretend that requiring warrants for searches of cellphones seized incident to arrest did not risk diminishing law enforcement's effectiveness—it simply recognized that allowing such warrantless searches posed an even greater risk to our Fourth Amendment rights considering the scope of data available on those phones. The court made a similar calculus in the 2012 case of *U.S. v. Jones* when it decided that the comprehensive long-term tracking of a car's movements on public roads using GPS technology constituted a search under the Fourth Amendment, even though tracking that only reveals information that would have been visible from public space would not traditionally be considered to violate a suspect's Fourth Amendment-based reasonable expectation of privacy.[50] Both the *Jones* and *Riley* cases can be viewed as the Court's attempt to compensate for the sharp increase in the government's surveillance capabilities thanks to digital technology by ratcheting up legal protections against government searches.[51] The use of encryption on cellphones can be seen as a similar means of compensating for the government's newfound technical powers during this "golden age of surveillance," using technology instead of the law to help restore the balance between government power and individual power to something closer to what the Founding Fathers intended.

Encryption opponents would push in the other direction and flip our Fourth Amendment rights on their head by instead casting the Fourth Amendment as a right of the government—a right to dictate that the contours of the physical and digital worlds be redesigned to facilitate even easier surveillance.[52] But there is no precedent for such a reading of the Fourth Amendment. As former computer crime prosecutor Marc Zwillinger recently put it,

---

[46] *Id.* at 2489.
[47] *Id.*
[48] *Id.* at 2491.
[49] *Id.* at 2493.
[50] See *United States v. Jones*, 132 S. Ct. 945, 955-57 (2012) (Sotomayor, J., concurring), 957-963 (Alito, J., Ginsburg, J., Breyer, J., and Kagan, J., concurring).
[51] *See generally* Bankston & Soltani, *supra* note 33.
[52] James Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *Remarks at the Brookings Institution*, October 16, 2014, *available at* http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (*e.g.*, encryption is "the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?"); Vance, *supra* note 3 (Vance, the Manhattan District Attorney, describing how Apple and Google's new features "push mobile devices beyond the reach of warrants and thus beyond the reach of government law enforcement. This would make mobile devices different from everything else. Even bank security boxes — the "gold standard" of the pre-digital age — have always been searchable pursuant to a judicial warrant.").

> I don't believe that law enforcement has an absolute right to gain access to every way in which two people may choose to communicate… And I don't think our Founding Fathers would think so, either. The fact that the Constitution offers a process for obtaining a search warrant where there is probable cause is not support for the notion that it should be illegal to make an unbreakable lock. These are two distinct concepts.[53]

Zwillinger's comments echoed those made by Senator John Ashcroft during the original Crypto Wars: "There is a concern that the Internet could be used to commit crimes and that advanced encryption could disguise such activity. However, we do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant government the Orwellian capability to listen at will and in real time to our communications across the Web?"[54] Or, as a more recent commentator put it:

> This argument [that encryption foils the police's right to obtain evidence with a search warrant] misunderstands the role of the search warrant. A search warrant allows police, with a judge's approval, to do something they're not normally allowed to do. It's an instrument of permission, not compulsion. If the cops get a warrant to search your house, you're obliged to do nothing except stay out of their way. You're not compelled to dump your underwear drawers onto your dining room table and slash open your mattress for them. And you're not placing yourself 'above the law' if you have a steel-reinforced door that doesn't yield to a battering ram.[55]

The law has never prohibited the creation of unbreakable locks, nor required us to hand our keys over to the government just in case it might need them for an investigation, whether those keys are physical or digital. Indeed, the Founders themselves used ciphers to communicate with each other,[56] and presumably would have viewed a demand that they hand over the key to their encryption scheme as abhorrent to their rights—not only their Fourth Amendment right against government intrusion but also their First Amendment right to speak and associate both freely and anonymously.

7. It would threaten First Amendment rights here and free expression around the world.

Repeated court challenges to export controls on encryption during the Crypto Wars illustrate how any attempt by the government to limit the distribution of encryption software code, which is itself speech, would raise serious First Amendment concerns. As one federal district court held when considering a First Amendment challenge to 90s-era encryption export controls,

---

[53] *See* Nakashima and Gellman, *supra* note 17.

[54] John Ashcroft, *Keep Big Brother's Hands Off the Internet* (1997), *available at* http://rense.com/general31/keepbigbrothershands.htm.

[55] Kevin Poulsen, "Apple's iPhone Encryption is a Godsend, Even if Cops Hate It," *Wired*, October 8, 2014, *available at* http://www.wired.com/2014/10/golden-key/.

[56] *See* "Thomas Jefferson Used Encryption," *Laissez Faire*, September 1, 2012, *available at* https://lfb.org/thomas-jefferson-used-encryption/ (describing how James Madison, Thomas Jefferson and James Monroe correspondence in code to protect against the U.S. government reading their letters). The Jefferson's Wheel Cipher remained immune from attacks for over 150 years, gaining Thomas Jefferson the title "Founder of American Cryptography." Alexander Stanoyevitch, *Introduction to Cryptography with Mathematical Foundations and Computer Implementations* 107 (2010).

> This court can find no meaningful difference between computer language…and German or French. All participate in a complex system of understood meanings within specific communities {in this case, that of programmers and mathematicians}.... Contrary to defendants' suggestion, the functionality of language does not make it any less like speech.... Instructions, do-it-yourself manuals, recipes, even technical information about hydrogen bomb construction, are often purely functional; they are also speech.[57]

The Ninth Circuit Court of Appeals agreed, holding that the challenged encryption export regulations constituted a prior restraint on speech that offends the First Amendment. [58] Therefore, not only would attempting to police the distribution of strong encryption code inside the United States require an endless and ineffective game of Internet whack-a-mole as old and new encryption code proliferated across cyberspace, but the extensive censorship that would be necessary to fight that losing battle would also likely violate the freedom of speech. Similarly, a legal regime that forced individuals to cede their private encryption keys to the government or to their communications providers for law enforcement purposes would also raise novel issues of compelled speech under the First Amendment.

However, the free speech impact of a mandate against unbreakable encryption and in favor of backdoors for government would reach far beyond just the communication of encryption code, and chill a wide variety of online expression. When individuals believe that they may be under surveillance, there is a "chilling effect" that can curb free speech and the free flow of information online.[59] If individuals must assume that their online communications are not secure but may instead be acquired by the U.S. government or by anyone else who might exploit an encryption backdoor, they will be much less willing to communicate freely. By contrast, encouraging the availability of strong encryption free of surveillance backdoors can enable free expression both in the United States and around the world,[60] including by stymieing the censorship and surveillance efforts of governments with less respect for human rights than our own.

8. It would encourage countries with poor human rights records to demand backdoor access of their own.

The governments of countries like China, [61] India, [62] and the United Arab Emirates[63] have proposed a variety of measures that would require companies to implement key escrow systems

---

[57] *Bernstein v. U.S. Dept. of State*, 922 F.Supp 1426, 1431 (N.D. Cal. 1996).

[58] *See Bernstein v. United States Dept. of Justice*, 176 F.3d 1132 (9th Cir. 1999).

[59] A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Penn. L. Rev. 709, 815-822 (1995) (discussing "Chilling Effect on Speech" and "Anonymity and the Freedom of Association"); Human Rights Watch & The American Civil Liberties Union, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy* (2014), *available at* https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.

[60] *See* Kehl et al., *supra* note 4.

[61] In February 2015, China put forth a proposal that would require tech companies operating in the country — including American companies — to provide them with copies of encryption keys and other means to defeat security measures. The United States government sent a letter objecting to the measure, and U.S. Trade Representative Michael Froman said that "[t]he Administration is aggressively working to have China walk back from these troubling regulations." Quoted in Lorenzo Franceschi-Bicchierai, "The United States Is Angry That China Wants Crypto Backdoors, Too," *Motherboard*, February 27, 2015, *available at* http://motherboard.vice.com/read/the-united-states-is-angry-that-china-wants-crypto-backdoors-too.

or other forms of backdoors or stop doing business in those countries, proposals that the United States government has criticized.[64] Yet how can the United States credibly criticize, for example, the Chinese government for proposing an anti-terrorism bill that would require U.S. companies to hand over their encryption keys, if we impose a similar requirement here at home? And how are U.S. companies to argue that they cannot implement such requirements and hand over the keys to foreign governments—even those with a history of human rights abuses—if they have already had to do so for the U.S. government?

As Marc Zwillinger has pointed out, if the U.S. mandates backdoor access to encrypted data, "multinational companies will not be able to refuse foreign governments that demand [the same] access. Governments could threaten financial sanctions, asset seizures, imprisonment of employees and prohibition against a company's services in their countries. Consider China, where U.S. companies must comply with government demands in order to do business."[65] Such a result would be particularly ironic considering the U.S.'s foreign policy goal of promoting Internet Freedom worldwide and in China especially, including the promotion of encryption-based tools to protect privacy and evade censorship.[66]

Internet Freedom begins at home, and a failure by the United States to protect Americans' ability to encrypt their data will undermine the right to encrypt and therefore human rights around the world.[67] The U.S. government supports the use of strong encryption abroad as part of our foreign policy objectives, and it should support the same for Americans here in the United States. This is especially true considering that…

---

[62] Anandita Singh Mankotia, "Government, BlackBerry dispute ends," *Times of India*, July 10, 2013, http://timesofindia.indiatimes.com/tech/tech-news/telecom/Government-BlackBerry-dispute-ends/articleshow/20998679.cms.

[63] In 2010, United Arab Emirates, citing encryption concerns, threatened to suspend Blackberry mobile services (including email and text messaging) because of the strong encryption Blackberry used. (Barry Meier and Robert F. Worth, "Emirates to Cut Data Services of BlackBerry," *The New York Times*, August 1, 2010, *available at* http://www.nytimes.com/2010/08/02/business/global/02berry.html.)

[64] *See, e.g.*, Jeff Mason, "Exclusive: Obama sharply criticizes China's plans for new technology rules," *Reuters*, March 2, 2015, *available at* http://www.reuters.com/article/2015/03/02/us-usa-obama-china-idUSKBN0LY2H520150302 (Says President Obama, "Those kinds of restrictive practices I think would ironically hurt the Chinese economy over the long term because I don't think there is any U.S. or European firm, any international firm, that could credibly get away with that wholesale turning over of data, personal data, over to a government.").

[65] *See* Marc Zwillinger, "Should Law Enforcement Have the Ability to Access Encrypted Communications? NO: It Violates Our Rights—Without Improving Security," *The Wall Street Journal*, April 19, 2015, *available at* http://www.wsj.com/article_email/should-law-enforcement-have-the-ability-to-access-encrypted-communications-1429499474-lMyQjAxMTE1NjI5MDMyMzA2Wj.

[66] Since 2009, the American government has invested over $125 million in programs to support Internet Freedom abroad, including "work to support counter-censorship and secure communications technology," much of which relies on encryption. Scott Busby, "10 Things You Need to Know About U.S. Support for Internet Freedom," *IIP Digital*, May 29, 2014, *available at* http://iipdigital.usembassy.gov/st/english/article/2014/05/20140530300596.html#axzz32vEtH3C9.

[67] Cynthia Wong, "Global Internet Freedom Begins at Home," *Index on Censorship*, June 21, 2011, *available at* https://www.indexoncensorship.org/2011/06/global-internet-freedom-begins-at-home/. ("As the US government debates emerging internet policy challenges, it must face an inconvenient truth: the US is often viewed as the standard bearer for many (though not all) aspects of internet regulation and its laws can and will have an effect far beyond American borders.")

9. An overwhelming majority of the House of Representatives and the President's own hand-picked advisors have already rejected the idea.

Echoing the House's overwhelming support for the SAFE Act during the Crypto Wars of the 90s, an overwhelming and bipartisan majority of the House of Representatives already rejected the idea of encryption backdoors just last year.[68] That's when, by a vote of 293 to 123,[69] the House approved the Sensenbrenner-Massie-Lofgren amendment to the Defense Appropriations Act, H.R. 4870. That amendment, responding to reports of that the NSA had worked to insert surveillance backdoors into a variety of hardware and software products, would have prohibited the NSA or the CIA from using any funds "to mandate or request that a person…alter its product or service to permit the electronic surveillance…of any user of said product or service for said agencies."[70] Although the amendment, which was supported by a quickly organized activist campaign[71] and a broad coalition of Internet companies and civil society organizations like Google and the American Civil Liberties Union,[72] did not make it into the final "CRomnibus" spending bill,[73] it was still a potent indicator that Congress is skeptical of U.S. government efforts that would weaken the security of American hardware and software products.

Equally skeptical of encryption backdoors were the five experts hand-picked by the President to review the NSA's surveillance activities. Echoing the conclusions of the National Academies in their groundbreaking study from 1997, the final report of the President's Review Group on Intelligence and Communications Technologies included this strongly worded recommendation prompted by its conclusion that strong encryption was necessary to the United States' national and economic security:

> **Recommendation 29**
> We recommend that, regarding encryption, the US Government should:
> (1) fully support and not undermine efforts to create encryption standards;
> (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and
> (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage.[74]

---

[68] Ellen Nakashima and Andrea Peterson, "House votes to curb NSA "backdoor" U.S. data searches," *The Washington Post*, June 20, 2014, *available at* http://www.washingtonpost.com/world/national-security/house-votes-to-curb-nsa-backdoor-us-data-searches/2014/06/20/54aacd28-f882-11e3-a3a5-42be35962a52_story.html

[69] The final vote count is *available at* http://clerk.house.gov/evs/2014/roll327.xml.

[70] Text of the amendment is *available at* https://www.eff.org/document/sensenbrenner-massie-lofgren-amendment-2014.

[71] *See* "Shut the NSA's Backdoor to the Internet," *available at* https://shutthebackdoor.net/.

[72] *See* "OTI Joins With Privacy Groups and Tech Companies To Tell Congress: End the NSA's Backdoor Access to Internet Users' Data," *New America's Open Technology Institute*, June 18, 2014, *available at* http://newamerica.net/node/114440.

[73] Sean Vitka, "This Meaningful Surveillance Reform Had Bipartisan Support. It Failed Anyway." *Slate*, December 10, 2014, *available at* http://www.slate.com/blogs/future_tense/2014/12/10/massie_lofgren_surveillance_reform_amendment_fails_despite_bipartisan_support.html.

[74] "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," December 12, 2013, at p. 36, *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Therefore, not only the House of Representatives but a blue-ribbon panel of experts including a former CIA Director and the White House's former anti-terrorism czar, have already concluded: mandating or even requesting the insertion of encryption backdoors into U.S. companies' products and services is a bad idea. As demonstrated by their support for the Sensenbrenner-Massie-Lofgren amendment, the Internet industry and the Internet activists agree, which is why…

10. It would be vigorously opposed by a unified Internet community.

Decades before the massive online advocacy campaign that stopped the SOPA and PIPA copyright bills in 2012,[75] The Crypto Wars—and, in particular, the battle against the Clipper Chip—represented the Internet community's first major political engagement. And it was a rousing success. An unprecedented alliance of Internet users, technologists, academics, the technology industry, and newly-emerging Internet rights advocacy organizations like the Electronic Frontier Foundation, the Center for Democracy and Technology, and the Electronic Privacy Information Center, flexed its muscles for the first time and made a huge difference in the political process. They organized experts to speak on panels, testified before Congress, and circulated electronic petitions, including one that got over 50,000 signatures — an extraordinary number in the early days of Internet activism.[76] That Internet community, which won the first Crypto Wars two decades ago and more recently blocked SOPA and PIPA, has only grown larger and more vocal in the intervening years, and will certainly make its voice heard if another round of Crypto Wars were to begin now.

That conflict can be avoided, however. Especially considering all of the above arguments, many of which are just as true if not moreso than they were twenty years ago, Congress can and should leave the idea of encryption backdoors in the dustbin of history where it belongs. Instead, policymakers should heed the lessons of the past and the advice of the President's Review Group by considering policies that will promote rather than undermine the widespread use of strong encryption and thereby help guarantee a more secure and prosperous future for America.

Thank you, and I welcome your questions on this important matter.

---

[75] For an in-depth discussion of the online organizing efforts and coordinated protest efforts that stopped the Stop Online Piracy Act (SOPA) and PROTECT IP Act (PIPA) in 2012, see Marvin Ammori, *On Internet Freedom* (Elkat Books: January 15, 2013), *available at* http://shop.fightforthefuture.org/products/on-internet-freedom-by-marvin-ammori.

[76] Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip* 34 (1997).

Mr. HURD. Thank you, Mr. Bankston.
Mr. Potter, 5 minutes.

STATEMENT OF JON POTTER

Mr. POTTER. Thank you, Chairman Hurd, Ranking Member Kelly, members of the subcommittee.

The 3-year-old App Developers Alliance includes more than 200 companies and more than 35,000 individuals worldwide. Thank you for inviting me to speak today about the challenges app developers and our digital industry partners face if we are required to both protect privacy and provide Government with privacy-breaching back doors.

First, it is important to highlight that protecting digital data through innovative security-based products is unquestionably good for businesses and consumers. In contrast, back doors make apps less secure and less trustworthy.

Second, we must remember that data protection is not only about civil liberties and privacy. Encryption prevents cybercrime, which threatens fundamental economic interests that operate digitally, including health care, transportation, banking, and manufacturing. Encryption also prevents identity theft, which has been consumers' top complaint to the Federal Trade Commission for 15 consecutive years.

Third, nearly every digital business wants to be global, but mandatory government back doors may spark a trade war and imprison businesses in their home country.

Fourth, Government's conflicting messages about data protection create uncertainty about business expectations. Uncertainty creates risk, inhibits growth and job creation, and especially harms startups and small business. Handling customer data securely is an essential business commitment. Customers worldwide demand this.

The media routinely report on data breaches and organized cybercrime. In response, and strongly encouraged by government agencies, including the FBI, developers have prioritized security.

Given the magnitude of cybercrime and of government resources committed to fighting it, law enforcement criticism of encryption is perplexing. For several years law enforcement has routinely encouraged and even required encryption to protect sensitive data.

Until recently, the FBI Web site recommended all organizations, quote, "encrypt data so the hacker can't read it," end quote. Quizzically, that recommendation was deleted from the FBI Web site just a few weeks ago. In contrast, the Federal Trade Commission continues to advise that, quote, "encryption is the key to securing personal information online."

Government mixed messages about privacy and security, slow product development, inhibit investors, worry customers, and harm all companies, especially startups. Every digital business opportunity is global. So the worldwide impact of mandatory government back doors is important. Unauthorized U.S. Government collection of global communications has created international outrage and backlash that is already costing American companies billions of dollars.

Mandating back doors that weaken encryption will exacerbate global distrust, and we should expect two reactions. First, international governments will demand their own security back doors. Second, U.S.-based apps will be deemed noncompliant with international privacy laws and be locked out of those markets.

Developers will have to build many versions of apps to serve many markets with different law enforcement demands and privacy laws or risk being blocked from those markets. Building multiple versions of any product increases costs and runs contrary to every rule of digital business.

Additionally, for good reason, some might be concerned if other countries or particular countries demand their own back doors. If markets become inaccessible to U.S. Apps because of mandatory back doors, then a digital trade war could break out.

The App Developers Alliance membership is global because apps create jobs and deliver value globally. Closed markets may benefit some of our members in the short term, but the large majority of our members recognize that encryption and privacy trade war is substantially negative.

Finally, the basics of technology, security, and privacy are critical. Any security opening creates vulnerability. You can't build a back door that only the good guys can walk through. Hackers know it. The FBI knows it. And increasingly customers know it.

Forced insecurity harms consumers in all industries, but it especially harms startups and small innovators because building back doors that are only slightly ajar is technically challenging and very expensive.

There are situations that justify law enforcement access to our cell phones, to our apps, to the cloud, but there are many legal methods to accomplish this with court approval. Congress must insist that law enforcement and national security agencies utilize these processes. This is fundamental to America's civilian government.

In closing, please remember that encryption technologies are a market response to well-founded consumer, commercial, and government demand. When an app developer builds a thriving business model around security and consumer trust only to be told the FBI wants the product to be secure, but not too secure, this disrupts the marketplace. It is bad for innovation, for business, and for consumers. Thank you.

[Prepared statement of Mr. Potter follows:]

Data Protection, Law Enforcement and the Global Digital Economy

Testimony of Jon Potter
President, Application Developers Alliance

U.S. House of Representatives
Subcommittee on Information Technology
Committee on Government Oversight and Reform
Hearing on "Encryption Technology and Possible U.S. Policy Responses"

April 29, 2015

Chairman Hurd, Ranking Member Kelly and Members of the Subcommittee:

Consumers want their personal data protected and businesses want their confidential data protected. Cyberhackers and data thieves are a constant threat. For several years law enforcement and consumer protection officials have encouraged the data protection marketplace and used enforcement tools to insist and demand that consumer data be protected. And responding appropriately to marketplace and government forces, app developers and our digital industry partners regularly provide and promote encryption tools to ensure that consumers' personal information and private communications remain private.

Thank you for inviting me to share with you today the challenges that app developers and our digital industry partners will face if we try to both protect privacy *and* provide privacy-breaching back doors to the government. Others will testify about the technological impossibility of this task. I will speak to the resulting legal and investment uncertainty, consumer mistrust, and business turbulence. And when this hearing and the longer debate concludes, I urge Congress to remain committed to protecting Americans' privacy, empowering encryption solutions that can eradicate cyberhacking and data theft, and upholding traditional American values that require law enforcement to abide by the Constitution.

The Application Developers Alliance (the "Alliance") was founded in January 2012 to support app developers as entrepreneurs, innovators, and creators. Alliance membership includes more than 200 companies and an additional 36,000 individuals.

On behalf of the app industry and our innovative, entrepreneurial members, I ask you to consider the following:

1. The Federal Trade Commission (FTC), State Attorneys General, the FBI, privacy advocates and consumers are correct: protecting data while using it to build exciting new products and services is unquestionably good for businesses and consumers. The entire app ecosystem is committed to both data innovation and data protection.
2. By challenging the use of encryption and sending a conflicting message about data protection, law enforcement is introducing doubt about what is expected or perhaps required of app developers and digital businesses. This creates uncertainty for all, but especially for risk-averse, resource-constrained startups and small innovators. Investors and customers often flee from uncertainty, and though talented app developers can code virtually anything, they should not have to choose between conflicting government demands – particularly of the gravity of privacy and data security.
3. The app marketplace is international and nearly every app wants to be global. If apps are required to provide back doors to the U.S. government, then many other governments will require their own access key or their own back doors, and still other governments will cite these back doors as evidence of non-compliance with their national privacy laws. Instead of enjoying global digital opportunities, apps will be buffeted by conflicting laws that force unpleasant choices while imposing financial and legal risk. App developers and their customers will have to choose between compliance and market access.
4. Privacy-breaching back doors make apps inherently less secure and less trustworthy. By providing access to one or more governments, the developer is creating a vulnerability that can be exploited by hackers and thieves.
5. For 15 consecutive years, identity theft has been the #1 consumer complaint to the FTC. Data protection prevents cybercrime and identity theft, and encryption is the best data protection tool we know. Encryption proponents are not simply favoring privacy and civil liberties, we also favor crime prevention – the essential result of strong data protection.

Today's Privacy vs. Law Enforcement Debate is Not New, But It Is Different

Like many policy debates spawned by technological advances, today's encryption debate is like a new cover version of an old song. America's privacy vs. law enforcement debate really began in the 1700s, when colonists resisted British soldiers who were permitted unfettered access to homes, businesses, and property. The Fourth Amendment – prohibiting unreasonable searches and seizures – is the direct result of colonists' umbrage and is the foundation of 200 years of America's civilian government.

More than 200 years after the Bill of Rights was ratified, innovators were building and commercializing the first wave of digital networks and privacy-focused companies were deploying the first generation of encryption technologies. At that time America's national security and law enforcement agencies expressed urgent concern about hostile foreign entities having access to that era's best encryption technology. In response, Congress approved the Communications Assistance for Law Enforcement Act ("CALEA") and thereby required companies to build law enforcement back doors into broadband and Voice-Over-IP networks and related equipment. Despite guaranteeing law enforcement access to communications, Congress sought to ensure that legal process would be followed prior to that access being utilized. Moreover, Congress recognized the importance of data security and included explicit protection for encryption and encrypted communications.

Today's debate is different, however, in part because circumstances have changed but also because law enforcement goals have transformed.

One significant new circumstance is that businesses and consumers are more technologically savvy and are smarter about data protection. Weekly reports about leading companies being hacked by organized cybercriminals, combined with so many consumers' personal experiences with identity theft, have propelled a market for security and encryption products. Identity theft has been the top consumer complaint to the FTC for fifteen consecutive years, and that trend is driving commercial activity.

Consumers and businesses are also responding to recent revelations of widespread, untargeted, bulk surveillance by national security and law enforcement agencies. This activity, including seemingly willful disdain for proper legal process, has made citizens justifiably skeptical of law enforcement promises that unfettered access to digital networks will be utilized judiciously. International governments are similarly provoked, and are requiring U.S. companies

to ensure that international consumers' (including businesses) data is protected, including against the U.S. government.

Encryption is no longer a niche market. In 1994, there were few digital products and services and the market for encryption was small and specialized. But today on my phone I have a traditional mobile telephone service as well as Viber, WhatsApp, Google Hangouts and Skype. Each of these apps, the operating system on my phone, the software in each network access point and the networks themselves may incorporate encryption so that my private conversations remain private. This privacy is also critical for business and enterprise apps to ensure privacy of, for example, trade secrets, financial and health care data.

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

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

The Implications of Today's Privacy v. Law Enforcement Debate Are More Significant and Potentially Much More Severe

In light of the ubiquity of digital products and services, and the magnitude of cybercrime and identity theft, it is perplexing that the FBI and law enforcement are disparaging the very large, substantial and determined encryption market that it has encouraged. This effort cuts against prevailing wisdom and sends confusing, unhelpful suggestions to app developers, and to the publishers and enterprises that developers work with.

First, developers whipsawed by the government's mixed messages may be paralyzed in their development cycle. As developers, investors and customers ask which government agency is in charge and whether data protection is really a government-approved value, the marketplace

can freeze up. If this uncertainty continues for too long then lawyers will have to help developers make a difficult and perhaps pyrrhic decision: which federal mandate should I follow and which one should I ignore?

The Subcommittee should appreciate the magnitude of mixed messages developers have received. Over the course of several years virtually every government law enforcement and consumer protection agency has sung from the encryption and data protection hymnal.

- The FTC advises consumers that "[e]ncryption is the key to keeping your personal information secure online," and consistently requires app developers to use "reasonable" data security practices, including encryption, to protect consumers' information from hackers and data thieves.
- California Attorney General Kamala Harris recommends that app developers "transmit user data securely, using encryption" and endorses legislation "requiring encryption to protect personal information in transit."
- The FBI recommended organizations "encrypt data so the hacker can't read it."
- President Obama's Review Group on Intelligence and Communications Technologies recommended that the U.S. Government promote national security by "fully supporting and not undermining" encryption standards and generally available commercial encryption, and "supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage."
- And in February President Obama personally called on industry to protect Americans' privacy and civil liberties, and proclaimed himself "a strong believer in strong encryption.... there's no scenario in which we don't want really strong encryption."

Against this backdrop, industry responded. Hardware manufacturers are selling encrypted Blackphones. Companies such as Apple, Google and Yahoo are embedding encryption into their software and operating systems. Snapchat, Yik Yak and SpiderOak are offering encrypted consumer solutions, and industries such as banking, health care, transportation and manufacturing are extremely focused on secure, encrypted solutions.

Additionally, nearly every app is pursuing international customers and every contract developer seeks international clients. Thus, it is important that Congress consider other

countries' reactions to U.S. digital policy and how other countries' policies could create challenges to American digital services or America's global interests.

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

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

Third, mandatory back doors diminish consumer trust and create challenges for apps and all digital businesses. In addition to government risk, app developers will face marketplace challenges if forced to provide privacy-breaching back doors to law enforcement. Our customers – in the United States and abroad – expect their communications to be private and secure when purchasing or using apps. Since our sector's inception just a decade ago, developers have prioritized the security and handling of their customers' data because they know that good data stewardship is critical to business success. Enabling governments to access data without proper legal process risks undermining the customer trust that app developers worked hard to obtain.

Congress should also anticipate that governments worldwide will demand their own back door key or separate back doors for their own security and law enforcement interests. This will

increase further the risk that consumer and business data could be compromised. Larger consumer app publishers might have the resources to build multiple back doors and might have enough consumer trust to withstand the associated scrutiny, but startups and resource-limited small innovators will be challenged to find resources to build multiple back doors, and will also have greater trust problems than established competitors. Of course, all apps not complying with other governments' demands could easily be locked out of those markets.

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

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

Fourth, forcing holes in encryption harms startups and small innovators the most. Many – perhaps most – of the small companies that are Alliance members lack the resources to create country-specific access points for law enforcement agencies around the world. It is relatively easy to build a back door, but difficult to build a back door that only certain people – the right people – can access. While the U.S. government is pleading to tech companies "let us in," they simultaneously warn companies to keep hackers and other countries out. Because building a back door that is slightly ajar is technically challenging and very expensive, it is extremely difficult for large companies, let alone startups, to meet these conflicting demands. App developers and startups already must overcome significant cost hurdles before products get to market, and any regulatory inconsistency or redundancy is one burden too many.

While situations may occasionally justify law enforcement and national security agencies' access to our cell phones, such as a missing child, or matter of exigency, our statutes are filled with multiple, well-established, legal methods to access this data. Congress should insist that U.S. law enforcement and national security agencies utilize these processes before mandating back doors into apps, digital products and digital services.

* * * * *

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

Americans correctly demand that their personal data is secure. Just as importantly, businesses deserve clear and consistent messages from our government to ensure a stable marketplace. I look forward to your questions and the Alliance looks forward to working with Congress on this important issue.

Mr. HURD. Thank you, Mr. Potter.
Dr. Blaze, 5 minutes to you.

STATEMENT OF MATTHEW BLAZE, Ph.D.

Mr. BLAZE. Thank you, Mr. Chairman.

As a technologist, I am finding myself in the very curious position of participating in a debate over the desirability of something that sounds wonderful, which is a security system that can be bypassed by the good guys, but that also reliably keeps the bad guys out.

And we could certainly discuss that. But as a technologist, I can't ignore a stark reality, which is simply that it can't be done safely. And if we make wishful policies that assume and pretend that we can, there will be terrible consequences for our economy and for our national security.

So it would be difficult to overstate today the importance of robust, reliable computing and communications to our personal, commercial, and national security. Modern computing and network technologies are obviously yielding great benefits to our society, and we are depending on them to be reliable and trustworthy in the same way that we depend on power and water and the rest of our critical infrastructure today.

But, unfortunately, software-based systems, which is the foundation on which all of this modern communications technology is based, are also notoriously vulnerable to attack by criminals and by hostile nation-states.

Large-scale data breaches, of course, are literally a daily occurrence, and this problem is getting worse rather than better as we build larger and more complex systems. And it's really not an exaggeration to characterize the state of software security as an emerging national crisis.

And the sad truth behind this is that computer science, my field, simply does not know how to build complex large-scale software that has reliably correct behavior. This is not a new problem. It has nothing to do with encryption or modern technology.

It has been the central focus of computing research since the dawn of the programmable computer. And as new technology allows us to build larger and more complex systems, the problem of ensuring their reliability becomes actually exponentially harder with more and more components interacting with each other.

So as we integrate insecure, vulnerable systems into the fabric of our economy, the consequences of those systems failing become both more likely and increasingly serious. Unfortunately, there is no magic bullet for securing software-based systems. Large systems are fundamentally risky, and this is something that we can, at best, manage rather than fix outright.

There are really only two known ways to manage the risk of unreliable and insecure software. One is the use of encryption, which allows us to process sensitive data over insecure media and insecure software systems to the extent that we can. And the other is to design our software systems to be as small and as simple as we possibly can to minimize the number of features that a malicious attacker might be able to find flaws to exploit.

This is why proposals for law enforcement access features frighten me so much. Cryptographic systems are among the most fragile and subtle elements of modern software. We often discover devastating weaknesses in even very simple cryptographic systems years after they are designed and fielded.

What third-party access requirements do is take even very simple problems that we don't really know how to solve and turn them into far more complex problems that we really have no chance of reliably solving.

So backdoor cryptography of the kind advocated by the FBI might solve some problems if we could do it, but it's a notoriously and well-known difficult problem. We have found subtle flaws even in systems designed by the National Security Agency, such as the Clipper Chip two decades ago.

And even if we could get the cryptography right, we'd be left with the problem of integrating access features into the software. Requiring designers to design around third-party access requirements will basically undermine our already tenuous ability to defend against attack.

It's tempting to frame this debate as being between personal privacy and law enforcement. But, in fact, the stakes are higher than that. We just can't do what the FBI is asking without seriously weakening our infrastructure. The ultimate beneficiaries will be criminals and rival nation-states.

Congress faces a crucial choice here: To effectively legislate mandatory insecurity in our critical infrastructure or to recognize the critical importance of robust security in preventing crime in our increasingly connected world. Thank you very much.

[Prepared statement of Mr. Blaze follows:]

MATT BLAZE

UNIVERSITY OF PENNSYLVANIA[1]

US HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT OVERSIGHT AND REFORM
INFORMATION TECHNOLOGY SUBCOMMITTEE
ENCRYPTION TECHNOLOGY AND POSSIBLE US POLICY RESPONSES

APRIL 29, 2015

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

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

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

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

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

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

Unfortunately, modern computing and communications technologies, for all their benefits, are also notoriously vulnerable to attack by criminals and hostile state actors. And just as the benefits of increased connectivity and more pervasive computing will continue to increase as technology advances, so too will the costs and risks we bear when this technology is maliciously compromised. It is a regrettable (and yet time-tested) paradox that our digital systems have largely become *more* vulnerable over time, even as almost every other aspect of the technology has (often wildly) improved. New and more efficient communication technologies often have less intrinsic security than the systems they replaced, just as the latest computers and other devices regularly suffer from unexpected vulnerabilities that are exploited remotely by malicious attackers. Large-scale data breaches and similar security failures have so become commonplace that they now only make the news when their consequences are particularly dramatic. Serious security failures are literally a daily occurrence, and it is not an exaggeration to characterize this situation as an emerging national crisis.

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

While a general solution to the problem of software reliability and correctness has eluded us (and will continue to do so absent some

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

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

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

II. Law Enforcement Access Requirements Carry Great Risks

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

At first blush, a "lawful access only" mechanism that could be incorporated into the communications systems used by criminal suspects might seem like an ideal technical solution to a difficult policy problem. Unfortunately, harsh technical realities make such an ideal solution effectively impossible, and attempts to mandate one would do enormous

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

harm to the security and reliability of our nation's infrastructure, the future of our innovation economy, and our national security.

A. Access Requirements Make Encryption Vulnerable and Expensive

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

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

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

There are several fundamental problems with such schemes.

The most basic problem with law enforcement access cryptography is simply that we do not fully understand how to design them, even at an

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

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

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

This is not simply an abstract concern. Virtually all law enforcement key recovery or key escrow proposals made to date, including those designed by the National Security Agency (the Clipper Chip[5]), have had unanticipated design weakness discovered after the fact.

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

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

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

---

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

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

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

Further risks arise from the *operational complexity* of managing access to the secrets keys. Key access centers must presumably be prepared to respond to law enforcement requests for key data 24 hours a day, completing transactions within a short time of receiving each request and in complete secrecy from the target of the investigation. There are thousands of law enforcement agencies in the United States authorized to perform electronic surveillance; the escrow centers must be prepared to identify, authenticate and respond to any of them within a short time frame. Even if we imagine relaxing these requirements considerably (e.g., one day or even one week response time), there are few existing secure systems that operate effectively and economically on such a scale and under such tightly constrained conditions.[7] It is simply inevitable that lawful access systems that meet the government's requirements will make mistakes in giving out the wrong keys from time to time or will be vulnerable to unauthorized key requests. Nation-state adversaries could be expected to be particularly interested in, and adept at, fraudulent access to our law enforcement access services.[8]

B. Access Requirements Make Critical Software Vulnerable to Attack

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

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

---

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

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

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

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

There has not yet been a specific proposal that specifies exactly which digital products and services for which the FBI seeks surreptitious data access mandates But even under a very conservatively applied mandate, ensuring law enforcement access in this way would be necessarily add complex requirements to an exceptionally broad range of consumer, business, and infrastructure-support software. We enjoy today flourishing, heterogeneous software and service marketplace. Everything from small mobile apps that provide instant messaging services to large-scale communication and data storage platforms routinely process communication and stored data that might potentially serve as evidence.

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

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

only the minimum resources possible to meet the requirements. The result will be that while the features might work in the sense that they allow law enforcement access, they can also be expected to account for a large proportion of the potentially exploitable defects in the system as a whole.

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

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

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

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

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

This is not simply a matter of weighing our desires for personal privacy and to safeguard against government abuse against the need for improved law enforcement. That by itself might be a difficult balance for policymakers to strike, and reasonable people might disagree on where that balance should lie. But the risks here go far beyond that, because of the realities of how modern software applications are integrated into complete systems.

Vulnerabilities in software of the kind likely to arise from law enforcement access requirements can often be exploited in ways that go

beyond the specific data they process. In particular, vulnerabilities often allow an attacker to effectively take control over the system, injecting its own software and taking control over other parts of the affected system.[9] The vulnerabilities introduced by access mandates discussed in the previous section are likely to include many in this category. They are difficult to defend against or contain, and they current represent perhaps the most serious practical threat to networked computer security.

For better or worse, ordinary citizens, large and small business, and the government itself depend on the same software platforms that are used by the targets of criminal investigations. It is not just the Mafia and local drug dealers whose software is being weakened, but everyone's. The stakes are not merely unauthorized exposure of relatively inconsequential personal chitchat, but also leaks of personal financial and health information, disclosure of proprietary corporate data, and compromises of the platforms that manage and control our critical infrastructure.

In summary, the technical vulnerabilities that would inevitably be introduced by requirements for law enforcement access will provide rich, attractive targets not only for relatively petty criminals such as identity thieves, but also for organized crime, terrorists, and hostile intelligence services. It is not an exaggeration to understand these risks as a significant threat to our economy and to national security.

[9] Such vulnerabilities, for example, are how so-called "botnets" are able to take control over large numbers of computers on the Internet.

Mr. HURD. Thank you, Dr. Blaze.

I would now like to recognize my fellow Texan, Blake Farenthold, for 5 minutes.

Mr. FARENTHOLD. Thank you very much, Mr. Chairman.

Could we get the slide up?

I think it was Mr. Potter that pointed out the FBI had some recommendations on their Web site about encryption that was recently taken down. I want to read the two that are highlighted.

And, Ms. Hess, I want to get a couple questions for you on that.

"Depending on the type of phone, the operating system may have encryption available. This can be used to protect the user's personal data in case of a loss or theft."

And it also says, "Pass code-protect your mobile device. This is the first layer of physical security to protect the contents of this device."

These are now off of the FBI Web site. Why did the FBI take down this guidance?

Ms. HESS. Yes, sir. Actually, we decided to provide a link to that information. That same information actually appears through the link to IC3.

Mr. FARENTHOLD. And you agree that that is probably good advice. You still advise people it is a good idea to encrypt their data?

Ms. HESS. Yes, sir. We fully support encryption.

Mr. FARENTHOLD. All right. Now, Dr. Blaze, you talked about the good guys versus the bad guys. Who is a good guy today may not always be a good guy. I mean, that definition of good guy, bad guy—I mean, it is overly simplistic.

Who are the good guys? Who are the bad guys? And who makes that decision?

Mr. BLAZE. That is certainly true. And I think, even if we can draw a line between who we want to have access and who we don't, which is, of course, an impossible task in practice, we'd still be left with the problem that we wouldn't be able to provide access.

Mr. FARENTHOLD. And, Mr. Bankston, let's talk a little bit about a golden key. That is one of the things that folks are looking at.

Wouldn't that become the biggest hacker target in the world if it were known there were a golden key and what we have today that might be deemed secure as computing power increases might become a lot easier to break?

Mr. BANKSTON. Yes, Congressman. That is absolutely the case. I think that, as Professor Blaze made clear, attempting to build such a system would add incredible levels of complexity to our system such that it would inevitably, as the cybersecurity coordinator at NIST said recently, lead to unanticipated vulnerabilities.

And that doesn't even count the possibility of bad actors obtaining the keys. Even if you were to split those keys apart, as the NSA director has suggested, you have to put that key together somewhere, and wherever you do do that is going to be a critical target for anyone who wants to compromise our security.

Mr. FARENTHOLD. Yeah. I have got a very limited time. I don't mean to cut you off. I am just trying to get some broad general answers. We can get down to the weeds in another opportunity.

Is there anybody on the panel who believes we can build a technically secure back door with a golden key? Raise your hand and I will recognize you if you think that can be done.

All right. Let the record reflect no one on the panel thinks that that can be done.

All right. Let's talk a little bit about if we were to go ahead and do it. The United States—let's assume they are a good guy and we agree to put in a back door for them. All of a sudden we want to sell this same product in another country. So China wants a back door. North Korea wants a back door.

Basically, every country is going to want a back door. Does anybody disagree with that statement?

I see no hands coming up for that one either.

So we then are good. So do we put all of these back doors into every system, making it that much more difficult, or do we then say, "All right. Well, this phone is sold in the United States. We are going to put a U.S. back door in"?

Well, that doesn't help our intelligence community abroad. And if I wanted to avoid that, I would go to the Cayman Islands, which I would assume would have better privacy laws—I don't know—there would be some haven country—and buy my phone there. Would it then be seized by Customs?

I mean, I don't see a practical way to implement this. I am now appointing you to the NSA. You are the head of the NSA. Anybody got a way we can do what we want to do? Raise your hand if you have got any suggestions that you think we can do it.

Mr. Conley.

Mr. CONLEY. Yeah. I am no expert. I am probably the least technologically savvy guy in this room, maybe. But there are a lot of great minds in the United States. I'm trying to figure out a way to balance the interests here. It is not an either-or situation.

And Dr. Blaze said—you know, he's a computer scientist. I'm sure he's brilliant. But, jeez, I hate to hear talk like, "That cannot be done." I mean, think about if Jack Kennedy said, "We can't go to the moon. That cannot be done." He said something else, "We're going to get there in the next decade."

So I would say to the computer science community let's get the best minds in the United States together on this. We can balance the interests here.

Mr. FARENTHOLD. And I appreciate that because I am a proud American as well. But I think what we are saying today is—it would be the equivalent of President Kennedy saying, "We will be able to get to the moon in 10 years and nobody else will ever be able to get there ever." I think that is the distinction I would like to draw there.

It is not like we are saying we can't develop a secure system, but we are also saying that can we really develop a secure system that will be secure for any length of time that somebody smarter might not be able to hack 5 years down the road or so.

Anyway, I see I am already out of time. I appreciate your indulgence, Mr. Chairman.

Mr. HURD. Thank you.

Votes have been called on the House floor. And what we are going to do is go to Ranking Member Kelly for questions, and then we will recess and reconvene 10 minutes after votes.

I would now like to recognize my good friend, Ms. Kelly from Illinois.

Mr. CONNOLLY. Would my friend Ms. Kelly yield just for a second? Because I may not be able to come back.

I just want to welcome Mr. Potter, who is an old friend and colleague of mine. And I wish to welcome Mr. Conley, though I wish he would learn how to spell his name.

Thank you very much.

Ms. KELLY. Thank you, Mr. Chair.

Mr. Bankston, a core component to what we are doing here today is examining what we can do to protect the privacy of consumer data and not serve as a barrier to law enforcement communities' ability to do work that keeps us safe. I know I have heard from a number of folks on both sides of the data privacy issue.

And so my question is: Is there such a thing as creating a back door that is only for the good guys?

Mr. BANKSTON. I am also not a technical expert. I am a policy expert. But based on what every expert in the field has said not only in the current debate, but also 20 years ago in a many-multi-year debate over exactly this issue, the answer is a clear no and, in fact, a unanimous no.

Ms. KELLY. Also, could the existence of a back door created in the interest of public safety actually serve as a Trojan horse that cybercriminals exploit to their advantage?

Mr. BANKSTON. Absolutely. Any back door is going to necessarily weaken the security of a system in a way that another actor, someone with worse interests than our own Government trying to protect us, could exploit.

Ms. KELLY. Any other comments about that?

Ms. HESS. Yes, ma'am. First off, when we are discussing solutions, what we found in the past is that, if solutions are developed on the front end of a design, they're ultimately more secure than something that is patched on to the back end of an existing solution, of an existing network, or an existing device.

That we also found with respect to what Mr. Bankston refers to 20 years ago when a law was enacted that, essentially, most thought would decrease security of systems, and that turned out not to be the case. To the contrary. Companies actually developed more secure ways of being able to still conduct the surveillance that we were able to enact back 20 years ago.

Mr. BANKSTON. If I may respond to that, I assume Assistant Director Hess is referring to CALEA, the Communications Assistance for Law Enforcement Act, which actually explicitly provided that the phone companies subject to its intercept capabilities were under no obligation to prevent or assist in the decryption of encryption that was done by their users or even encryption that they offered where they did not hold the keys. So protection for encryption and, in fact, end-to-end encryption was protected explicitly in CALEA.

Ms. KELLY. Thank you.

I yield back.

Mr. HURD. The gentlelady yields back.

I would like to recognize the chairman of the committee, Chairman Chaffetz, for 5 minutes.

Mr. CHAFFETZ. Thank you.

And I again thank you all for being here.

There are some important questions that face us.

Ms. Hess, you have a very important role within the FBI, and we appreciate the work that you are doing. But it was said earlier—and I want to ask you and give you a chance to respond to it.

But does encryption actually help prevent crime, in your opinion?

Ms. HESS. Yes, sir, it does.

Mr. CHAFFETZ. But the policies that the FBI is advocating, specifically the Director, don't necessarily fall in line with that, do they? I struggle with what the Director is asking for because—are you going to have encryption? Not encryption?

Ms. HESS. Yes, sir. I think the distinction comes from the idea that we are not supportive or in favor of encryption, and that is not true. That is not accurate. We actually want encryption. It secures our networks. It obviously assists us in providing security and blocking the cyber threats.

However, all we're asking for is a way for us to be able to, with a lawful order, be able to get information from the company so that the provider would be able to provide in readable form the potential evidence that we would need in an investigation.

Mr. CHAFFETZ. So you want encryption, but a key. And doesn't that key by its very definition create a vulnerability?

Ms. HESS. In today's world, sir, I think that there is no such thing as absolute security in either the physical or the digital world. What we are asking for is not to lower those standards by developing some type of lawful intercept or lawful access capability but, rather, to come up with a way that we may be able to implement perhaps multiple keys or some other way to be able to securely access the information—or, actually, rather, be able to be provided with the information.

Mr. CHAFFETZ. And that is the concern, is that, if you create a key—let's pretend it is a key to your house. You can go down to Ace Hardware and make a copy of it. Right? Somebody is going to be able to figure it out. You can get a locksmith who can go and open up your front door.

And the same principle—unless there is some new technology that we don't know about, that is the concern. And that is the disconnect from what we hear from the FBI and the reality of—do you create the hardest, strongest encryption possible, which means not having a key?

And, again, I know we won't necessarily solve it all right here in this debate. But I have got to ask you something else before I run out of time.

One of the keen concerns that I have—and I have sponsored a bill called the GPS Act—deals with geolocation. There is a debate and discussion about metadata versus content, for instance, in emails.

If you and I are trading emails, you have heard the Department of Justice argue that the fact that I communicated with you is just the metadata. It is not the content of what we were talking about.

Does the Department of Justice believe that your geolocation is content or do they just think that that is metadata?

Ms. HESS. Well, sir, first off, for geolocation information, we do obtain a search warrant for that information.

Mr. CHAFFETZ. Always?

Ms. HESS. But I——

Mr. CHAFFETZ. Always?

Ms. HESS. I would have to ask that we maybe brief you about that in more detail at a later time.

But at the same time, to address your issue about metadata and geolocation information, clearly those certainly are useful tools, usual techniques, for us to be able to paint the picture of what happened in an investigation, but they are not wholly inclusive of all the evidence we may need to be able to show intent, for example, with the content of the communication.

Mr. CHAFFETZ. I understand the need. And I don't have a problem if you have probable cause or get a warrant or even articulable suspicion.

What I have a problem with is you tracking geolocation at will. And I think Americans have a reasonable right to privacy.

So post-Jones, what I still struggle to understand from the Department of Justice is: What is their guidance? What are their rules of the road?

I mean, I would like to know if you all track my wife or not. Do you do that? I know you can. My question is: Do you do it?

And you are giving me a, "Well, I am not"—I mean, clarify that for us. It is not a yes or a no. That is the concern. I am not getting a yes or no from you.

Ms. HESS. I would answer in response to that question that, certainly, to obtain any type of information, we would go through lawful process.

Mr. CHAFFETZ. Is lawful process your ability to track geolocation without getting a warrant?

Ms. HESS. Currently we do get a warrant, is my understanding.

Mr. CHAFFETZ. And I amasking: Do you always get a warrant to track geolocation? The answer is no, isn't it?

Ms. HESS. There's exigent circumstances. That is correct.

Mr. CHAFFETZ. Okay. So describe those circumstances.

At what level? What is the threshold? What is the guidance?

Ms. HESS. So, first, I believe it would depend on the type of data that we are talking about——

Mr. CHAFFETZ. Geolocation.

Ms. HESS. —and the type of geolocation data, whether that's GPS data or whether that's some type of other geolocation type of data.

I again would request that we could certainly brief you on this in more detail.

Mr. CHAFFETZ. Yeah. I want you to brief the American people. This is why I am going to continue asking these questions.

Mr. Chairman, I am out of time. And we have a vote on the floor. But this is one of the deep questions I have for the Department of Justice.

Believe me, you are not the first person that can't clearly answer this, and I think people have the right to know what that answer is.

Is the Government tracking their geolocation? And right now I think the answer unfortunately is, yes, they are. And certainly they are at times without a warrant and without articulable suspicion.

With that, I yield back.

Mr. HURD. Votes have been called on the House floor. We will recess and reconvene 10 minutes after voting.

[Recess.]

Mr. HURD. The Subcommittee on Information Technology will reconvene.

I would like to now recognize my colleague from California and fellow recovering computer scientist, Ted Lieu, for 5 minutes.

Mr. LIEU. As a recovering computer and science major, it is clear to me that creating a pathway for decryption only for good guys is technologically stupid. You just can't do that.

But I am more interested now in knowing, if this were to happen, what would the effect of this be on global companies and global app developers.

And, Mr. Potter, in your testimony, you raise concerns that device pathway will introduce technological vulnerabilities to mobile application.

What effect would the pathway have on the global application developers' market?

Mr. POTTER. Thank you for that question, Congressman Lieu.

Today every app developer thinks that their marketplace is global, their opportunity is global. The Google Play Store is global. The Apple devices are global.

The challenge is in Europe we have a very different privacy regime than we have in the United States. And Europe has already made—European leaders have already spoken quite bluntly that, if they strengthen their privacy laws, it will, in fact, harm U.S. companies and create business opportunities for European companies.

So European leaders in the privacy area are very concerned about—and they've been pretty blunt about it—Facebook, Amazon, Google, collecting data and things like that and what do they do with the data. And they are extraordinarily distressed with the U.S. Government vacuuming up data throughout the world, including listening to phone calls of some of their leaders.

The combination of that, of the political angst and the business stress, creates a very easy opportunity for them to simply say that any company that has a back door particularly to the U.S. Government, which at least in the minds of European leaders, does not have a great history of using those back doors with discipline, creates a vulnerability that is unlawful under European privacy law; and, therefore, you'd be banned from the European market.

Mr. LIEU. Thank you. I appreciate that.

I am going to reserve the balance of my time to make a statement. It is primarily directed at Mr. Conley. I respect your public service. I take great offense at your testimony today.

You mention that unaccountable corporate interests such as Apple and Google are essentially protecting those who rape, de-

fraud, assault, and kill. I think that is offensive. It is a fundamental misunderstanding of the problem.

Why do you think Apple and Google are doing this? It is because the public is demanding it, people like me, privacy advocates, a public that doesn't want an out-of-control surveillance state. It is the public that is asking for this. Apple and Google didn't do this because they thought they would make less money. This is a private sector response to government overreach.

Let me make another statement that somehow these technology companies are not credible because they also collect private data. Well, here is the difference. Apple and Google don't have coercive power. District attorneys do. The FBI does. NSA does. And, to me, it is very simple to draw out the privacy balance when it comes to law enforcement and privacy. Just follow the damn Constitution.

And because the NSA didn't do that and other law enforcement agencies didn't do that, you are seeing a vast public reaction to this. Because of NSA, your colleagues have essentially violated the Fourth Amendment rights of every American citizen for years by seizing all of our phone records, by collecting our Internet traffic. That now is spilling over to other aspects of law enforcement.

And if you want to get this fixed, I suggest you write to NSA and the FBI should tell the NSA "Stop violating our rights" and then maybe you would have the public much more on the side of supporting some of what law enforcement is asking for.

And then let me just conclude by saying I do agree with law enforcement that we live in a dangerous world and that is why our Founders put in the Constitution of the United States of America—that is why they put in the Fourth Amendment, because they understand that an Orwellian, overreaching Federal Government is one of the most dangerous things that this world can have.

I yield back.

Mr. CONLEY. Do I get to respond to that?

Mr. HURD. The gentleman yields back.

I would like to recognize my colleague, Mr. Blum from Iowa, for 5 minutes.

Mr. BLUM. Thank you, Chairman Hurd.

I would like to welcome today the panelists. I appreciate your insights on this topic.

And I also would like to acknowledge law enforcement. I know it is not easy what you do, and I am so appreciative of the amazing job that your departments do. And I love the Thin Blue Line. So thank you so much for what you do.

Ms. Hess, my questions are probably addressed to you. I just want to make sure I understand this.

Law enforcement wants to force the private sector to build a back door, if you will, or backdoor key into cell phones, into software, things such as that. Is that correct?

Ms. HESS. Sir, I would actually phrase that from the sense that we are simply asking for information that we seek in response to a lawful order in a readable format. How that actually happens should be the decision of the provider.

Mr. BLUM. So you are not asking for a backdoor key into the encrypted software or cell phone?

Ms. HESS. If we don't have the key, but, yet, the provider can get us that information by maintaining the key themselves, then that would be obviously a legitimate way to respond to our lawful order.

Mr. BLUM. Okay. And what you are asking for only would be used if a warrant is issued. Is that correct?

Ms. HESS. Yes, sir. Everything we are discussing today. Yes, sir.

Mr. BLUM. And what we are discussing today would arguably make law enforcement's job quicker, easier to apprehend the bad guys, as we said. Is that correct?

Ms. HESS. Yes, sir.

Mr. BLUM. I am a software developer myself, and I am also a homebuilder. So I would just like to give you an analogy as I understand this.

Isn't this analogous to the Government asking or requiring homebuilders to put a video camera in every room of every new home that they build with the guarantee or the promise that the Government won't turn it on, "Don't be concerned. The Government will not turn this camera on unless we get a warrant"? And that would make law enforcement's job easier, correct, and quicker if there is a crime in the home? Isn't this analogous to that? Because you are saying, "Trust us. We will only do this if we need to do it."

Ms. HESS. Sir, I think the analogy may be better described as if we should need to know what is going on in that home. Then, as long as the company can respond quickly. Now, that may mean that they wire the home, but it certainly doesn't mean they necessarily have to have the cameras installed as long as they can do that quickly.

On the other hand, if they can come up with a different way to tell us what is going on inside that home and do it quickly in a timely manner that is quickly available to us when needed, then whatever way they come up with would be acceptable.

Mr. BLUM. Because what troubles me is law enforcement tends to agree with—and I will paraphrase here—but that there is a reasonable standard of privacy, Fourth Amendment rights, when one is in their own home. I think most people in law enforcement would agree with that.

But when it comes to our cell phone conversations, our emails, anything that is electronic and data, it seems like this reasonable right to privacy isn't there. The people in my district in Iowa feel the same way.

Would you address that, please.

Ms. HESS. Yes, sir. I would like to.

I believe that is inaccurate. Certainly you do have a reasonable expectation of privacy, which is why what we are referring to today and discussing here today requires a warrant. Whether that is realtime communications or the data stored on that device, it still would require a warrant. And that is the threshold under the Constitution.

Mr. BLUM. Thank you.

And this next question is for anyone on the panel. Does law enforcement have other ways, other ways, other than what you are asking for, to access the necessary data needed in, let's say, 99 percent of the criminal cases? Are there other ways of doing this?

Because it seems like we are always given, as citizens, the dichotomy of liberty and giving up liberty and freedom for safety. And I believe in American exceptionalism. I believe we can have both.

Aren't there other ways law enforcement can do this?

Ms. HESS. Yes, sir. I would like to address that.

I also believe that we can balance liberty and security and public safety. I would say that there are certainly—when law enforcement is stymied by a particular obstacle in an investigation, we will seek all other ways to get the information we need.

But those other ways may delay us in getting that information. They may not be timely solutions. They may not be encompassing solutions to where we might be able to identify other victims or other coconspirators or the vast nature of the crime or the impact of the crime, and that is what concerns us, to be able to get that information quickly.

Mr. BLUM. And I am out of time. I yield back, Mr. Chairman.

But, once again, I would like to thank law enforcement for the amazing job that you do. Thank you very much.

Mr. HURD. The gentleman yields back.

I would like to recognize myself for 5 minutes for questions. I have got questions for everyone.

So we will start with you, Dr. Blaze. Can you tell us a little bit about your background, quickly, your degrees, how long have you been involved as a computer scientist in cryptology.

Mr. BLAZE. I am computer scientist. My specialty is in computer security and cryptography and the applications of cryptography to building large-scale systems.

As a particular focus of my research area, I have been concerned with surveillance technologies and some of the issues at the intersection of technology and public policy. In this issue, 20 years ago I discovered some flaws in the previous U.S. Government proposal, the Clipper Chip.

Mr. HURD. And you are at a university that the department is pretty well known worldwide when it comes to cryptology and computer science. Is that correct?

Mr. BLAZE. I would like to think so.

Mr. HURD. And I know you are a modest man. So I don't mean to ask an indelicate question.

But you are considered an expert when it comes to cryptology and encryption?

Mr. BLAZE. I suppose so.

Mr. HURD. So in your expert understanding, is there any way to do a split-key approach to encryption?

Mr. BLAZE. There are things we can do, like splitting the key between multiple locations, that can reduce some aspects of some of the risks in a system like this.

Mr. HURD. But it does create additional vulnerabilities——

Mr. BLAZE. That is right.

Mr. HURD. —that anyone who has technical capability would be able to take advantage of?

Mr. BLAZE. That is right. We can move the risks around from one part of the system to another, but there are still fundamental problems that we don't know how to solve.

Mr. HURD. And this was ultimately part of the problem with the Clipper Chip from the 1990s?

Mr. BLAZE. That is right. There were a number of problems with the Clipper Chip proposal, but that was one of them.

Mr. HURD. Thank you, sir.

Mr. Potter, as a politician, I am always told don't answer hypothetical questions, but I am going to pose a hypothetical question to you.

If there were a back door or a front door put into applications or programs of U.S. businesses, how do you think—the impact that would have on businesses in China, Russia and Iran?

Mr. POTTER. I have to anticipate, sir, that those governments would ask for their own back door.

Mr. HURD. Thank you.

Mr. Bankston, we are going to save you for last.

Mr. Conley, if you have a properly issued warrant to go into someone's house and there is a safe in that house that is locked, what happens?

Mr. CONLEY. The safe will be taken out and it would be broken into.

Mr. HURD. Okay. So in your testimony you mentioned that Google—and I believe we can infer Apple—stated that its new operating system would make its mobile devices inaccessible to law enforcement officials even with a warrant signed by a judge. Is that correct?

Mr. CONLEY. That is correct.

Mr. HURD. So if you had a properly issued warrant, would you not be able to get that device?

Mr. CONLEY. You could get the device. You couldn't get the information off the device if it is running iOS 8.

Mr. HURD. So iOS 8—the default setting is a five-digit PIN. Correct?

Mr. CONLEY. Is it five? It is a pass code of some sort.

Mr. HURD. Dr. Blaze, I am a little rusty when it comes to—so that is 5 factorial over 5. Right? And it would take, what, 13,000 possible iterations of a potential five-digit PIN? Actually, it is a four-digit PIN, I believe what it is, four-digit PIN.

Mr. BLAZE. Yes.

Mr. HURD. So that is 4 factorial over 4, which is even less than 13,000.

Mr. BLAZE. 10 to the 4th. So about 10,000.

Mr. HURD. For a brute-force method with today's technology, is that difficult?

Mr. BLAZE. That is well within the range of a brute-force attack.

Mr. HURD. And how long would that take, roughly?

Mr. BLAZE. On modern computing hardware, essentially no time at all.

Mr. HURD. So would you agree that that is the equivalent of taking a safe out of a home and using some safe-cracking skills? This would be the digital equivalent?

Mr. BLAZE. No. This would be much easier than that.

Mr. HURD. Because you are good. You know? I think my colleagues from Texas A&M would probably be able to do it, too.

Now, my next question is to you, also, Mr. Conley, on the up-skirting example that you used, if you had surveillance on someone doing up-skirting, the fact that they are putting a camera to try to take pictures of someone, would that not be enough to arrest them?

Mr. CONLEY. That would not be enough. In order to commit the crime, you have to have taken the photo, and there would be no way to prove it. There would be no way to prove that the actual photo was taken, what it was taken of. So we could not successfully prosecute that case without the photograph, in my opinion.

Mr. HURD. Excellent.

I would like to yield to my colleague from California, Mr. Lieu.

Mr. LIEU. Thank you, Mr. Chair.

I do have some more questions along the lines of how easy it would be to defeat one of these pathways. So let's say we pass law that says: Okay. The Apple iPhone now has to have this pathway only for good guys.

What is to keep a terrorist—and this is for Dr. Blaze—for example, from saying, "Even though I like their multi-colored Apple iPhones, I am going to switch to Samsung phones?" Is there anything stopping that from happening?

Mr. BLAZE. No. Fundamentally, the ease of loading application software and the wide variety of platforms that we have make it very simple for somebody who is determined to use unbreakable encryption to do so. It might not be as easy or as inexpensive as we would like it to be, but there are no fundamental barriers to it.

Mr. LIEU. And currently, right now, there is nothing preventing two people anywhere in the world from downloading an encryption program to encrypt end to end those two communications that would make this pathway essentially meaningless. Is that correct?

Mr. BLAZE. That is right. Now, there may be vulnerabilities on the computers that run that software, and, in fact, there likely would be for the reasons that I discussed in my written testimony. But the encrypted messages themselves in transit would be effectively impossible in practice to decrypt.

Mr. LIEU. And is it your understanding that sometimes terrorists now resort to something as simple as just writing something on a piece of paper so they are off the grid?

Mr. BLAZE. Well, I am not an expert on terrorists, but I would imagine that paper-and-pencil technology is well within their——

Mr. LIEU. And we don't say that companies who make paper shredders are somehow protecting terrorists. Correct?

Mr. BLAZE. I have never heard that said.

Mr. LIEU. So let's talk a little about computer code. It is true, isn't it, that computer code is neutral, that is, the code cannot tell if the person reading the code or accessing the code is Asian or the leader of Hamas or the FBI director or gay or a woman or a man? As long you have got the key to that encryption, you get in the system. Correct?

Mr. BLAZE. That is right.

Mr. LIEU. The NSA, would you agree, has one of the most secure systems in the world?

Mr. BLAZE. I think they have enormous expertise.

Mr. LIEU. Curious, isn't it, that we now know so many secrets about the NSA not because of technology, but because we have human beings?

And so another aspect of all of this is you would be asking the American public to trust all the human beings in the Federal Government who could be looking at private data.

And it turns out, right, that sometimes human beings do things you don't want them to do, such as this one person who now disclosed all these secrets of the NSA, even though that is one of the most secure systems in the world?

Mr. BLAZE. The operational aspects of maintaining any kind of large-scale secure system are enormously daunting, as I think the NSA discovered 2 years ago.

Mr. LIEU. Thank you.

And I yield back.

Mr. HURD. Thank you.

I would like to recognize the ranking member, my good friend Ms. Kelly from Illinois, for 5 minutes.

Ms. KELLY. Thank you.

Ms. Hess and Mr. Conley, when you are not doing your job, you are citizens of our society. So how do you reconcile the need for this data with people's privacy interests in their data? Because you are a person, too, and then you are in law enforcement. So how do you reconcile this?

Ms. HESS. Yes, ma'am. I will start.

I certainly obviously value my privacy. I want to make sure that my system is as secure as possible. And I think that goes back to the points that certainly the FBI is trying to make, which is that we support encryption. We want secure networks.

It is just this inability that, for example, if I was committing criminal activity, that that information would be completely inaccessible. So in the safe example, we would never be able to access what is inside that safe, and that, I think, is more to the point of the question because certainly we do value privacy and certainly the safeguards of the Constitution.

Ms. KELLY. Thank you.

Mr. CONLEY. As I mentioned in my remarks, too, I value my privacy as much as the next person. Just to give you an example, recently my computer at home was infiltrated by somebody. And so anytime I click onto a link, I get bombarded with all sorts of merchandising messages and so forth. Somewhat innocuous, but it is clear that my computer was infiltrated. So I went out and bought some security software and loaded it onto my computer. So I am certainly very cognizant of the need to protect my privacy. I do all my banking and so forth on this.

My position has always been just very simple, that we ought to not be able to completely hide valuable evidence of a crime that is being committed or has been committed to hold individuals accountable for their actions. And that is what I am advocating for, some sort of balancing of the interests here so that everyone's right to privacy is acknowledged and glorified, really, but at the same time law enforcement is not completely kept in the dark about these sorts of things.

Ms. KELLY. I appreciate all of your testimony. And, obviously, encryption of data, from what I am hearing, should be conducted in a way that respects both law enforcement and private consumers' interests.

So, again, I want to thank the chairman for holding this very important hearing.

Mr. CONLEY. Mr. Chairman, you had asked the question about the pass code and about brute force. And far be it from me, I suppose, to challenge Dr. Blaze on brute force.

But my iPhone is owned by the Commonwealth of Massachusetts, and it has seven digits. My pass code is not four, but seven. So I suppose the exponential issue there is considerably larger, obviously, with seven digits. And I am told that, after 10 attempts to break into my—using my pass code, that is it. I am blocked out and there is some erasure that goes on.

So at least up to this point in this hearing, I believed that there is no brute-force technology out there available that could allow law enforcement to break into somebody's handheld device.

And I also ask this question: Can this issue be bifurcated in some way so that big corporate computer networks and so forth can remain encrypted without any sort of golden key, but devices like this, mobile devices, which are now the tools of terrorists and criminals, can be accessed on probable cause after a magistrate issues a warrant?

Mr. HURD. Thank you, Mr. Conley.

And to answer that question, when I left the CIA, I spent about 5 years helping build a cybersecurity company. We did penetration testing, technical vulnerability assessments.

And I would always offer my clients—a lot of times we worked with banks, and I would offer my clients the option of, "You pay our fee or we get to keep what we take." Nobody took us up on the last one because we never not got in.

So the tools, the technical capabilities, are out there. That is something that—having a conversation about how do we get the right tools and expertise to law enforcement may be a conversation where that may be a positive thing that comes from this conversation.

Mr. Conley, last question for you, sir, or sets of questions. In the up-skirting example, are there up-skirters in Boston that haven't been caught because they have used encryption?

Mr. CONLEY. Well, this encryption technology is nearly brand new. So I am not aware of any cases yet. You know, when we caught an up-skirter in Massachusetts, we realized actually there was no statute that made it a crime. So the Massachusetts legislature quickly took up this issue and made it a crime, meteoric.

Mr. HURD. As it should be.

Mr. CONLEY. As it should be.

Mr. HURD. As it should be.

And, also, to you, I appreciate your work and what you do. You know, 9 years I was an undercover officer overseas collecting intelligence on threats to the homeland. I collected that intelligence to help law enforcement and help folks like you and your colleagues put these bad guys away. You do this at a threat to your own life. You do this at a threat to your family. And I thank you for that.

But, also, you know, because of the role you play and the importance you play, I actually hold you all up to a higher standard as well, and I am always proud to stand side by side with you all.

Ms. Hess, question for you. What is the FBI asking for?

Ms. HESS. Yes, sir, Mr. Chairman.

I would say that certainly what we are asking for, first and foremost, is exactly what we are doing here today and just the opportunity for the American public to consider these issues and to weigh the risks.

Because clearly we recognize that there is no absolute security, again, in either the physical or the digital world. Everything may present a vulnerability. There may already be vulnerabilities in place.

But for law enforcement to not have the ability to accept or to receive the information that we might need in order to hold those accountable who conduct heinous crimes or who will conduct terrorist attacks, that's the question that I think we need to balance in the American public. And just by having that conversation will help us, I think, to make better informed decisions.

Mr. HURD. Thank you.

And, Ms. Hess, does the FBI have any information or data that suggests that the inherent vulnerabilities that have been discussed about dual encryption is that there is a way to do it?

Ms. HESS. We certainly believe and share Mr. Conley's hope that there is some type of innovative solutions out there, that we might be able to see government and industry work together to come up with—certainly they won't be bulletproof, as has been said earlier, but certainly more secure ways of being able to get law enforcement what it needs, yet at the same time provide layers and layers and layers of security so that the providers can provide the customer what they need as well.

Mr. HURD. Thank you.

Mr. Bankston, in your written testimony, you talked about the President's Review Group.

Can you characterize quickly for me what the President's Review Group was.

Mr. BANKSTON. The President's Review Group was a panel of experts picked by the President, five of them, to review the NSA's intelligence activities, including a former CIA director and a former anti-terrorism czar of the White House. They concluded that it should be the policy of the United States to promote rather than undermine the use of strong encryption.

Mr. HURD. And you highlighted Recommendation 29.

Mr. BANKSTON. Number 29.

Mr. HURD. And I would like to read that. And I do appreciate all of you all's written testimony. But you had a lot of great information here.

Mr. BANKSTON. Thank you.

Mr. HURD. And Recommendation 29 that President Obama's Review Group provided was that they recommend, regarding encryption, the U.S. Government should fully support and not undermine efforts to create encryption standards; number two, not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and, number three, increase

the use of encryption and urge U.S. companies to do so in order to better protect data in transit, at rest, in the cloud and other storage. I think that is a pretty good recommendation.

And I would like to close my remarks with some of the quotes from Ms. Hess' written testimony: "Following the rule of law and upholding civil liberties and civil rights are not burdens. They are what make all of us safer and stronger." I couldn't agree more with that.

And, again, I started in the CIA in October of 2000. And on September 12, I was the fourth employee in the unit that prosecuted the war in Afghanistan and helped infiltrate Americans into Afghanistan to bring Al Qaeda and the Taliban to justice for their acts of terrorism on our shores.

And if somebody would have told me on September 13 that it would be 14 years prior to an attack happening on our homeland again, I would have said you are absolutely crazy. And the reason nothing has happened these last 14 years is because our men and women in the intelligence community, in law enforcement, are acting as if it is September 12, 2001, every single day. The velocity that that requires, the dedication, the countless hours of sacrifice, is incredible, and I applaud everyone for that.

But that is why I hold everyone in the law enforcement intelligence community to a higher standard and that upholding civil liberties and civil rights are not burdens. They are what make all of us safer and stronger.

And this is a good conversation, but I would recommend or comment that any other future proposals or comments that are going to come before this body will be carefully scrutinized by this committee, by many of our colleagues, because we can protect our country and our civil liberties at the exact same time, and that is what we must do.

So I want to thank all of you all for your time today and this conversation. I think it is always helpful. This has helped me better understand my opinions on this topic. And I would like to thank our witnesses for taking the time to appear before us today.

If there is no further business, without objection, the subcommittee stands adjourned.

[Whereupon, at 4:28 p.m., the subcommittee was adjourned.]