

S. HRG. 114-905

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

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JULY 8, 2015

Serial No. J-114-22

Printed for the use of the Committee on the Judiciary



*www.judiciary.senate.gov
www.govinfo.gov*

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

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

HEARING
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JULY 8, 2015

Serial No. J-114-22

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

ORRIN G. HATCH, Utah	PATRICK J. LEAHY, Vermont, <i>Ranking</i>
JEFF SESSIONS, Alabama	<i>Member</i>
LINDSEY O. GRAHAM, South Carolina	DIANNE FEINSTEIN, California
JOHN CORNYN, Texas	CHARLES E. SCHUMER, New York
MICHAEL S. LEE, Utah	RICHARD J. DURBIN, Illinois
TED CRUZ, Texas	SHELDON WHITEHOUSE, Rhode Island
JEFF FLAKE, Arizona	AMY KLOBUCHAR, Minnesota
DAVID VITTER, Louisiana	AL FRANKEN, Minnesota
DAVID PERDUE, Georgia	CHRISTOPHER A. COONS, Delaware
THOM TILLIS, North Carolina	RICHARD BLUMENTHAL, Connecticut

KOLAN L. DAVIS, *Majority Staff Director*

KRISTINE LUCIUS, *Minority Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Grassley, Hon. Charles E.	1
Prepared statement	55
Leahy, Hon. Patrick J.	3
Prepared statement	57

WITNESSES

Comey, James B.	7
Prepared statement	59
Responses to written questions	146
Lin, Herbert, Ph.D.	34
Prepared statement	93
Responses to written questions	157
Swire, Peter	36
Prepared statement	124
Responses to written questions	158
Vance, Cyrus R., Jr.	32
Prepared statement	71
Responses to written questions	160
Yates, Sally Quillian	6
Prepared statement	59
Responses to written questions	151

APPENDIX

Items submitted for the record	53
--------------------------------------	----

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

WEDNESDAY, JULY 8, 2015

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

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

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

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

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

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

The core of the Fourth Amendment is the requirement that, with limited exceptions, when a law enforcement officer is investigating a crime, the officer must obtain an individual warrant or a court order to conduct a search that would violate a person’s reasonable expectation of privacy. That order must be issued by a neutral and detached judge based on facts that demonstrate probable cause. Through this brilliant framework, for over 200 years now, our constitutional system has preserved the rule of law, ensured our public safety is maintained, and protected our individual privacy and civil liberties in part through the separation of powers. Recently, promi-

ment law enforcement officials have been questioning whether the laws Congress has enacted over the years to adapt that framework to changing technology, such as the Communications Assistance for Law Enforcement Act—and I will call that “CALEA,” as it is known around here—whether or not that is adequate to the task for today.

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

First, they report a decreasing ability to intercept real-time communications, such as phone calls, emails, texts, and other kinds of so-called data in motion. Second, they relate a similar concern regarding their inability to execute search warrants on encrypted phones, laptops, and other devices, which store what they refer to as “data at rest.”

Companies are increasingly choosing to encrypt these devices in such a way that the company itself is unable to unlock them, even when presented with a lawful search warrant. These encrypted devices, they fear, are becoming the equivalent of closets and safes that can never be opened, even when a judge has expressly authorized a search for evidence inside them. In their view, this development has the potential to impact the fair and impartial application of our laws by effectively placing certain places, and, therefore, certain people, outside of the law. These officials describe the cumulative effect of these changes on their ability to do their jobs as “Going Dark.” It is not a new issue. According to them, it is a problem that is getting dramatically worse, and it is having a real effect on their ability to protect the public and to bring criminals to justice.

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

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

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

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

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

I know many of our privacy and technology communities are highly skeptical that any reform can be accomplished without unacceptably undermining both the privacy interests of our citizens as well as the international competitiveness of our technology companies. These are, no doubt, fundamental important considerations. As a start, we need to have an open and honest conversation that examines the costs and benefits both of potential reforms, as well as continuing down the path we are headed. We need to do so with humility and respect for those who come to the issue from different perspectives.

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

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

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

[The information appears as a submission for the record.]

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

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

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

We know how the internet has transformed the lives of Vermonters and all Americans over the last 20 years. We use it to communicate, make financial transactions; we get our medical records, we file taxes. We store personal information, and I cer-

tainly store an awful lot of photographs I have taken, including photographs of both of you.

Critical to the digital revolution has been the development and use of strong encryption. Ensures that if we send or store electronically—and I am thinking now of financial records and medical records and things like that—it is protected against hackers or criminals or spies. We also know that it is creating problems for law enforcement.

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

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

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

In the 1990s, I opposed efforts to regulate the development of encryption technology. I was concerned that if you regulated encryption, you are going to stifle innovation, you would harm American businesses, you would impede technological advancement, undercut security, and, of course, all our competitors worldwide would just go ahead and do it anyway, and we would be left behind.

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

Chairman GRASSLEY. Without objection.

[The information appears as a submission for the record.]

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

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

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

Chairman GRASSLEY. Without objection.

[The information appears as a submission for the record.]

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

Thank you.

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

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

Our second witness is FBI Director James Comey, and I often say how smart he is because he married a girl from Iowa. Mr. Comey took over the leadership of the FBI in 2013. He previously served under President George W. Bush as Deputy Attorney General, U.S. Attorney for the Southern District of New York, and Managing Assistant U.S. Attorney in the Eastern District of Virginia. Between his careers in public service, Mr. Comey was general counsel at Lockheed Martin and worked at a hedge fund. Mr. Comey is from New York, received his undergraduate degree from William and Mary, and went to law school at the University of Chicago.

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

Deputy Attorney General YATES. I do.

Director COMEY. I do.

[Witnesses are sworn in.]

Chairman GRASSLEY. Thank you.

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

**STATEMENT OF HON. SALLY QUILLIAN YATES, DEPUTY
ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE,
WASHINGTON, DC**

Deputy Attorney General YATES. Good morning, Chairman Grassley, Ranking Member Leahy, and Members of the Senate Judiciary Committee. Thank you for this opportunity to talk with you this morning about the information and collection problem that we commonly refer to as “Going Dark.” I think that Senators Leahy and Grassley’s statements this morning really pointed out a number of the difficult issues surrounding this problem.

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

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

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

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

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

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

The need and the justification for the evidence has been established, and yet that evidence cannot be accessed. Critical information becomes, in effect, warrant-proof. Because of this, we are creating safe zones where dangerous criminals and terrorists can operate and avoid detection. It impacts us in two ways: We cannot get access to information that is stored on someone’s smartphone, like a child pornographer’s photographs or a gang member’s saved text messages. This is known as “data at rest.” We also at times can no longer effectuate wiretap orders to intercept certain communications as they happen, like ISIL members plotting to carry out

an attack in the United States or a kidnapper communicating with co-conspirators. This is known as “data in motion.”

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

The current public debate about how to strike the careful balance between private rights and public safety has at times been challenging and highly charged. I believe that we have to protect the privacy of our citizens and the safety of the internet. Those interests have to be balanced against the risks that we face from creating warrant-proof zones of communication.

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

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

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

I look forward to answering your questions.

[The prepared statement of Deputy Attorney General Yates appears as a submission for the record.]

Chairman GRASSLEY. Thank you, Ms. Yates. Director Comey, thank you.

**STATEMENT OF HON. JAMES B. COMEY, JR.,
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION,
WASHINGTON, DC**

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

As Senator Leahy said, I have heard lots of folks refer to what went on 20 years ago as the “Crypto Wars.” I am not looking to fight a war. I am not up here trying to win anything. I think the folks involved in this conversation in the private sector and in the Government care about the same things. I care deeply—it is part

of my job, it is also part of my life—about security on the internet. One of our primary responsibilities at the FBI is cybersecurity. Encryption is a great thing. It keeps us all safe. It protects innovation. It protects my children. It protects my health care. It is a great thing.

We also care about public safety. That is what I have devoted my life to. That is what Sally Yates has devoted her life to. I think all Americans care about the same things. There is not a war being fought here. There is, I hope, a conversation among serious people to figure out is there a way to maximize both, to keep ourselves secure on the internet and, as best we can, to keep ourselves safe in our streets and our communities, because I do believe, as the Deputy Attorney General has said, we stand at an inflection point. There has always been a crypto discussion, but the world has changed in the last 2 years. Decryption has moved from being something available to something that is the default, both on devices and on data in motion, as you said, Mr. Chairman. We are moving inexorably to a place where all of our lives, all of our papers and effects, all of our communications will be covered by universal strong encryption, and that is a world that in some ways is wonderful and in some ways has serious public safety ramifications. I hope we can have a conversation about that before we get to that world and people start looking at us and saying, “What do you mean you cannot? What do you mean you cannot do what we pay you to do?”

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

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

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

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

Thank you for this opportunity.

[The prepared statement of Director Comey appears as a submission for the record.]

Chairman GRASSLEY. Thank you both for your testimony.

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

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

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

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

Director COMEY. Thank you, Mr. Chairman. I think the American people need to know the terrorism threat today is very different. Al-Qaeda, before 9/11 and in the years after 9/11, was focused on the national landmark, multi-pronged sophisticated attack where they would carefully select operatives, put them in place, train, surveil over many, many months or years.

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

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

I have investigations in all 50 States of people who are consuming this stuff. It is buzzing in their pocket all day long, and they are trying to seek meaning in some sick way, and they are responding to this. Then they disappear and move over to mobile messaging apps. This is an enormous problem. It is very different. Al-Qaeda would never vet an operative by tasking them. ISIL says, "Go kill, go kill, and here is a list of military members you can go kill. Go do it."

We are stopping these things so far through tremendous hard work, the use of sources, the use of online undercovers. It is incredibly difficult. I cannot see me stopping these indefinitely. I am not trying to scare folks. I just want people to know this is a change

in my world, in the top responsibility of the FBI, that implicates this going dark problem, they come together. I really think we have to talk about it.

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

In January, the President acknowledged that, quote, “The laws that might have been designed for the traditional wiretap have to be updated,” end of quote. Yet this administration still has not come forward with a legislative proposal.

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

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

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

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

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

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

Chairman GRASSLEY. Okay. Senator Leahy.

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

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

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

Chairman GRASSLEY. Oh, yes, without objection.

[The information appears as a submission for the record.]

Senator LEAHY. Okay.

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

Deputy Attorney General YATES. That is right. We are not suggesting a legislative solution today. That may ultimately be necessary, but we are hopeful that it will not be.

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

A group of the world's leading computer scientists issued a report detailing the significant security risk, as they see it, of providing special law enforcement access to encrypted data. That is this report. They concluded that the security risks are even greater now than they were in the 1990s when we first debated this. The report highlights that the technical challenges have become even more difficult, and multiple countries seek their own methods of access. We learned what happened with OPM, the hack that affected millions of Federal workers and reduced confidence in the Government being able to protect data. I know the device encryption presents a different set of security issues.

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

Deputy Attorney General YATES. Absolutely, Senator. We do have to carefully consider it.

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

Senator LEAHY. I remember when we had a debate in this Congress on the illegal sale of content on the various companies that have websites and how upset they were and got everybody all upset that we were somehow delving into their personal information, and so the legislation went nowhere. Then about a week later, it turned out one of the biggest of those companies was data mining their

own customers, the sort of things they were warning them about, because they were selling ads.

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

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

[The information appears as a submission for the record.]

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

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

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

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

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

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

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

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

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

Consumers have, understandably, demanded greater privacy protections, and tech companies have responded to this by offering very strong encryption in the services that they offer.

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

is, of course, Congress' job, it is Congress' duty to consider any appropriate solutions.

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

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

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

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

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

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

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

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

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

Deputy Attorney General YATES. There has been an evolution—very recently, but there has been an evolution—where, yes, some companies do not retain access either to data in motion or data at rest. What that means, for example, if we were to get some phones, some cell phones, it is essentially a brick to us. We cannot access any of the information on that phone. That is a problem for a number of reasons. We know pedophiles, for example, those who are exploiting children, maintain their information, maintain the photographs and records of the children they are abusing on their phones. We cannot get that information, we cannot identify other victims, and we cannot identify others who are abusing and exploiting children because we cannot get access to that device. We cannot get it because the company no longer has access to that device.

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

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

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

Senator FEINSTEIN. Thanks very much, Mr. Chairman.

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

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

I actually think she is correct. I think this is a most serious problem, and I myself, who represents Silicon Valley, have tried to

interact with them. In May, I met with the general counsels from several of the major internet and social media companies, to include Google, Facebook, Yahoo, Twitter, and Microsoft. I met in California; also the general counsel from Microsoft came back to meet me here in Washington. That was to discuss the terrorists' use of their products to recruit, inspire, and direct attacks. I would like to just tell you what I understand the companies are doing.

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

I think, as you have suggested, Director Comey, that there really are grounds to have these discussions and would like to suggest that you pull together the CEOs of these big companies and say directly to them what you have said to us. I have no question from an intelligence point of view supporting virtually every one of your words. You are absolutely correct, because where we are going is to allow those who would do us enormous harm a respite from any kind of interaction with law enforcement. That is the black situation that is increasingly existing.

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

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

Director COMEY. Yes, Senator.

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

Let me ask a couple of questions. If the FBI was aware of communications happening on messaging apps, regardless of whether those apps are used on Apple or Android devices, what judicial process is currently available to obtain those communications?

Director COMEY. In theory, a court order from a judge in a criminal case under Title III or a court order from a judge in a national security intelligence case. If the data is strongly encrypted, we can collect it, but it will be gobbledygook.

Senator FEINSTEIN. What you are saying—

Director COMEY. Strong encryption—

Senator FEINSTEIN [continuing]. Is you have no recourse—is that right?—if the data is encrypted, currently, for a national security concern, to obtain that data.

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

Chairman GRASSLEY. Senator——

Senator FEINSTEIN. Mr. Chairman.

Chairman GRASSLEY. Go ahead.

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

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

Senator FEINSTEIN. Thank you.

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

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

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

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

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

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

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

Deputy Attorney General YATES. That is absolutely right.

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

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

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

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

Director COMEY. Thank you.

Senator TILLIS. Or need.

Director COMEY. Sorry for the gobbledygook in my head.

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

Director COMEY. The encryption is a piece of a broader problem we call going dark. Sometimes going dark includes just our ability to get companies to comply, who have the capability, to comply with the laws that exist today. That is actually a significant issue we face where folks could do it but they say, “We are not going to do it.” We are faced with a dearth of a lack of enforcement mechanisms.

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

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

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

Chairman GRASSLEY. Senator Whitehouse, and then Senator Cornyn.

Senator WHITEHOUSE. Thank you.

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

Deputy Attorney General YATES. Before the evolution of the type of encryption that we are talking about today, the company would have retained access, the ability to be able to open the phone, and so—

Senator WHITEHOUSE. The company would have done that.

Deputy Attorney General YATES. The company would have. We would have had to have gotten a warrant for the company to then open the phone—

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

Deputy Attorney General YATES. We could, and that is all we are seeking now is for the company to have the ability to be able to open the phone.

Senator WHITEHOUSE. They have made the essentially unilateral decision not to—or actually to close off that access, correct?

Deputy Attorney General YATES. Some companies have, and some still retain that access, yes.

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

Director COMEY. Senator, I am sure that we have a record of it. I cannot sit here and give you chapter and verse on it, but—

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

Director COMEY. Sure, and we would be happy to give you that.

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

Director COMEY. Yes.

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

I do not know if you have undertaken that, but if you have, I would appreciate it if you would share that with us, and if you would consider doing it, I think that might be helpful to us.

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

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

Deputy Attorney General YATES. That is certainly one way to look at it, and perhaps the companies have done greater analysis on that than we have. It is certainly something we can look at.

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

Chairman GRASSLEY. Thank you, Senator Whitehouse.

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

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

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

Director COMEY. Senator, we are going to do, as we do every day—I do nothing. I lead a remarkable organization. I have a whole lot of people who do a lot every day to do everything they can to make sure that does not happen. As I said, the tools we are given are the ones the American people give us through you. Whatever we have, we will work 24 hours a day to make sure that does not happen. I just think it would be irresponsible for me not to come to the Committee and say I see this tool, its effectiveness diminishing steadily, and I can imagine a future where it is useless to me. I am left having to follow people physically to see if I can tell what is in their head, trying to get undercovers in to talk to them or sources in to talk to them. We will do all of that.

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

Senator CORNYN. It certainly raises the risk.

Director COMEY. Yes, it sure does.

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

Director COMEY. You can assert a Fifth Amendment right not to answer the question, and then if—

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

Director COMEY. No. I think it is what they call black letter law that the grand jury is entitled to every man's—every person's evidence.

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

Director COMEY. Yes, sir.

Senator CORNYN. It strikes me that there may be some way of—just trying to think about the framework in which we ought to look at this—it strikes me as irresponsible, and perhaps worse, for a company to intentionally design a product in such a way that it prevents them from complying with a lawful court order, which is what Ms. Yates said you are seeking, a means to allow a response to a lawful court order. If you intentionally design a product in such a way that it prevents you from complying with a lawful court order, it strikes me that it is not a lot different. Maybe that is just food for thought. We ought to let that roll around in our brains awhile and think about that. I think we need to think about how

to think about this and not in sort of any absolutist terms that will result in a higher risk of people being actually successfully targeted by ISIL here in the homeland, and then just responding after the fact, which I know you do not want to do and we do not want to do either.

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

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

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

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

[The information appears as a submission for the record.]

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

Chairman GRASSLEY. Senator Franken.

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

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

Network and data security protect not only individuals' personal and financial privacy, but also protect the well-being of our critical infrastructure and the industries that drive our economy. With each new story about a cyber attack or breaches, Americans learn more about just how significant a security interest that we have in strong encryption.

Before we or a regulatory body could really consider taking any kind of action in this arena, I think we first need to have a similarly clear understanding of the scope and the magnitude of law

enforcement's security interest. To this date, we have not seen any real data about how often encryption is thwarting investigations. Can you shed any light on that? If DOJ does not have numbers to share at this time, is that something that could be studied?

Deputy Attorney General YATES. Thank you, Senator. I want to tell you that we at the Department share your desire for strong encryption and share the desire that all of us in this country have for strong encryption.

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

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

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

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

I can tell you from personal experience it is happening, and it is happening every day, but we do not really have a mechanism—and I know that is frustrating for you, but we do not really have a mechanism to be able to give you numbers.

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

Deputy Attorney General YATES. Right, we do not go—we do not seek a warrant in a situation where we know we are not going to be able to get the information. We do not seek a wiretap when we know that it is encrypted and we know that we cannot get it.

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

Deputy Attorney General YATES. Right.

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

Deputy Attorney General YATES. I think you are right. If we do this wrong, it could potentially increase the risk, which is one of the reasons why we are not coming to you today with a one-size-fits-all solution, which is one of the reasons why we really want to work with the industry on a company-by-company basis of what is going to be the best way for them to be able to ensure that their information remains secure, but in those instances where we have a valid court order, that we are able to get the information we need there. I think you are right, we have got to do this the right way.

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

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

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

Chairman GRASSLEY. Go ahead.

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

You know, 230 years ago, I do not think James Madison ever envisioned the internet, but he struggled with this thing that we are struggling with today of the balance between public safety and personal privacy. I look at the technology being developed, and it seems to be coming at us faster and faster. Here we have apps, we have platforms. This encryption is a very serious thing, and yet 1994 was the last time we had any real legislative adjustment here. I think that was CALEA. You know, just to put that in perspective, that was when Navigator—Netscape Navigator was introduced in 1994. It was a long time ago. We know this is a tough question.

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

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

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

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

Director COMEY. Senator, I think that it is, as the Deputy Attorney General said, something that we have to work on urgently. I also agree it is an unbelievably complicated problem. The proliferation of innovation is a wonderful thing, but it also makes it hard to work with individual players because there is a new garage every single day, and there is a big international component to this that I get that we have to figure out how to untangle as part of this so we do not hurt American innovation.

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

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

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

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

My question is, with all of us working together, how could we maximize both? Is it really impossible? Is it really binary? If you do it at all, it is all going to fall apart? I find that hard to believe.

I know it was very hard in the 1990s. We have got a lot of smart people out there.

Senator PERDUE. Thank you again for what you are doing.

Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Hatch.

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

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

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

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

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

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

Senator HATCH. Thank you.

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

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

Deputy Attorney General YATES. Thank you, Senator. First, we are not going to ask the companies for any keys to the data. Instead, what we are going to ask is that the companies have an ability to access it and, then with lawful process, we be able to get the information. That is very different from what some other countries, other repressive regimes, from the way that they are trying to get access to the information. I know that there is concern, for exam-

ple, that if there is an ability here in this country for the companies to be able to access the data, that other countries such as China will require the same thing. In China and other countries, they do not follow the same lawful process that we do here. If they did, then they could potentially get the same information. China's system is not set up that way.

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

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

Deputy Attorney General YATES. That is the reason why we are not going to ask for the keys.

Senator HATCH. That is the big reason—

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

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

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

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

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

Senator HATCH. My time is up, and I want to thank both of you for appearing here today.

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

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

There has been some discussion, I know—first of all, thank you both for your great work. I really appreciate your service to our Nation, and on this issue particularly, which is complex and chal-

lenging and I think offers no simple or simplistic answers, and I appreciate your addressing it as thoughtfully as you have.

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

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

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

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

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

Director COMEY. I think America has a unique ability to drive this discussion because we are the source of the innovation, and that is the beauty of this amazing country. It is here. The providers are here. Most of the clever apps are here. It is all here. What we do matters enormously, which is why it is so important, as the Deputy Attorney General said, that we get it right, because the rest of the rule-of-law countries, especially our colleagues in Europe, will be strongly influenced by that model.

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

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

Deputy Attorney General YATES. It is certainly a potential solution perhaps down the road, but we do believe that it is important now, rather than seeking a legislative fix that is across the board, that we try to work with the individual companies, because what works for Apple might not be the best solution for another of the communication providers. We really think they know their systems best. They know the way they can maximize privacy and internet security while still being able to comply with lawful court orders.

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

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

Senator BLUMENTHAL. Can we, in this body, be helpful?

Deputy Attorney General YATES. Certainly to the extent that you can encourage the industry to work with us to try to find a solution that accommodates all of these really critically important interests, I think that would be welcome.

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

Chairman GRASSLEY. Senator Flake.

Senator FLAKE. Thank you, Mr. Chairman. Thank you for the thoughtful testimony and willingness to come here and speak in a classified setting as well. I just like the tone of this discussion because it really is in search of a solution here.

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

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

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

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

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

sponse given that scenario if we do decide that we just cannot go there?

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

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

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

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

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

Director COMEY. I cannot think of a case off the top of my head. I am sure that we can find one. The evidence is important both to find the guilty and to clear others who have fallen under suspicion, so logic tells me that in every case where I cannot get access to evidence, I cannot do either of those things. Someone who the finger is pointed at we will not be able to clear, just as we will not be able to figure out who the bad guy really is. I bet we can come and find you cases where devices have been used to say so-and-so was not at the shooting actually, we can prove through texts or something that he was at home with his mother, so he is actually not guilty of this crime.

Chairman GRASSLEY. Senator Lee, then Senator Franken.

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

In that circumstance, how do you think the manufacturer of this safe, this safety deposit box, might react if told or strongly encouraged perhaps by the Government that it needed to provide a back door? Similarly, how do you think the people who owned those safe-

ty deposit boxes would feel upon learning that somebody at the corporate headquarters or the manufacturer had a back-door method into it and that somebody working there perhaps could take that information with them and sell it to the highest bidder?

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

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

Senator LEE. You would blow it up.

Director COMEY. You would blow it up. There is not a safe—I do not know of a safe in the world that cannot be opened.

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

Director COMEY. That would be the end of the data, too. That is my reaction, which is I think ordinary Americans, when they hear this, think so long as it is pursuant to the Fourth Amendment, it is okay to live in a world where a judge can make a showing of probable cause and issue a warrant to get access to a safe or to a phone. I do not exactly know where the great demand for this is coming from. I have not met ordinary folks who say, “You know what? I really want a device that cannot be opened, even if an American judge finds that it ought to be opened because it is really important.”

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

Chairman GRASSLEY. Senator Franken, and then, Senator Tillis, would you signal me if you want a second round? Because—you do not? You do not want a second round, OK. Senator Franken.

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

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

judge gives us permission, to be able to get into a room or get into a device.

Senator FRANKEN. Okay. Fair enough.

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

Deputy Attorney General YATES. Certainly, Senator, we can work on ways where we try to gather information to be able to answer your question about how big of a problem is this, whether it is numbers or more specific examples to be able to do that, because this is the first time that we have really encountered warrant-free zones. This is new for us. We are grappling ourselves with how—not only to get our arms around the problem, but how to quantify the problem as well.

Senator FRANKEN. Okay. Thank you. Thank you both. Thank you, Mr. Chairman.

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

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

[Pause.]

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

Mr. VANCE. I do.

Mr. LIN. I do.

Mr. SWIRE. I do.

[Witnesses are sworn in.]

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

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

Dr. Herbert Lin, who is senior research scholar of cyber policy and security at the Center for International Security and Cooperation and research fellow at Hoover Institution, both at Stanford University. Dr. Lin is also chief scientist emeritus for the Computer Science and Telecommunications Board at the National Research Council of National Academies where he served 1990 through 2014. Dr. Lin also served as a professional staff member

and staff assistant to the House Armed Services Committee. He received his doctorate in physics from MIT.

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

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

**STATEMENT OF HON. CYRUS R. VANCE, JR.,
DISTRICT ATTORNEY, NEW YORK COUNTY,
NEW YORK, NEW YORK**

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

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

I would like to address two of the questions, Mr. Chairman, that were alluded to today: How should we balance the benefits, the clear benefits of encryption technology and privacy rights with the responsibilities we have in law enforcement to protect victims' rights? Second, who gets to decide that balance?

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

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

It is undisputed that phones are used by criminals committing murders, rapes, and robberies, and most of the thousands of felonies we prosecute each year, and that key evidence is on those phones. At this time, it is unfortunate, but criminals are literally

and figuratively laughing in the faces of law enforcement. That is not hyperbole. I would like to give you a real example from a case in my office where a defendant in jail for a felony case is speaking with his friend on a recorded landline outside of jail. I am here quoting from the transcript.

“Apple and Google came out with these softwares that can no longer be unencrypted by the police. If our phones are running on the iOS 8 software, they can’t open my phone. This may be another gift from God,” end of quote.

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

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

Like everyone here, all the prior speakers, I value my privacy. I understand there is a fear of mass security breaches, collection of bulk data, and warrantless surveillance. I believe, Mr. Chairman, that those are valid and legitimate concerns. That is not the access local and State law enforcement seeks or expects. Our access to electronic data is grounded in and it is limited by the Fourth Amendment to our Constitution authorizing only reasonable searches based on probable cause, supported by a particularized search warrant, and only after approval by a neutral judge.

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

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

As it stands today, Apple and Google have decided who can access key evidence in criminal investigations. I do not and I cannot believe it is right that they should decide the path toward justice for victims around the country or for our Nation as a whole. I do not think by default we should cede this important decision to the

tech industry. Senators, I believe this decision should and must be yours.

Thank you for the opportunity and the honor of addressing you. [The prepared statement of Mr. Vance appears as a submission for the record.]

Chairman GRASSLEY. Thank you, Mr. Vance. Now, Dr. Lin.

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

Dr. LIN. Mr. Chairman, Senator Franken, Members of the Committee, thank you for inviting me to testify today. I have worked on cybersecurity issues for many years, mostly at the National Academies, now at Stanford, but the views I present today are my own. The previous panel discussed going dark, and I want to address three issues here.

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

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

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

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

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

Would a similar approach work in analyzing a proposed NOBUS mechanism? I think so, but I could be wrong about that. That is what makes it a research problem. We need to assess whether such methodologies can be usefully applied to estimate how long it

might take for a bad guy to hack any specific mechanism. The Government has not provided any specifics, arguing, as we heard in the last panel, that the private sector should do it. At the same time, the vendors are not interested in doing it because their customers are not demanding such access. Many of them do not think it is possible to do anyhow.

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

Exactly the same issues came up in the 1990s, only then the Government did propose a specific mechanism. When the National Academies studied the problem then, it made a recommendation that still makes sense today: a prerequisite for going down this path is for the Government to gain experience about how to properly operate a Government-only system allowing such access, before deploying it on a large scale. If you do it without that experience, deploying it on a large scale across the entire Nation is just asking for trouble.

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

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

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

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

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

[The prepared statement of Dr. Lin appears as a submission for the record.]

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

Professor Swire.

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

Professor SWIRE. Thank you, Chairman Grassley and Members of the Committee, for the opportunity to testify today.

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

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

First, the Review Group, after top secret briefings on encryption issues, concluded that strong cybersecurity and strong encryption should be vital national priorities. Our recommendation stated, quote, "We recommend that, regarding encryption, the U.S. Government should fully support and not undermine efforts to create encryption standards; second, we should not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and, third, increase the use of encryption and urge U.S. companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."

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

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

Let me emphasize that I agree there are specific ways that law enforcement and national security agencies lose specific previous capabilities due to changing encryption technology. As electronic

communications and evidence evolves, there will indeed be certain categories of information that are no longer available.

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

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

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

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

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

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

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

Chairman Grassley asked whether changing technology is upsetting the balance between public safety and privacy. For reasons stated here, the balance has indeed shifted in the last 25 years, clearly in the direction of law enforcement having the evidence it never had before in human history.

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

[The prepared statement of Professor Swire appears as a submission for the record.]

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

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

Senator FRANKEN. Thank you, Mr. Chairman. Would it be OK, since I——

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

[Laughter.]

Senator FRANKEN. I know your mom watches these things on the web.

[Laughter.]

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

Let's see what I have here. Dr. Lin, thank you for your testimony. It is clear that this difficult issue is not just about hardware. Director Comey and Deputy Attorney General Yates spoke this morning about the availability and use of end-to-end encrypted messaging apps. Even if all U.S. device manufacturers agreed to maintain the ability to give the Government access, there would still be developers offering fully encrypted programs or apps, whether authorized or unauthorized.

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

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

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

Senator FRANKEN. That would affect that industry.

Dr. LIN. It certainly would not do it any good.

Senator FRANKEN. Okay. It would have a negative effect.

Professor Swire, to maintain our global competitiveness, it is crucial that American tech companies have access to European markets. Given your role years ago in development of the safe harbor agreement to allow data to flow between the EU and the U.S., I

imagine you may be uniquely positioned to offer thoughts on the effect of requiring U.S. companies to issue full encryption might have on their ability to compete abroad. What would the ramifications of this be, do you believe?

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

The magnitude of this, when you talk to people in the field, has been much greater than people anticipated. It is continuing, and the encryption debates that are happening now reinforce the tendency in other countries to say stay away from U.S. products.

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

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

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

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

Mr. VANCE. I very much appreciate—

Senator FRANKEN. Turn on your mic.

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

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

I do not want the Committee to believe that this is simply a Federal issue, that it deals with a limited number of cases. Indeed, the

impact is going to be around the country and at the local level of all the citizens.

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

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

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

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

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

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

Mr. VANCE. Thank you, sir.

[Whereupon the hearing was recessed and reconvened.]

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

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

Question: Is metadata a good substitute for the content of communications in your investigation? Are either relying on access to cloud storage or obtaining passwords from users unrealistic options for State and local law enforcement? Your reason why or why not.

Mr. VANCE. Thank you, Mr. Chairman.

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

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

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

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

Another statistic, Senator, you were out when I gave it: We have started to monitor since September 14 the number of phones that come into our own lab at the D.A.'s office, and we have to do a part of the forensics for our phones because we have so many. Of the roughly 92 iPhone 8's that came in in that time period, 70-plus of them were locked. That means of that 70, we were really unable to move toward getting access to the contents. That includes crimes of murder and everything else.

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

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

Chairman GRASSLEY. Dr. Lin—and then I will have a question for Professor Swire—in your testimony you proposed a method to test the risks associated with providing built-in law enforcement access to encryption. You suggest that this type of risk analysis might help to move the public debate forward. Yesterday, a group of noted cryptographers and security experts also issued a report opposing law enforcement access to encrypted systems, but also posing certain questions and technological requirements for such a system.

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

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

The approach that I am wanting to take is to see—to apply a certain methodologies to see how long an exceptional access system, a NOBUS system, could be resistant to a bad guy hacking it, how long it would take. As I say, if the analysis comes out that it takes 30 seconds, then it is a silly idea, that that mechanism is a silly idea. If it takes 1,000 years, then maybe that is good enough. You want to be able to do the analysis to see where the number comes out.

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

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

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

Continuing to quote, “In 1999, the U.S. Government concluded that strong encryption was precisely that type of valuable tech-

nology. It was worth going at least slightly dark in order to reap the many benefits of effective encryption,” end of quote.

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

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

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

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

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

The point to Mr. Vance’s very sensible concerns from law enforcement—and as a junior lawyer, I worked in the Manhattan D.A.’s office. I have great respect for the history of that office and all that it does. I think in terms of metadata helping, one thing metadata helps is to reveal co-conspirators, who is everybody you called and texted and emailed. In the old days, if you turned one co-conspirator in a criminal investigation, maybe you could get him to testify. Today, if you have a co-conspirator, you can give that person use immunity and compel them on pain of jail time to open up their phone for you, and then all the contents of everything they said to the main suspect are there plain for you to see.

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

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

If I may—

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

Mr. VANCE. Actually it is a case that we spoke about with Federal colleagues. There are individuals who maintain content on their phone that is so incriminating and disturbing that, if given the option between an order by the court to—an order including immunity, some kind of immunity, use immunity to open the phone or contempt, the choice would be not to open the phone, number one.

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

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

There are a lot of doomsday scenarios that are being portrayed about hacking, and I think all those should be taken seriously. It has yet to be identified what exactly was insecure about iOS 7 when in that format the Government—the company maintained a digital key as well as the user.

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

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

[Laughter.]

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

Senator Whitehouse.

Senator WHITEHOUSE [presiding.] Thank you very much, Chairman Grassley. Let me welcome District Attorney Vance particu-

larly here. I appreciate how busy the Manhattan D.A. is, and clearly it is a key matter for you when you have taken the trouble to prepare your testimony and come down here, and I appreciate it.

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

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

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

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

Mr. VANCE. To date, they have not been answered, and the question I asked to both, and I am quoting from the letter, “If Google kept a key so that it was able to unlock phones, would the phones be more vulnerable to hackers than if Google had no structure key? Is there a key or similar device that Google might keep without sacrificing the security of Android devices from hackers? Is there a way to measure or quantify the vulnerability of hackers of Android phones, A, if Google kept a key as compared to, B, if it did not keep a key?” These, Senator, respectfully, I think are the questions that need to be answered in order to have an accurate assessment about industry’s claim that they are going to be made unduly vulnerable and law enforcement’s desire to gain access to evidence.

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

Mr. VANCE. Thank you.

Senator WHITEHOUSE. You also run an office that has an unusually wide array of offenses that you prosecute, everything from very simple low-level street crime to very significant financial fraud to national security investigations. Clearly, you have mentioned a couple of things. You have mentioned time-sensitive investigations, a kidnapping or a child snatching where you need quick access to all the information you can. You have mentioned investigations where the content itself on the phone is criminal—pictures of child abuse and so forth. I know you have a vivid concern about national security.

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

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

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

When the door knock was heard, the young man with the phone, a father of two, turned his phone to the door, and in the door you could see on the iPhone a picture of a man with a gun. The man filming was shot and killed by the man with the gun whose picture is on the iPhone video. The iPhone video drops, the phone drops, and records the voice of the shooter threatening everyone in the room what he will do to them if they go to police—iOS 6. If that had been iOS 8, when that phone had dropped, the passcode to the phone would have died with its user. We would not have been able to obtain the actual killing itself memorialized on a video on the phone. We were able in that instance to obtain it, and he was sentenced to 35 years to life after he was successfully prosecuted.

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

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

This is the State court experience every day in 3,000 counties around the country. I have always thought it was ironic, personally, that the victims, the true victims of this security upgrade preventing search warrants to be executed on phones, the true victims are going to include the customers of Apple and Google themselves, who are going to be victims of crime and are going to be unable to have law enforcement access to phones of the conspirators that would prove they are the victims of crime. At the end of the day,

Senator, I think this is a matter of such significance that it is a policy question which has to be decided by you, the lawmaker. It should not be, in my opinion, up to industry to say this is where we draw the line on access to information which we know may be critical not just on national security but on protecting our citizens in every city and town across the country.

Senator WHITEHOUSE. I would add particularly if they have no liability for what goes wrong and only the benefit for being able to market this technology.

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

Does NOBUS mean something different than what I just described?

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

Senator WHITEHOUSE. That is not what anybody is asking for here. What we are asking for, at least to the extent that there is an ask on the table to be debated, is that there be a mechanism that has been the case heretofore where the company itself maintains access to the information and then yields it only when a judge has signed a search warrant that allows that information to be shared with law enforcement because law enforcement has proven probable cause that evidence of a crime is contained in that information.

Dr. LIN. Under the circumstances you describe, the only purpose of asking the company to—of requiring the company to do it is, in fact, to provide Government access. That is the scenario that you just proposed.

Senator WHITEHOUSE. Yes.

Dr. LIN. Effectively it does count, because the company itself by assumption has no reason to want to get to its data.

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

Dr. LIN. Fair enough.

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

Dr. LIN. Sir, with the—

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

Dr. LIN. I agree with you that if the world were adjusted in such a way that they did have liability, the business interests change. I think that is what you are proposing, and I think——

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

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

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

Dr. LIN. The idea is new to this debate, and I commend you for—you know, thank you for introducing that into this debate. It is worth studying.

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

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

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

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

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

Senator KLOBUCHAR [presiding.] Okay. Thank you very much. Sorry I was late. We were at the White House—always a good ex-

cuse—trying to save the EXIM Bank. I appreciate you guys still hanging around here after a long hearing.

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

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

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

Senator, first of all, like so many people here, I am an Apple/Google fan. I want to put that on the record. I wrote my remarks on an Apple laptop using Google Docs. I understand the value of what they do. I was very concerned when the iOS 8 came out and that marketing language was included on Apple's website. I think it does send a signal—it certainly sent a signal to me in law enforcement, and, by the way, I am not aware that Apple or Google had any dialog with law enforcement whatsoever before it conducted this upgrade to assess its potential impact. I was concerned. I addressed that concern to them directly when I traveled earlier this year, in March, to speak with them. I communicated it, and I do not believe that my conversations were enough to convince them to return to the status pre-iOS 8, which is really what ultimately I think was working. We had a system where, prior to September 2014, where I am not sure exactly what the risk was that was causing so much trouble. Apple has not identified how its phones were at risk on September 13th of 2014, but no longer at risk on September 17th of 2014. Part of the problem is you cannot get into the box. You are not really getting data about the impact of these matters by the company itself. What you are hearing is industry and experts saying this is going to have a big impact, this is—makes us much more vulnerable. I have yet to actually hear what was vulnerable about the Apple iPhone.

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

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

Senator KLOBUCHAR. Suppose they would have the technological ability if they changed their product?

Dr. LIN. If they did have the technological capability to, then I think they are obligated under all of the penalties that attend to

not complying. I do not think there is any question about it. I do not think that anybody has disputed that.

Senator KLOBUCHAR. Professor Swire.

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

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

When you see these very big flaws and bugs and breachers, customers start to expect an upgrade. What we have seen across the line from sophisticated customers wanting good security for their own products is better security than we had pre-Snowden. I think the Apple announcement, properly understood, is part of the upgrade the whole industry is trying to do because they found out they had flaws they did not know they had.

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

I understand this privacy concern, and that is why somehow allowing the law enforcement to get in to get this data and differentiating that from hackers and not equating law enforcement with hackers to me is the answer, because if you do not have law enforcement to go after the hackers, they are just going to keep doing it and finding new ways.

Professor SWIRE. The point that I am making is a security concern, not primarily a privacy concern, which is, are we going to have systems that we know can be compromised at scale? We want to build systems that are not subject to that. We saw a lot of public reporting—a lot of which I wish we had not had as public report-

ing. We saw a lot of public reporting of hacks at scale, and the industry is responding by tightening up security.

Senator KLOBUCHAR. Mr. Vance.

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

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

[Laughter.]

There are many others: T.J. Maxx.

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

Senator KLOBUCHAR. Nordstrom's. Okay.

Mr. VANCE. I understand there is a theoretical concern, but it seems to me that from everything we know, Apple held on to these individualized keys in a way that was secure unless something has happened that I do not know about.

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

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

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

[Laughter.]

Senator KLOBUCHAR. Okay. Very good. I want to thank all of you, and I want to also thank you, Mr. Vance, for your good work on sex trafficking and what you have been doing.

Mr. VANCE. Thank you.

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

Mr. VANCE. Thank you also.

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

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

[Additional material submitted for the record follows.]

A P P E N D I X

Miscellaneous submissions:

Abelove, Joel E., letter	266
Alvarez, Anita, letter	275
American Civil Liberties Union (ACLU)	267
Application Developers Alliance, July 8, 2015	254
Association of Prosecuting Attorneys	303
Baker, Brooks T., letter	280
Baker, Jean Peters, letter	279
Brennan, Bridget G., letter	282
Brown, Richard A., letter	283
BSA/The Software Alliance	262
Budelmann, Jon E., letter	284
Cannizzaro, Leon A., Jr, letter	285
Civil Society Organizations, letter	193
Computer Science and Artificial Intelligence Laboratory Technical Report ...	221
Conley, Daniel F., letter	286
D'Amico, Joseph A.	293
Farrell, James R., letter	294
Ferman, Risa Vetri, letter	295
Fitzpatrick, William J., letter	296
Freeman, Michael O., letter	297
Gardner, Valerie G., letter	298
Grady, William V., letter	299
Gunning, Patricia, letter	300
Harms Caused by Edward Snowden	376
Hawk, Susan, letter	301
Heggen, Karen A., letter	302
Information Technology Industry Council and Accelerating Innovation in Technology, Data & Media	220
Intschert, Cindy F., letter	305
Jordan, J. Anthony, letter	307
Kane, Kevin T., letter	350
Kaye, David	199
Kelly, Raymond W., letter	352
Kilmartin, Peter F., letter	353
Lacey, Jackie, letter	354
LaHood, Nicholas "Nico", letter	355
Liberty and Security in a Changing World	164
Master, Daniel L., Jr., letter	356
Modafferi, Peter A., letter	357
Montgomery, Bill, letter	359
Moore, Hillar C., III, letter	361
Moore, Michael, letter	363
Murray, R. Andrew, letter	364

New America, Doomed to Repeat History	309
Pennsylvania District Attorneys Association	306
Purdue, Marsha King, letter	366
Rich, Ashley M., letter	367
Rundle, Katherine Fernandez, letter	368
Safehorizon, letter	369
Sarcone, John P., letter	372
Sedita, Frank A., III, letter	373
Singas, Madeline, letter	378
Stone, Isaac McDuffie, III, letter	380
Thomas, Tammy J., letter	276
Thompson, Jonathan F., letter	365
Thompson, Kenneth P., letter	381
Underhill, Rod, letter	382
Various organizations, letter	291
Weirich, Amy P., letter	383
Wetmore, Weeden A., letter	384
Williams, R. Seth, letter	385
Wolfson, Steven B., letter	386
Wong, Cynthia M.	264
Wylie, Andrew J., letter	387
Zugibe, Thomas P., letter	281

**Prepared Statement by Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Hearing On “Going Dark:
Encryption, Technology, and the Balance Between Public Safety and Privacy”
Wednesday, July 8, 2015**

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

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

What they have been telling us is that increasingly, even after they have obtained authority from a judge to conduct a search for evidence of a crime, they lack the technical means to do so. Director Comey and Deputy Attorney General Yates have recently spoken out about this issue, and I’ve heard about it from state and local officials in Iowa as well. They describe two distinct but related components to the problem. First, they report a decreasing ability to intercept real-time communications, such as phone calls, email, texts, and other kinds of so-called “data in motion.” And second, they relate a similar concern regarding their inability to execute search warrants on encrypted phones, laptops, and other devices, which store what they refer to as “data at rest.” Companies are increasingly choosing to encrypt these devices in such a way that the company itself is unable to unlock them, even when presented with a lawful search warrant.

These encrypted devices, they fear, are becoming the equivalent of closets and safes that can never be opened, even when a judge has expressly authorized a search for evidence inside them. In their view, this development has the potential to impact the fair and impartial application of our laws by effectively placing certain places, and therefore certain people, outside the law. These officials describe the cumulative effect of these changes on their ability to do their jobs as “Going Dark.” It’s not a new issue. But according to them, it’s a problem that’s getting dramatically worse, and it’s having a real effect on their ability to protect the public and to bring criminals to justice.

The reason for these sweeping changes isn't difficult to understand. Rapidly changing technology has made the way we store and communicate our personal data today quite different than in 1776 – let alone even five or ten years ago.

Today's revolution, then, is a technological one. It's a revolution that's resulted in a proliferation of new devices, networks, apps, and other modes of communication. And by leading this revolution, some of our finest American companies are enriching our lives. Through their ingenuity and innovation, they are allowing us to be in closer touch with our loved ones, sharing the things important to us in new ways.

However, as more of our lives have ended up on digital platforms, devices and on the internet, our data has increasingly become a target for hackers, criminals and foreign governments. We pick up the newspaper and read about breaches that have left personal data exposed almost on a daily basis. So we want our data to remain private and secure, and it's natural that companies seek to respond to this market demand. But at the same time, these wonderful technologies are also being employed by those who seek to do us great harm.

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

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

I know many in our privacy and technology communities are highly skeptical that any reform can be accomplished without unacceptably undermining both the privacy interests of our citizens as well as the international competitiveness of our technology companies. These are, no doubt, fundamentally important considerations. But as a start, we need to have an open and honest conversation that examines the costs and benefits both of potential reforms, as well as continuing down the path we are headed. And we need to do so with humility and respect for those who come to the issue from different perspectives.

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

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

**Statement of Senator Patrick Leahy (D-Vt.),
Ranking Member, Senate Judiciary Committee,
Hearing on “Going Dark: Encryption, Technology, and the Balance
Between Public Safety and Privacy”
July 8, 2015**

Over the past 20 years, the Internet has transformed the lives of Vermonters and the American people. We use the Internet to communicate, make financial transactions, access medical records, file taxes, and store personal information and photographs.

Critical to this digital revolution has been the development and use of strong encryption. Encryption ensures that the digital information we send or store electronically is protected against hackers, criminals, and spies. But as we will hear this morning, the increased use of encryption also presents challenges for law enforcement.

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

As a former prosecutor, I am sympathetic to these public safety concerns. Encryption can impede investigations by federal, state and local law enforcement officials. So this is an important discussion for us to have. But as we learned in the 1990s, this is a complicated problem with no easy solutions.

Some have suggested that technology companies should build special law enforcement access into their systems. But we also have to consider the risks of this approach. Strong encryption has revolutionized the online marketplace and protects American businesses and consumers from cybercrime, espionage, identity theft, stalking, and other threats on the Internet. Undermining strong encryption could make our data more vulnerable.

In the 1990s, I opposed efforts to regulate the development of encryption technology. I sponsored and otherwise supported legislation that authorized the use of any type of encryption technology in the United States; prohibited the government from requiring key recovery features; and eased export restrictions limiting the sale of encryption technology abroad. I also opposed efforts to promote the “Clipper Chip,” a cryptographic device for voice communications that facilitated government access to those communications.

I was concerned that regulating encryption would stifle innovation, harm American businesses, impede technological advancements, and undercut security. In 1996, I wrote an open letter to the Internet – and became the first member of Congress to use the popular encryption program Pretty Good Privacy and sign a letter using an encrypted digital signature – arguing that regulating encryption was a “hopelessly outdated” policy that “fails to account for the real needs of individuals and businesses in the global marketplace.” The Clinton administration ultimately abandoned efforts to limit encryption technology. Many experts now credit this decision for helping create the modern Internet, in which consumers use encryption to facilitate online retail, banking, social media, and other communications.

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

The President's Review Group on Intelligence and Communications Technology also explained in their December 2013 report that "in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud."

We also have to consider the effect on U.S. government efforts to promote encryption and secure communications technology around the world. As Ranking Member of the Appropriations Subcommittee on State, Foreign Operations and Related Programs, I know we have appropriated more than \$100 million dollars just in the past two years to promote Internet freedom, including providing strong encryption technology to human rights workers, journalists, and political dissidents working under repressive regimes.

Even if the United States were to take steps to facilitate law enforcement access to encrypted communications, we need to evaluate how much it would help. Strong encryption would still be available from foreign providers. Some say that any competent Internet user would be able to download strong encryption technology, or install an "app" allowing encrypted communications -- regardless of restrictions on American businesses. But it would put American companies at a disadvantage in the global marketplace.

These are among many factors this Committee must consider. The Committee is hearing some important perspectives today, but there are other voices that need to be part of this conversation. When the Chairman holds further hearings on this topic, I hope that he will also include witnesses from the technology industry, which would be directly affected by any effort to regulate encryption. I ask that materials from industry trade associations be placed in the record.

I welcome Deputy Attorney General Yates, who is with us for the first time since her confirmation. And it is always good to see Director Comey, who I was pleased to host in Vermont a couple of months ago. I look forward to hearing from both of you.

#####



Department of Justice

STATEMENT OF

**SALLY QUILLIAN YATES
DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE**

AND

**JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

BEFORE THE

**COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE**

AT A HEARING ENTITLED

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

PRESENTED

JULY 8, 2015

**Statement of
Sally Quillian Yates
Deputy Attorney General
Department of Justice**

and

**James B. Comey
Director
Federal Bureau of Investigation**

**Before the
Committee on the Judiciary
United States Senate**

**At a Hearing Entitled
“Going Dark: Encryption, Technology, and the Balance
Between Public Safety and Privacy”**

**Presented
July 8, 2015**

Good morning, Chairman Grassley, Ranking Member Leahy, and Members of the Judiciary Committee. Thank you for the opportunity to testify today about the growing challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant. We in law enforcement often refer to this problem as “Going Dark”.

We would also like to thank this Committee more generally for its continued support for the mission of the Department of Justice. We know that you, like us, take very seriously the role of the Department in protecting the public in a manner that upholds the Constitution and the rule of law.

Introduction

In recent years, new methods of electronic communication have transformed our society, most visibly by enabling ubiquitous digital communications and facilitating broad e-commerce. As such, it is important for our global economy and our national security to have strong encryption standards. The development and robust adoption of strong encryption is a key tool to

secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cybersecurity. The Department is on the frontlines of the fight against cybercrime and we know first-hand the damage that can be caused by those who exploit vulnerable and insecure systems. We support and encourage the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data so as to promote our overall safety.

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

We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance—not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children; and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public. One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds reason to believe that certain private communications contain evidence of a crime, then the government can conduct a limited search for that evidence. For example, by having a neutral arbiter—the judge—evaluate whether the government’s evidence satisfies the appropriate standard, we have been able to protect the public and safeguard citizens’ Constitutional rights.

The Department of Justice has been and will always be committed to protecting the liberty and security of those whom we serve. In recent months, however, we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data. As a result, law enforcement is sometimes unable to recover the content of electronic communications from the technology provider even in response to a court order or duly-authorized warrant issued by a Federal judge. For example, many communications services now encrypt certain communications by default, with the key necessary to decrypt the communications solely in the hands of the end user. This applies both when the data is “in motion” over electronic networks, or “at rest” on an electronic device. If the communications provider is served with a warrant seeking those communications, the provider cannot provide the data because it has designed the technology such that it cannot be accessed by any third party.

Threats

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

When changes in technology hinder law enforcement’s ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to root

out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence.

These are not just theoretical concerns. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the Department of Justice, including the FBI, and the United States government as a whole.

Of course, encryption is not the only technology terrorists and criminals use to further their ends. Terrorist groups, such as ISIL, use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. For example, in recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters.

Outside of the terrorism arena we see countless examples of the impact changing technology is having on our ability to affect our court authorized investigative tools. For example, last December a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from State to State and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. The trucker claimed that the woman he had kidnapped engaged in consensual sex. The trucker in this case happened to record his assault on video using a smartphone, and law enforcement was able to access the content stored on that

phone pursuant to a search warrant, retrieving video that revealed that the sex was not consensual. A jury subsequently convicted the trucker.

In a world where users have sole control over access to their devices and communications, and so can easily block all lawfully-authorized access to their data, the jury would not have been able to consider that evidence, unless the truck driver, against his own interest, provided the data. And the theoretical availability of other types of evidence, irrelevant to the case, would have made no difference. In that world, the grim likelihood that he would go free is a cost that we must forthrightly acknowledge and consider.

We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

Legal Framework

We would like to emphasize that the “Going Dark” problem is, at base, one of technological *choices and capability*. We are not asking to expand the Government’s surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe.

The rules for the collection of the content of communications in order to protect public safety have been worked out by Congress and the courts over decades. Our country is justifiably proud of the strong privacy protections established by the Constitution and by Congress, and the Department of Justice fully complies with those protections. The core question is this: once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?

We would like to describe briefly the law and the extensive checks, balances, and safeguards that it contains. In addition to the Constitution, two statutes are particularly relevant to the Going Dark problem. Generally speaking, in order for the Government to conduct *real-time*—i.e., data in motion—electronic surveillance of the content of a suspect’s communications, it must meet the standards set forth in either the amended versions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (often referred to as “Title III” or the “Wiretap Act”) or the Foreign Intelligence Surveillance Act of 1978 (or “FISA”). Title III authorizes the Government to obtain a court order to conduct surveillance of wire, oral, or electronic communications when it is investigating Federal felonies. Generally speaking, FISA similarly relies upon judicial authorization, through the Foreign Intelligence Surveillance Court (FISC), to approve surveillance directed at foreign intelligence and international terrorism threats. Regardless of which statute governs, however, the standards for the real-time electronic surveillance of United States persons’ communications are demanding. For instance, if Federal law enforcement seeks the authority to intercept phone calls in a criminal case using the Wiretap Act, a Federal district court judge must find:

- That there is probable cause to believe the person whose communications are targeted for interception is committing, has committed, or is about to commit, a felony offense;
- That alternative investigative procedures have failed, are unlikely to succeed, or are too dangerous; and
- That there is probable cause to believe that evidence of the felony will be obtained through the surveillance.

The law also requires that before an application is even brought to a court, it must be approved by a high-ranking Department of Justice official. In addition, court orders allowing wiretap authority expire after 30 days; if the Government seeks to extend surveillance beyond this period it must submit another application with a fresh showing of probable cause and

investigative necessity. And the Government is required to minimize to the extent possible its electronic interceptions to exclude non-pertinent and privileged communications. All of these requirements are approved by a Federal court.

The statutory requirements for electronic surveillance of U.S. persons under FISA are also demanding. To approve that surveillance, the FISC, must, among other things, find probable cause to believe:

- That the target of the surveillance is a foreign power or agent of a foreign power; and
- That each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power.

Similarly, when law enforcement investigators seek access to electronic information *stored*—i.e., data at rest—on a device, such as a smartphone, they are likewise bound by the mandates of the Fourth Amendment, which typically require them to demonstrate probable cause to a neutral judge, who independently decides whether to issue a search warrant for that data.

Collectively, these statutes reflect a concerted Congressional effort, overseen by an independent judiciary, to validate the principles enshrined in our Constitution and balance several sometimes-competing, yet equally-legitimate social interests: privacy, public safety, national security, and effective justice. The evolution and operation of technology today has led to recent trends that threaten this time-honored approach. In short, the same ingenuity that has improved our lives in so many ways has also resulted in the proliferation of products and services where providers can no longer assist law enforcement in executing warrants.

Provider Assistance

Both Title III and FISA include provisions mandating technical assistance so that the Government will be able to carry out activities authorized by the court. For example, Title III

specifies that a “service provider, landlord...or other person shall furnish [the Government]...forthwith all...technical assistance necessary to accomplish the interception.” As the communications environment has grown in volume and complexity, technical assistance has proven to be essential for interception to occur. These provisions alone, however, have not historically been sufficient to enable the Government to conduct electronic surveillance in a timely and effective manner.

In the early 1990s, the telecommunications industry was undergoing a major transformation and the Government faced a similar problem: determining how best to ensure that law enforcement could reliably obtain evidence from emerging telecommunications networks. At that time, law enforcement agencies were experiencing a reduced ability to conduct intercepts of mobile voice communications as digital, switch-based telecommunications services grew in popularity. In response, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. CALEA requires “telecommunications carriers” to develop and deploy intercept solutions in their networks to ensure that the Government is able to intercept electronic communications when lawfully authorized, although it does not require a carrier to decrypt communications encrypted by the customer unless the carrier provided the encryption and possesses the information necessary to decrypt. Specifically, it requires carriers to be able to isolate and deliver particular communications, to the exclusion of other communications, and to be able to deliver information regarding the origination and termination of the communication (also referred to as “pen register information” or “dialing and signaling information”). CALEA regulates the capabilities that covered entities must have and does not affect the process or the legal standards that the Government must meet in order to obtain a court order to collect communications or related data.

While CALEA was intended to keep pace with technological changes, its focus was on telecommunications carriers that provided traditional telephony and mobile telephone services, not Internet-based communications services. Over the years, through interpretation of the statute by the Federal Communications Commission, the reach of CALEA has been expanded to include facilities-based broadband Internet access and Voice over Internet Protocol (VoIP) services that

are fully interconnected with the public switched telephone network. Although that expansion of coverage has been extremely helpful, CALEA does not cover popular Internet-based communications services such as email, Internet messaging, social networking sites, or peer-to-peer services.

At the time CALEA was enacted, Internet-based communications were in a fairly early stage of development, and digital telephony represented the greatest challenge to law enforcement. However, due to the revolutionary shift in communications technology in recent years, the Government has lost ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA.

The harms resulting from the inability of companies to comply with court-ordered surveillance warrants are not abstract, and have very real consequences in different types of criminal and national security investigations.

Going Forward

Mr. Chairman, the Department of Justice believes that the challenges posed by the Going Dark problem, are grave, growing, and extremely complex. At the outset, it is important to emphasize that we believe that there is no one-size-fits-all strategy that will ensure progress. We have been asked what we should do going forward. We believe we will need to pursue multiple paths:

All involved must continue to ensure that citizens' legitimate privacy interests can be effectively secured, including through robust technology and legal protections.

We must continue the current public debate about how best to ensure that privacy and security can co-exist and reinforce each other, and continue to consider all of the legitimate concerns at play, including ensuring that law enforcement can keep us safe. The debate so far has been a challenging and highly charged discussion, but one that we believe is essential to have. This includes a productive and meaningful dialogue on how encryption as currently

implemented poses real barriers to law enforcement's ability to seek information in specific cases of possible national security threat.

We also cannot lose sight of the international implications of this issue. It is clear that governments across the world, including those of our closest allies, recognize the serious public safety risks if criminals can plan and undertake illegal acts without fear of detection. It is also true that other countries—particularly those without our commitment to the rule of law—are using this debate as a cynical means to create trade barriers, impose undue burdens on our companies and undermine human rights. We should be clear that any steps that we take here in the United States may impact the decisions that other nations take—both our closest democratic allies and more repressive regimes. In addition, any next steps we identify will be more effective if we are working together with our allies, and made more difficult if we are isolated.

We should also continue to invest in developing tools, techniques, and capabilities designed to mitigate the increasing technical challenges associated with the “Going Dark” problem. In limited circumstances, this investment may help mitigate the risks posed in high priority national security or criminal cases, although it will most likely be unable to provide a timely or scalable solution in terms of addressing the full spectrum of public safety needs.

We don't have any silver bullet, and the discussions within the Executive Branch are still ongoing. While there has not yet been a decision whether to seek legislation, we must work with Congress, industry, academics, privacy groups and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months. But we can all agree that we will need ongoing honest and informed public debate about how best to protect liberty and security in both our laws and our technology.

Conclusion

Mr. Chairman and Ranking Member Leahy, we would like to thank you and the members of this Committee again for your attention to this subject of national importance. While technology may change, our basic commitment at the Department to upholding the rule of law and our constitutional traditions does not. Our goal at the Department is to work collaboratively

and in good faith with interested stakeholders to explore approaches that protect the integrity of technology and promote strong encryption to protect privacy, while still allowing lawful access to information in order to protect public safety and national security.

We would be happy to answer any questions that you may have.



**Written Testimony of New York County District Attorney Cyrus R. Vance, Jr.
Before the United States Senate Committee on the Judiciary**

**“Going Dark: Encryption, Technology, and the
Balance Between Public Safety and Privacy”**

**Washington, D.C.
July 8, 2015**

Good morning Chairman Grassley, Ranking Member Leahy, and Members of the Senate Judiciary Committee. Thank you for your leadership on these issues, and for the opportunity to testify today.

Encryption and government access to data stored on electronic devices have largely been discussed as a federal and national security issue. In truth, the implications of this discussion are equally, or even more importantly, of significant concern to state and local law enforcement. That is because more than 90 percent of all criminal cases filed annually are filed and adjudicated in state courts around the country.¹

To use the New York County District Attorney’s Office as a point of reference, my Office handles more than 100,000 criminal cases each year, which is more than all of the cases handled by the Department of Justice nationwide. And the range of those cases is broad – from murder, rape, and robbery, to identity theft, financial fraud, and terrorism.

¹ See http://www.ncsc.org/Sitecore/Content/Microsites/PopUp/Home/CSP/CSP_Intro;
<http://www.bjs.gov/content/pub/pdf/fjs12st.pdf>.

People live their lives today on their smartphones, which they use for, among others things, emailing, texting, taking pictures, posting pictures, shopping, conducting business, and searching the web. To investigate these 100,000 cases without smartphone data is to fight crime with one hand tied behind our backs.

Therefore, I want to focus my testimony on an issue deeply troubling for law enforcement at all levels: the encryption of smartphone data by Apple and Google. I believe that by having an open discussion among lawmakers, law enforcement, and the private sector, we can reach a solution that strikes the right balance between privacy and public safety.

I. The Use of Smartphone Evidence Pursuant to Judicial Warrants

As you know, the Fourth Amendment of the United States Constitution authorizes reasonable searches and seizures, providing law enforcement agencies access to places where criminals hide evidence of their crimes – from car trunks, to storage facilities, to computers, mobile devices, and digital networks. In order to safeguard Fourth Amendment rights, these searches are conducted pursuant to judicial warrants, issued upon a neutral judge’s finding of probable cause. The probable cause standard represents a balance between privacy and public safety carefully calibrated by centuries of jurisprudence, and it guides individuals and companies in developing their expectations of privacy.

Through this judicial process, my Office obtains smartphone evidence to support all types of cases – homicides, sex crimes, child abuse, fraud, assaults, robberies, cybercrime, and identity theft. Many perpetrators, particularly those who commit sexual offenses, take photos and videos of their acts, and store them on computers and smartphones.

Between October 2014 and June 2015, 35 percent of the data extracted from all phones by my Office was collected from Apple devices; 36 percent was collected from Android devices.² That means that when smartphone encryption is fully deployed by Apple and Google, 71 percent of all mobile devices examined—at least by my Office’s lab—may be outside the reach of a search warrant.

I want to emphasize I am testifying from a state and local perspective. I am not advocating bulk data collection or unauthorized surveillance. Instead, I am concerned about protecting local law enforcement’s ability to conduct targeted requests for information, scrutinized by an impartial judge for his or her evaluation as to whether probable cause has been established. Importantly, and *by Apple’s own admission*, governmental request for information have affected only .00571 percent of Apple’s customers.³

II. Apple and Google’s New Encryption⁴ Policies

Last fall, Apple and Google, whose operating systems run 96 percent of smartphones worldwide, announced with some fanfare, but without notice to my Office or other law enforcement offices I have spoken to, that they had engineered their new mobile operating systems such that they can no longer assist law enforcement with search warrants written for passcode-protected smartphones. According to Apple’s website:

On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. . . . Apple *will not perform iOS data*

² The remaining 29 percent of data was extracted from other types of phones, such as flip phones and burner phones.

³ <https://www.apple.com/privacy/government-information-requests/>.

⁴ Data transmitted between phones, computers, and other digital devices can be encrypted (i) while in transit between those devices and (ii) on the devices themselves. This latter type of encryption is referred to as full-disc encryption, and that is the type of encryption that I am concerned with here.

extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess. [Emphasis added.]⁵

Apple's announcement led to an immediate response by law enforcement officials who pointed out that allowing a phone or tablet to be locked such that it would be beyond the reach of lawful searches and seizures was unprecedented and posed a threat to law enforcement efforts – in effect, a boon to criminals. Unless law enforcement officials can obtain the passcode from the user, which will be difficult or impossible in many cases, or can use “brute force” to obtain the passcode (again, difficult or impossible, and attempts to do this would likely lead to the destruction of evidence on the iPhone), the search warrant would be of no consequence, because no one will be able to unlock the phone, notwithstanding the court order.

Law enforcement's warnings are hardly idle. Recently, a father of six was murdered in Evanston, Illinois. City of Evanston Police believe that prior to his murder, the victim was robbed of a large sum of money. There were no eyewitnesses to or surveillance footage of the killing. Found alongside the body of the deceased were an iPhone 6 and a Samsung Galaxy S6 Edge running Google Android. Cook County prosecutors served Apple and Google with judicial warrants to unlock the phones, believing that relevant evidence might be stored on them. Apple and Google replied, in substance, that they could not, because they did not know the user's passcode. Information that might be crucial to solving the murder, therefore, had effectively died with the victim. His homicide remains unsolved. His killer remains at large.

It is not hyperbole to say that beginning in September 2014, Americans conceded a measure of their protection against everyday crimes to Apple and Google's new encryption policies. Yet, I

⁵ <https://www.apple.com/privacy/government-information-requests/>.

would note that, before the changes, neither company, to our knowledge, ever suggested that their encryption keys, held by the companies, were vulnerable to hacking or theft.

Fully one-quarter of our felony cases now involve cybercrime or identity theft, so I am keenly aware of the dangers and impact of these crimes on our community (which happens to be situated in a world financial center and is the number one target for terrorism in the world). Because of this, my Office has invested heavily in becoming highly proficient and active in the prosecution of these crimes, and in the promotion of best cybersecurity practices for New York consumers and companies. From my vantage point, and in my opinion, for reasons set forth later in my testimony, Apple and Google's new encryption policies seem to increase protection for consumers from hackers only minimally, if at all. But those policies create serious new risks for my constituents and the millions of visitors and workers passing through Manhattan every day.

III. The Problem Created by Apple and Google's New Encryption Policy

Some commentators have argued that the effective unsearchability of smartphones will not be significant because law enforcement has other avenues for investigation.⁶ These arguments are flawed, for the reasons set forth below. While Apple is not the only company to have announced a similar program, for ease of presentation, and because Apple has been the most vocal company on the relevant issues, I address here only Apple's program, devices, and statements. I believe that the arguments and reasoning here would apply as well to Google's program and any similar program.

A. The Search of an iCloud Account is Not a Substitute for the Search of an iPhone

Apple's new encryption policy currently does not affect law enforcement officials' ability to obtain user data from an iCloud account. Law enforcement officials who obtain a search warrant

⁶ See, e.g., http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html?_r=0.

for a person's iCloud account can serve that warrant on Apple, and thus obtain the contents of the account, regardless of whether the person's iPhone uses iOS 8.

But searching a person's iCloud account is not the same as searching the person's iDevice.⁷ The ability of law enforcement officials to obtain a search warrant for an iCloud account does not mean that those officials will obtain the same content as they would if they could search the user's device. In many cases, law enforcement officials cannot obtain the entirety of an iPhone's data by obtaining the contents of the associated iCloud account.

First, and most fundamentally, users of iDevices are not required to set up iCloud accounts or to back-up to iCloud accounts. Therefore, not all users of iDevices will have data stored to iCloud. It is clear that even minimally sophisticated wrongdoers who use their iDevices to perpetrate crimes will take the relatively simple steps necessary to avoid backing up those devices to iCloud.

Second, even when a user chooses to back up his or her data to iCloud routinely, some data may not be backed up and would, therefore, be unattainable through a search warrant for an iCloud account. Data that is saved on an iPhone will not be backed up to the cloud until the iPhone is connected to Wi-Fi. So, if evidence is stored on an iPhone when the phone is disconnected from Wi-Fi, and the iPhone is recovered by law enforcement officials before it is reconnected to Wi-Fi, then the evidence would exist only on the iPhone itself.

iPhone users are given only five gigabytes of free storage space on iCloud, whereas iPhone 6s come with either 16, 64, or 128 gigabytes of storage space on the device itself. Thus, unless a user pays for additional iCloud storage space, the vast majority of their storage space will be on the iPhone itself.

⁷ Mobile devices manufactured by Apple are called iDevices, and include phones (iPhones), tablets (iPads), and MP3 players that play audio and video files (iPods).

Third, it may be possible to recover at least some deleted data from an iDevice. Once data has been deleted from an iCloud account, however, it is not recoverable.⁸ Thus, the iPhone is the only route to evidence that has been deleted – which may, of course, be among the most probative evidence.

Fourth, it will often be more difficult for a prosecutor to prove who uses the data on a particular iCloud account than it would be to prove who owns a particular iDevice. iDevices are often recovered from a person, which supports the inference that the person controls the device. To establish the person's ownership of the device, a prosecutor may simply have to call one witness – the officer who recovered the device. By contrast, the identity of the user of an iCloud account may be more difficult to establish. A prosecutor may need to present testimony or records from Apple relating to the subscriber information, IP login history,⁹ and/or content of the account, testimony or records from internet service providers regarding the subscriber information of certain IP addresses, and/or testimony of forensic analysts, among other witnesses.

B. The Difficulty of Getting Passcodes from Defendants

In many cases, the iPhone that may contain evidence about a criminal case belongs to the defendant, and thus it is her or his passcode that prevents the government from gathering the

⁸ Apple Legal Process Guidelines, <https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf>, page

9.

⁹ An IP address is a series of numbers separated by three periods (i.e. 192.168.10.12) that uniquely identifies a particular connection to the internet at a specific date and time. Apple maintains a record of the IP addresses used to log in to iCloud accounts within a recent time period. Pursuant to appropriate legal process, law enforcement officials can obtain the IP login history for a particular iCloud account, that is, a list of IP addresses that the user of the iCloud account used to connect to the internet prior to signing in to his or her iCloud account, as well as the dates and times of those log-ins. After law enforcement obtains this information from Apple, law enforcement officials can send a subpoena to the internet service provider that owns each IP address listed requesting the subscriber information for each IP address. Examples of internet service providers include Time Warner Cable or Comcast. The subscriber information for the IP address will be the name and contact information provided by the user of the particular internet service account when they signed up for that account.

evidence. In most cases, it will be almost impossible to compel a defendant to provide her or his passcode to the government.

Case law holds almost universally that a defendant cannot be compelled (by, for example, a grand jury subpoena or order of the court) to provide the government with her or his passcode, because such compulsion would violate the defendant's Fifth Amendment right against self-incrimination.¹⁰ There are two potential exceptions to this rule.

First, it is an open question whether, instead of being compelled to provide the government with a passcode, the defendant might be compelled to unlock her or his iPhone *using* the passcode. There have been no cases of which we are aware that consider this precise question, and although a court might conclude that it is no different from the situation in which a defendant is compelled to provide the government with the password, it might also determine that the situations are somewhat different.¹¹

Second, if the existence of particular evidence on the iPhone is a foregone conclusion, then the defendant may have no Fifth Amendment privilege with respect to those contents of the iPhone, and thus may be compelled to provide the government with the passcode.¹² It would be very

¹⁰ The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const., amend. V. The amendment's prohibition against self-incrimination has been "incorporated" so that it applies to state criminal proceedings, as well as federal. See *Malloy v. Hogan*, 378 U.S. 1, 6 (1964); *Griffin v. California*, 380 U.S. 609, 615 (1965). The cases addressing the question whether a defendant may be compelled to provide her or his password to the government, and holding that such compulsion would violate the Fifth Amendment include: *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *United States v. Kirschner*, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010).

¹¹ Professor Oren Kerr has suggested that because it is (or may, in many cases be) a "foregone conclusion" that a person knows the password to her or his own smartphone, it would not violate the Fifth Amendment to compel a phone owner to use her or his password to open the phone. See Kerr, *Apple's Dangerous Game*, on *The Volokh Conspiracy* (September 19, 2014) (citing *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009)). This may be correct, although it has not been tested in any case (*Boucher* suggests that if the *content* of the smart phone is known (a "foregone conclusion"), then requiring the password may not implicate the Fifth Amendment; it does not say that a person's knowledge of her or his password would satisfy the foregone conclusion requirement.)

¹² See, e.g., *People v. Havrsh*, 8 NY3d 389, 395 (N.Y. 2007); *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009) at *3; *In re Friscos*, 841 F. Supp.2d 1232, 1237 (D. Colo. 2012).

difficult in most circumstances, however, for the government to establish with the requisite degree of certainty the existence of evidence in the contents of an iPhone that would clear the “foregone conclusion” hurdle.

In any event, even if the government could lawfully compel a defendant to disclose her or his passcode – or to open her or his phone using the passcode – there is a substantial likelihood that any defendant who faces potentially serious criminal charges would simply refuse to comply with the subpoena or order, and go into contempt.¹³

The consequence of the foregoing is that in almost all cases, it will be legally impossible to compel a defendant to provide his or her passcode or to use the passcode to open her or his iPhone, and that, in those few cases in which it might be legally possible to compel the defendant to provide the information, it would be impossible as a practical matter to compel a recalcitrant defendant facing serious charges to do so. And, of course, whatever powers law enforcement might have to compel a defendant to cooperate in opening her or his phone, those powers are irrelevant to the situation in which the phone that law enforcement needs to open belongs to an unavailable victim (for example, the deceased, in a murder case) or to a witness or potential defendant who fled the scene of the crime.

IV. Apple’s Stated Reasons for Its New Encryption Policy

Apple, to our knowledge, has given four principal justifications for its new policy.

First, it has suggested that the new policy is a response to public concerns expressed in light of the revelations by Edward Snowden about data collection by the National Security Agency.¹⁴

¹³ See, e.g., *In re Weiss*, 703 F.2d 653, 660-65 (2d. Cir. 1983).

¹⁴ http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html?_r=0.

Second, Apple has suggested that unless it makes its iDevices impregnable to lawful governmental access, Apple will lose customers, who will seek to purchase substitute, impregnable devices.¹⁵

Third, Apple has suggested that if it were to build its devices such that it could respond to lawful governmental requests for information in them, then the iDevices would be less secure than if Apple built them (as it has) to be impregnable to such requests.¹⁶

Fourth, Apple has also suggested that if it were to build its devices such that it could respond to lawful domestic governmental requests for information in them, then foreign governments would also request access to the information contained in the devices, or hack into the devices to gain access;¹⁷ if those government were repressive, commentators have suggested, then it would, in effect, be helping repressive governments to limit their citizens' liberty.

Each of these proposed justifications will be addressed in turn.

A. American Customer Privacy Concerns Based on NSA's Actions

Apple's encryption efforts – and, more particularly, its announcement of those efforts – appear to be partially in response to concerns expressed by the public in the wake of revelations about incursions of privacy by the NSA, many of which were brought to light by Edward Snowden and others working with him.¹⁸ The encryption efforts are not a reasonable response to the Snowden-NSA issue for at least two reasons.

¹⁵ Id.

¹⁶ <http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.a3spud:Ugxb>.

¹⁷ <http://www.fastcompany.com/3046469/fast-feed/major-tech-companies-but-not-amazon-sign-letter-to-obama-against-security-backdoor>; <http://www.pcworld.com/article/2933397/tech-industry-redoubles-efforts-to-fight-us-govt-encryption-backdoors.html>.

¹⁸ <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2>; <http://www.bbc.com/news/world-us-canada-23123964>.

First, the effect of Apple's encryption is that it prevents (i) the necessity of Apple responding to lawful government requests and (ii) the government from examining the contents of iDevices, even when an independent judge has authorized such disclosure by issuing a search warrant. Of course, a search warrant cannot be issued absent a showing of probable cause to believe that a crime has been committed and that evidence or proceeds of the crime might be found on the iDevice to be searched.¹⁹

The warrant requirement has been described by the Supreme Court as "[t]he bulwark of Fourth Amendment protection,"²⁰ and there is no reason to believe that it cannot continue to serve in that role, whether the object to be searched is an iPhone or a home. In fact, what makes Apple's proposal remarkable is that it would provide greater protection to one's iPhone than one has in one's home, which, of course, has always been afforded the highest level of privacy protection.²¹ Every home can be entered with a search warrant. I cannot think of another device that has been knowingly designed in a way to prevent *lawful* government inspection. Thus, even if Apple's new encryption policy would have prevented the NSA's actions, or will be able to prevent similar conduct, it comes at a very high and unjustified cost.

Second, Apple's new encryption policy would not have prevented the NSA's gathering of data, which, at least according to press coverage, was not sanctioned by a court or covered by a

¹⁹ See U.S. Const., amend. IV ("... no Warrant 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."); *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (defining probable cause as "a fair probability that contraband or evidence of a crime will be found in a particular place").

²⁰ *Franks v. Delaware*, 438 U.S. 154, 164 (1978). See also, e.g., *Gonzales v. Beto*, 425 F.2d 963, 967 (5th Cir. 1970) ("The requirement of a search warrant is unquestionably a strong bulwark against the evils at which the fourth amendment is directed.").

²¹ See U.S. Const., amend. IV ("The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated . . ."); *Minnesota v. Carter*, 525 U.S. 83, 94 (1998) ("The people's protection against unreasonable search and seizure in their 'houses' was drawn from the English common-law maxim, 'A man's home is his castle.'" (Scalia, J., concurring)).

search warrant.²² That press coverage indicates that the NSA collected phone call data (including numbers called and the duration of phone calls), and the content of at least some phone conversations, often involving people for whom there was no reasonable suspicion of criminal activity, without judicial approval.²³ Of course, that is nothing like what we are suggesting, and, in any event, the encryption of iDevices would not have prevented the mass collection of phone call data, which is obtained from phone service providers rather than from phones themselves. And default full-disc encryption would not have prevented the NSA from intercepting communications in transit.

B. Security Concerns if Apple Can Decrypt

Apple has asserted that full-disc encryption maximizes the security of their users' devices and data. One should question that assertion for several reasons.

First, even before Apple enacted its new policy, a person who somehow obtained Apple's encryption key would still need the iPhone itself to obtain information on the device. It is highly unlikely that someone who snatches an iPhone from a subway commuter would also be a master hacker capable of breaching Apple's own security systems to obtain the encryption key. As best I can tell, Apple and Google's new encryption policies prevent lawful access by state and local law enforcement, and do nothing to address serious challenges like institutional data breaches or invasion by malware.

Second, if a user's phone were to be stolen, the user could use the Find My iPhone app in order to wipe the phone's data and prevent the thief from accessing that data. Users who have an

²² I am not opining on the legality of the NSA's activity, but merely relying on the news coverage about that activity. See, e.g., <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/07/second-circuit-rules-mostly-symbolically-that-current-text-of-section-215-doesnt-authorize-bulk-surveillance/>; http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?_r=0; *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015).

²³ See, e.g., ZDNET, NSA Planned Google Play Hack to Target Android Smartphones, May 21, 2015.

iCloud account can use the Find My iPhone app remotely to lock their phones or erase their data if their phones are lost or stolen. This app can effectively prevent thief-hackers from obtaining a phone's data.²⁴

Third, according to Apple, most data stored on the iCloud is encrypted.²⁵ As noted above, law enforcement officials are able to obtain some iCloud data through the service of a search warrant on Apple. The fair inference is that Apple retains the ability to decrypt this iCloud data. But if Apple's ability to decrypt data on the iCloud does not render that data insecure – and Apple touts the security of its iCloud data²⁶ – then presumably neither would Apple's retaining the ability to decrypt data on an iPhone.

C. Concern About Foreign Governments' Access to Customer Information

Apple has suggested that if it maintains an encryption key to iOS 8, then repressive governments would seek access to information contained on devices, including those belonging to dissidents. If Apple were to comply, this would impede those dissidents' civil liberties. This contradicts commentators' arguments, referenced above, that iOS 8 will not be a significant burden on law enforcement, which can still request data from a user's iCloud account. Apple cannot have it both ways: Either iOS 8 does deter investigations or it does not.

But even more fundamentally, Apple's desire not to cooperate with requests from repressive governments does not justify its refusal to cooperate with *bona fide* requests from local law enforcement, approved by independent state or federal courts, in the United States. As I said before, the warrant requirement of the United States Constitution has been the fundamental

²⁴ A similar app is also available for Apple tablets and computers.

²⁵ <https://support.apple.com/en-us/HT202303>.

²⁶ See, e.g., id.

protection for people's privacy and liberty in this country. It can and should apply to iOS 8, as it does to any other home or device.

V. The Cost of Evidence Made Inaccessible Through Apple's Encryption

Although encryption has been often discussed in the context of international terrorism, the NSA, and the CIA, the greatest cost of these new encryption policies may well be borne by local law enforcement. Smartphones are ubiquitous, and there is almost no kind of case in which prosecutors have not used evidence from smartphones. My Office (and, I expect, every other local prosecutor's office) has used evidence from cellphones in homicides, rape cases, human trafficking, assaults, domestic violence cases, narcotics cases, kidnappings, larcenies, frauds, identity theft, cybercrime, and robberies. Indeed, it is the rare case in which information from a smartphone is *not* useful. The following list of recent cases is representative:

- **Homicide:** *People v. Hayes*, Indictment Number 4451/12: The victim was filming a video using his iPhone when he was shot and killed by the defendant. The video captured the shooting. Because the iPhone was not locked, the video was recovered and admitted into evidence at trial. The video corroborated eyewitness testimony. The defendant was convicted of murder and sentenced to 35 years to life.
- **Sex Trafficking:** *People v. Brown*, Indictment Numbers 865/12, 3908/12, and 3338/13: The defendant directed a sex trafficking operation involving at least four women, using physical violence, threats of force, and psychological manipulation to coerce the women to engage in prostitution. Evidence recovered from electronic devices lawfully seized from the defendant's home proved crucial to his conviction at trial. In particular, the defendant's cellular phones contained photographs showing him posing his victims for online prostitution advertisements, and showing that he had "branded" multiple women, with his

nickname tattooed onto their bodies; text messages between him and several victims confirmed that he had engaged in acts of violence against the testifying witness and others. The defendant was convicted of multiple counts of sex trafficking and promoting prostitution and was sentenced to 10-20 years in prison.

- **Cybercrime and Identity Theft:** *People v. Jacas et al.*, Indictment Number 42/12 and *People v. Brahms et al.*, Indictment Number 5151/11: This case involved the successful prosecution of a 29-member identity theft ring, which was able to be investigated and prosecuted, in large part, because of evidence obtained early in the investigation from an iPhone, pursuant to a search warrant. An iPhone was recovered from a waiter who was arrested for stealing more than 20 customers' credit card numbers by surreptitiously swiping those credit cards through a card reader that stored the credit card number and other data. When the phone was lawfully searched, law enforcement officials discovered text messages between members of the group regarding the ring's crimes. Investigators were able to obtain an eavesdropping warrant, and ultimately arrested 29 people, including employees of high-end restaurants who stole credit card numbers, shoppers who made purchases using counterfeit credit cards containing the stolen credit card numbers, and managers who oversaw the operation. The group compromised over 100 American Express credit card numbers and stole property worth over \$1,000,000. All of the defendants pleaded guilty, and more than \$1,000,000 in cash and merchandise were seized and forfeited.
- **Sex Offenses:** *United States v. Juarez*, Case No. 12-CR-59: The defendant was arrested for unlawful surveillance by an NYPD officer after the officer observed the defendant using a cell phone to film up women's skirts. My Office obtained a search warrant for the phone.

During the subsequent search of the phone's micro SD card, forensic analysts discovered a series of images, taken by the defendant, showing a seven-year-old girl lying down on a bed and an adult man pushing aside her underwear, revealing her genitals. The case was referred to the United States Attorney's Office for the Eastern District of New York, which charged the defendant with producing child pornography.

- **Physical and Sexual Abuse of a Child:** *U.S. v. Patricia and Matthew Ayers*, Case No. 5:14 CR 0117 LSC SGC: In case after case, law enforcement has been able to discover and prosecute child abuse by using video or photographic evidence taken by the abuser. This case is illustrative: From 2010 to 2013, the defendants abused and exploited a young child in their care who, during that period, was six to nine years old. The couple took photographs of the child in lewd poses, as well as of each other engaged in sexual acts with the child. The defendants recorded the abuse with their smartphones and downloaded the images to a computer. In at least one instance, one of the defendants transmitted images to another individual, indicating that she would travel interstate with the child to the individual's home so the individual could also have sexual relations with the child. The federal judge overseeing the case described it as the worst case he has personally dealt with, including murders, in his 16 years on the bench. The defendants were ultimately convicted of producing child pornography, in violation of 18 U.S.C. § 2251(a), and were sentenced to 1,590 and 750 years, respectively, in federal prison.

There are many other cases—almost too many to count—that I might have selected, but the point is clear: We would risk losing crucial evidence in all of these cases if the contents of passcode-protected smartphones were unavailable to us, even with a warrant.

The enormity of the loss is fully appreciated by wrongdoers who use smartphones. Recently, a defendant in a serious felony case told another individual on recorded jailhouse call that “Apple and Google came out with these softwares that can no longer be encrypted [sic: *decrypted*] by the police. . . . If our phones is running on the i0[S]8 software, they can’t open my phone. That might be another gift from God.”

This defendant’s appreciation of the safety that the iOS 8 operating system afforded him, is surely shared by criminal defendants in every jurisdiction in America charged with all manner of crimes, including rape, kidnapping, robbery, promotion of child pornography, larceny, and presumably by those interested in committing acts of terrorism. Criminal defendants across the nation are the principal beneficiaries of iOS 8, and the safety of all American communities is imperiled by it.

VI. Proposed Solution: Return to a Balanced Approach – Requiring Phones To Be Manufactured So That They Would Be Accessible To Law Enforcement When Law Enforcement Has Obtained a Search Warrant

Apple has done something truly extraordinary. I am aware of no products other than those running iOS 8 and Google’s analogous Android devices that have been designed specifically to be impervious to lawful governmental processes. While Apple pursues an extraordinary path, I am proposing here a perfectly conventional one – a return to the balanced approach in place prior to the introduction of iOS 8. Apple’s products should be configured such that data on its iDevices can be accessed by law enforcement when it has judicial authorization to do so.

I believe that the only way Apple could be compelled to configure its products along the lines that I have suggested is through legislation. It is important to proceed with great caution, and any legislation must be carefully drafted to avoid stifling innovation or causing material harm to the United States technology sector, which is so vital to our national economy. But, in the fast-

changing field of technology, legislation is the right tool – far better than litigation – to effect change and balance social objectives.

Legislation can be changed, revised, amended, and tweaked, to accommodate valid social goals in the face of a shifting technological landscape. As Justice Alito has observed, “[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.”²⁷ Furthermore, legislation allows the public, rather than Apple or any other company, to set the balance between privacy and security. The trade-off is borne by the public, and it should be decided by the public as well.

Informed legislation, however, requires debate and open discussion. I have attempted to discuss with Apple many of the items that I have discussed here. In March of this year, I travelled to Apple’s headquarters and expressed my concerns directly to members of Apple’s management team as to how Apple’s encryption policy adversely affected law enforcement’s ability to protect the public safety. I followed up my visit with a letter, summarizing my questions about iOS 8. To date, I have not received a response. (A copy of my letter to Apple, and a copy of a similar letter that I wrote to Google, are attached to this written testimony.)

I would encourage this Committee to seek answers from Apple. The time has come for *someone* to determine the proper balance between the marginal benefits of full-disc encryption, and the need for state and local law enforcement to prosecute and prevent crime, and for victims to obtain justice. That someone should not be Apple or Google. It should be you, the Congress.

Thank you for the opportunity to testify today.

²⁷ *U.S. v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (citing Owen Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805-06 (2004)).



CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N.Y. 10013
(212) 335-9000

March 31, 2015

Jane Horvath, Senior Director of Global Privacy
Apple Headquarters
1 Infinite Loop
Cupertino, CA 95014

Re: Follow-up from our meeting of March 19, 2015

Dear Jane,

Thank you for the time you spent on March 19th with me and my colleagues, as well as representatives from the Secret Service and the National Computer Forensics Institute, discussing smartphone encryption and its impact on law enforcement. We found the discussion helpful.

For us better to understand some of the concerns that you expressed at our meeting, we have some additional questions which we hope that you can answer the following questions:

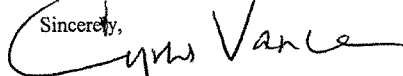
1. There was much discussion at our meeting about mobile phone data being "backed up" in the Cloud. Therefore, could you please advise us:
 - a. What percentage of Apple mobile device users have associated iOS backups stored on Apple's iCloud servers?
 - b. What percentage of current Apple mobile device users have the iCloud backup option turned on?
 - c. What percentage of current Apple mobile device users have utilized iCloud backup to produce at least one backup stored with Apple?
 - d. What is the retention period of an iCloud backup if the user decides to turn off iCloud backup?
 - e. Are the iOS8 backups stored on the iCloud encrypted?

2. As we explained, our view is that the judicially-issued search warrant is the bulwark for the protection of people's privacy. I understood that Apple believes that if Apple kept a "key" so that it was able to open locked iPhones, some foreign authorities might compel Apple to open iPhones and thus use them against their own citizens. That leads to the following questions:

- a. Is it accurate that, after the iOS8 upgrade, Apple no longer maintains the ability to unlock iPhones running on iOS8 anywhere in the world market? For example, does Apple no longer maintain the ability to unlock iPhones running iOS8 that it sells in China, India, or other world markets outside of the United States? Even if Apple does not maintain the ability to unlock devices running on iOS8, does Apple provide any foreign agency or entity the right or ability to unlock iOS8 devices?
 - b. In the past five (5) years, how many demands have there been from foreign jurisdictions to unlock iPhones, and has phone content been provided to those jurisdictions in response?
 - c. For the instances identified in 2(b) above, were those demands from foreign jurisdictions made directly to Apple, or through letters rogatory, or in some other fashion?
3. If Apple kept a "key" so that it was able to unlock iPhones, would the iPhones be more vulnerable to hackers than if Apple had no such "key"? Is there any "key" or similar device that Apple might keep without sacrificing the security of iPhones from hackers? Is there a way to measure or quantify the vulnerability to hackers of iPhones (a) if Apple kept a key, as compared to (b) if it did not keep a key?

We appreciate your time, and we look forward to further conversations. Thank you also for being gracious hosts; it was terrific to be on the Apple campus and see a true state of the art workplace.

Sincerely,



Cyrus R. Vance, Jr.



CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N.Y. 10013
(212) 335-9000

April 1, 2015

Kent Walker, Senior Vice President and General Counsel
Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Re: Follow-up from our meeting of March 19, 2015

Dear Kent,

Thank you for the time you spent on March 19th with me and my colleagues, as well as representatives from the Secret Service and the National Computer Forensics Institute, discussing smartphone encryption and its impact on law enforcement. We found the discussion helpful.

I was pleased and grateful to learn that Google intends to install a law enforcement portal to make interactions between law enforcement and Google, and responses to grand jury subpoenas and search warrants, as efficient and timely as possible.

It is my understanding that Google will continue its encryption initiative and that you expect more original equipment manufacturers to create more devices that support encryption over the next few months. As we made very clear, while we understand your position we feel that encryption that cannot be reached even by lawful process poses a significant problem for law enforcement, and a public safety threat.

To better understand some of the encryption-related matters that we discussed during our meeting, we have some questions that we hope you can answer:

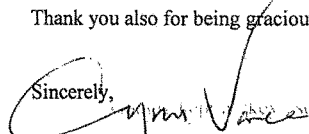
1. In response to our concern about our inability to extract data from cellular phones with full device encryption, it was suggested to us that an alternative means to obtain some of the data from the device would be to obtain data "backed up" to the cloud. Therefore, could you please advise us:
 - a. What percentage of Android mobile device users have associated backups stored on servers?
 - b. What percentage of current Android mobile device users have the backup option turned on?

- c. What percentage of current Android mobile device users have utilized cloud backup to produce at least one stored backup?
 - d. What is the retention period of a cloud backup if the user decides to turn off the backup?
 - e. Are the backups stored on the cloud currently encrypted? If it is not currently encrypted, are their plans to encrypt the cloud content and what is the timeline for such implementation?
2. If Google kept a "key" so that it was able to unlock phones, would the phones be more vulnerable to hackers than if Google had no such key? Is there any key or similar device that Google might keep without sacrificing the security of Android devices from hackers? Is there a way to measure or quantify the vulnerability to hackers of Android phones (a) if Google kept a key, as compared to (b) if it did not keep a key?

You expressed frustration at the fact that your employees are required to appear before the grand jury to authenticate Google's business records. I share your frustration, and have drafted proposed legislation that would allow business records to be authenticated by affidavit. A copy of our proposed legislation is enclosed herewith. Google supported an earlier, almost identical, version of this proposed legislation, and I presume that Google would support this as well.

Thank you also for being gracious hosts, and for showing us your state-of-the-art workplace.

Sincerely,



Cyrus R. Vance, Jr.

w/attachment

Testimony by Herbert Lin
 Senior Research Scholar, Center for International Security and Cooperation
 Research Fellow, Hoover Institution
 Stanford University
 Chief Scientist (Emeritus), CSTB, National Academies

Senate Judiciary Committee
 July 8, 2105

Ladies and Gentlemen, thank you for inviting me to testify today. I have worked on cyber policy and security issues for many years, mostly at the National Academies and now at Stanford University, but the views I present today are my own.

The previous panel discussed “going dark”, and I want to address 3 issues.

- First, the US government has framed solutions to the “going dark” problem around the concept of NOBUS access to encrypted data. (NOBUS stands for “nobody but us” where “us” is the government, a term first used publicly by Michael Hayden.) This approach has generated polarization around two positions. One side says NOBUS access inevitably weakens the security of a system and will eventually be compromised by a bad guy; the other side says it doesn’t weaken security and won’t be compromised. Neither side can **prove** its case, and we see a theological clash of absolutes.

To get out of this box, let’s instead consider time scale. If it takes a thousand years for a bad guy to figure out how to hack a NOBUS mechanism, that’s probably secure enough. If it takes him 30 seconds, using that mechanism is a dumb idea. So somewhere between 30 seconds and a thousand years, the mechanism changes from being unworkable to being secure enough.

How can we estimate the time the bad guy needs? We don’t understand very well today how to make these estimates for computer systems. But there are methodologies that are often used today to make such estimates for systems in other domains. For example, an approach called **probabilistic risk analysis** is often used in estimating the time before a nuclear reactor experiences a meltdown. Generally speaking, one estimates the probabilities of various sequences of events that could lead to failure-- what’s called fault and event tree analysis, and out of that comes an estimate that it will take 10,000 years or a million years. Opponents and proponents of nuclear power use different numbers to make their estimates, but at least they use the same methodology and they can identify where they disagree technically. That’s a better outcome than shouting at each other over a table saying “yes” or “no”.

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

Would a similar approach work in analyzing a proposed NOBUS mechanism? I think so, but I could be wrong. That’s why it’s a research problem—we should assess whether such methodologies can be usefully applied to estimate how long it might take for a bad guy to hack any specific NOBUS mechanism. But the government has not yet provided any specifics, arguing

that private vendors should do it. At the same time, the vendors won't do it, because its customers aren't demanding such features. Indeed, many customers would see such features as a reason to avoid a given vendor.

Without specifics, there will be no progress. I believe the government is afraid that any specific proposal will be subject to enormous criticism—and that's true—but the government is the party that wants NOBUS access, and rather than running away from such criticism, it should embrace any resulting criticism as an opportunity to improve upon its initial designs and provide a proof of principle that the approach is possible.

Exactly the same issues came up in the 1990s, only then the government did propose a specific mechanism. When the National Academies studied the problem then, it made a recommendation that still makes sense today—a pre-requisite for going down this path is for the government to gain experience about how to properly operate a government-only system allowing NOBUS access. Without such experience, large scale deployment of any access mechanism across the entire nation is asking for trouble.

A final point is asking the major vendors to provide NOBUS access is only the first step, as Director Comey implied in his comments regarding end-to-end encryption to CNN on June 18. The next step is to impose access requirements on small app and open source developers, because they can build apps that bypass NOBUS mechanisms built into the platforms. And then you have to prevent people from bringing into the U.S. apps from abroad that don't have NOBUS access, which means an Internet firewall around the United States that blocks such apps and border inspections and import controls.

- Second, a partial alternative to NOBUS access is for law enforcement authorities to obtain legal authorization to take advantage of the vulnerabilities that already exist in all software. With proper legal authorization, law enforcement could hack the devices of bad guys to obtain unencrypted information when the bad guys themselves accessed it, and they do this to some extent today.
- Third, criminals are just like the rest of us in that they also forget passwords, and if they have not saved them somewhere, certain crimes will not happen because the would-be perpetrators will not be able to get the information needed to commit them. Remember also that data is often backed up to the cloud by default. So criminals will want mechanisms that enable them to retrieve inaccessible data, and if they do, that's a way that law enforcement can gain access.

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

Documents for the record

- Executive summary to 1996 NRC report: Cryptography's Role in Securing the Information Society

Motivated in part by the U.S. government proposal to promulgate escrowed encryption and the Clipper chip as a solution to the "going dark" problem of the 1990s, this report provided an analysis of escrowed encryption that is a useful point of departure for understanding today's debate. The recommendation that the government gain experience in operating an escrowed encryption system in its own domain (government systems and applications) is discussed in this report.

- Blog post from Herb Lin - <http://www.lawfareblog.com/making-progress-encryption-debate>, <http://www.lawfareblog.com/echoes-past-encryption>.

The "Making Progress" blog post discusses my argument that the time needed to compromise a NOBUS mechanism is what matters to this debate. The "Echoes" post makes the point about criminals forgetting passwords too.

- Blog post from Jonathan Mayer- <http://webpolicy.org/2015/04/28/you-cant-backdoor-a-platform/>

The Mayer blog post describes the "first step" argument in greater detail.

- Bellovin et al-"Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet", <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njti> p.

The Bellovin et al paper makes the case that lawful hacking is a way for law enforcement authorities to gain much of the access they need without introducing additional security vulnerabilities.

- Blog post from Paul Rosenzweig - <http://www.lawfareblog.com/encryption-wars-continue>.

The Rosenzweig blog post elaborates the argument about default backup of data to the cloud.

Cryptography's Role in Securing the Information Society
<http://www.nap.edu/catalog/5131.html>

CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY

Executive Summary

In an age of explosive worldwide growth of electronic data storage and communications, many vital national interests require the effective protection of information. When used in conjunction with other approaches to information security, cryptography is a very powerful tool for protecting information. Consequently, current U.S. policy should be changed to promote and encourage the widespread use of cryptography for the protection of the information interests of individuals, businesses, government agencies, and the nation as a whole, while respecting legitimate national needs of law enforcement and intelligence for national security and foreign policy purposes to the extent consistent with good information protection.

BASIC POLICY ISSUES

The Information Security Problem

Today's information age requires U.S. businesses to compete on a worldwide basis, sharing sensitive information with appropriate parties while protecting that information against competitors, vandals, suppliers,

BOX ES.1
The Foreign Threat to U.S. Business Interests

Of the wide variety of information risks facing U.S. companies operating internationally, those resulting from electronic vulnerabilities appear to be the most significant. The National Counterintelligence Center (NACIC), an arm of the U.S. intelligence community established in 1994 by presidential directive, concluded that "specialized technical operations (including computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses) account for the largest portion of economic and industrial information lost by U.S. corporations." Specifically, the NACIC noted that

[b]ecause they are so easily accessed and intercepted, corporate telecommunications—particularly international telecommunications—provide a highly vulnerable and lucrative source for anyone interested in obtaining trade secrets or competitive information. Because of the increased usage of these links for bulk computer data transmission and electronic mail, intelligence collectors find telecommunications intercepts cost-effective. For example, foreign intelligence collectors intercept facsimile transmissions through government-owned telephone companies, and the stakes are large—approximately half of all overseas telecommunications are facsimile transmissions. Innovative "hackers" connected to computers containing competitive information evade the controls and access companies' information. In addition, many American companies have begun using electronic data interchange, a system of transferring corporate bidding, invoice, and pricing data electronically overseas. Many foreign government and corporate intelligence collectors find this information invaluable.

SOURCE: National Counterintelligence Center, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, July 1995, pp. 16–17.

customers, and foreign governments (Box ES.1). Private law-abiding citizens dislike the ease with which personal telephone calls can be tapped, especially those carried on cellular or cordless telephones. Elements of the U.S. civilian infrastructure such as the banking system, the electric power grid, the public switched telecommunications network, and the air traffic control system are central to so many dimensions of modern life that protecting these elements must have a high priority. The federal government has an important stake in assuring that its important and sensitive political, economic, law enforcement, and military information, both classified and unclassified, is protected from foreign governments or other parties whose interests are hostile to those of the United States.

Cryptographic Dimensions of Information Security Solutions

Information vulnerabilities cannot be eliminated through the use of any single tool. For example, it is impossible to prevent with technical means a party authorized to view information from improperly disclosing that information to someone else. However, as part of a comprehensive approach to addressing information vulnerabilities, cryptography is a powerful tool that can help to assure the confidentiality and integrity of information in transit and in storage and to authenticate the asserted identity of individuals and computer systems. Information that has been properly encrypted cannot be understood or interpreted by those lacking the appropriate cryptographic “key”; information that has been integrity-checked cannot be altered without detection. Properly authenticated identities can help to restrict access to information resources to those properly authorized individuals and to take fuller advantage of audit trails to track down parties who have abused their authorized access.

Law Enforcement and National Security Dilemmas Posed by Cryptography

For both law enforcement and national security, cryptography is a two-edged sword. The public debate has tended to draw lines that frame the policy issues as the privacy of individuals and businesses against the needs of national security and law enforcement. While such a dichotomy does have a kernel of truth, when viewed in the large, this dichotomy is misleading. If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States. Framing discussion about national cryptography policy in this larger law enforcement and national security context would help to reduce some of the polarization among the relevant stakeholders.

On the other hand, cryptography intended primarily to maintain the confidentiality of information that is available to the general public for legitimate purposes such as defending against information theft is also available for illegitimate purposes such as terrorism. Encryption thus does pose a threat to the capability that law enforcement authorities may seek under appropriate legal authorization to gain access to information for the purpose of investigating and prosecuting criminal activity. Encryption also poses a threat to intelligence gathering for national security

and foreign policy purposes, an activity that depends on access to information of foreign governments and other foreign entities.

Note that other applications of cryptography—for purposes of assuring data integrity and authenticating identities of users and computer systems—do not pose dilemmas for law enforcement and national security in the same way that confidentiality does.

National Cryptography Policy for the Information Age

For many years, concern over foreign threats to national security has been the primary driver of a national cryptography policy that has sought to maximize the protection of U.S. military and diplomatic communications while denying the confidentiality benefits of cryptography to foreign adversaries through the use of export controls on cryptography and related technical data. More recently, the U.S. government has aggressively promoted the domestic use of a certain kind of cryptography—escrowed encryption—that would provide strong protection for legitimate uses but would permit access by law enforcement officials when authorized by law. Today, these and other dimensions of current national cryptography policy generate considerable controversy.

All of the various stakes are legitimate: privacy for individuals, protection of sensitive or proprietary information for businesses, ensuring the continuing reliability and integrity of nationally critical information systems and networks, law enforcement access to stored and communicated information for purposes of investigating and prosecuting crime, and national security access to information stored or communicated by foreign powers or other entities and organizations whose interests and intentions are relevant to the national security and the foreign policy interests of the United States. Informed public discussion of the issues must begin by acknowledging the legitimacy both of information gathering for law enforcement and national security purposes and of information security for law-abiding individuals and businesses.

The conduct of the debate regarding national cryptography policy has been complicated because a number of participants have often invoked classified information that cannot be made public. However, the cleared members of the National Research Council's Committee to Study National Cryptography Policy (13 of the 16 committee members) concluded that **the debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis**. Classified material is often important to operational matters in specific cases, but it is neither essential to the big picture of why cryptography policy is the way it is nor required for the general outline of how technology will and policy should evolve in the future.

BOX ES.2 The Past and Future World Environment	
Past	Future Trends
Computing and communications were expensive and rare.	Computing and information acquisition, retrieval, and processing are inexpensive and ubiquitous. Rapid growth is evident in the development and deployment of diverse technology-enabled services.
Communications networks were analog and voice oriented; communications made heavy use of dedicated lines.	Communications networks are digital and oriented toward video and data transmissions.
Telecommunications was controlled by a small number of players. The U.S. economy was unquestionably dominant in the world.	Communications make heavy use of shared infrastructure and multiple channels of different media (e.g., satellites, wireless). Passive eavesdropping is thus harder to detect. Telecommunications involves a large number of players. The U.S. economy is important but not dominant in the world, and it is increasingly interlinked with allies, customers, suppliers, vendors, and competitors all over the world.
The economy was oriented toward material production. The security threat was relatively homogeneous (Soviet Union and Cold War).	The economy is oriented toward information and services. Security threats are much more heterogeneous than in the Cold War, both in origin and in nature.
Cryptography was used primarily for military and diplomatic purposes. Government had a relative monopoly on cryptographic expertise and capability.	Cryptography has important applications throughout all aspects of society. Non-governmental entities have significant expertise and capability built on an open, public, and expanding base of scientific and technical knowledge about cryptography.

The problems of information vulnerability, the legitimacy of the various national interests described above, and trends such as those outlined in Box ES.2 point to the need for a concerted effort to protect vital information assets of the United States. Cryptography is one important element of a comprehensive U.S. policy for better information security.

The committee believes that **U.S. national policy should be changed to support the broad use of cryptography in ways that take into account competing U.S. needs and desires for individual privacy, international economic competitiveness, law enforcement, national security, and**

world leadership. Because cryptography is an important tool for protecting information and because it is very difficult for governments to control, the committee believes that widespread nongovernment use of cryptography in the United States and abroad is inevitable in the long run. Accordingly, the proper role of national cryptography policy is to facilitate a judicious transition between today's world of high information vulnerability and a future world of greater information security, while to the extent possible meeting the legitimate needs of law enforcement and information gathering for national security and foreign policy purposes.

The committee found that **current national cryptography policy is not adequate to support the information security requirements of an information society.** Indeed, current policy discourages the use of cryptography, whether intentionally or not, and in so doing impedes the ability of the nation to use cryptographic tools that would help to remediate certain important vulnerabilities. National cryptography policy should support three objectives:

1. Broad availability of cryptography to all legitimate elements of U.S. society;
2. Continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including but not limited to U.S. computer, software, and communications companies; and
3. Public safety and protection against foreign and domestic threats.

Objectives 1 and 2 argue for a policy that places few government restrictions on the use of cryptography and actively promotes the use of cryptography on a broad front. Objective 3 argues that some kind of government policy role in the deployment and use of cryptography for confidentiality may continue to be necessary for public safety and national security reasons. These three objectives can be met within a framework recognizing that **on balance, the advantages of more widespread use of cryptography outweigh the disadvantages.**

The recommendations below address several critical policy areas. In the interests of brevity, only short rationales for the recommendations are given here. The reader is urged to read Chapter 8 of the report for essential qualifications, conditions, and explanations.

A FRAMEWORK FOR NATIONAL CRYPTOGRAPHY POLICY

The framework for national cryptography policy should provide coherent structure and reduce uncertainty for potential vendors and for nongovernment and government users of cryptography in ways that policy does not do today.

EXECUTIVE SUMMARY

7

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. Recommendation 1 is made to reinforce this particular aspect of the Administration's cryptography policy.

Recommendation 2: National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of law. Only a national discussion of the issues involved in national cryptography policy can result in the broadly acceptable social consensus that is necessary for any policy in this area to succeed. A consensus derived from such deliberations, backed by explicit legislation when necessary, will lead to greater degrees of public acceptance and trust, a more certain planning environment, and better connections between policy makers and the private sector on which the nation's economy and social fabric rest.

Recommendation 3: National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces. As cryptography has assumed greater importance to nongovernment interests, national cryptography policy has become increasingly disconnected from market reality and the needs of parties in the private sector. Experience with technology deployment suggests that reliance on market forces is generally the most effective way to promote the widespread use of a new technology. Since the committee believes that widespread deployment and use of cryptography are in the national interest, it believes that national cryptography policy should align itself with user needs and market forces to the maximum feasible extent. Accordingly, national cryptography policy should emphasize the freedom of domestic users to determine cryptographic functionality, protection, and implementations according to their security needs as they see fit; encourage the adoption of cryptographic standards by the federal government and private parties that are consistent with prevailing industry practice; and support the use of algorithms, product designs, and product implementations that are open to public scrutiny.

EXPORT CONTROLS

For many years, the United States has controlled the export of cryptographic technologies, products, and related technical information as mu-

nitions (on the U.S. Munitions List administered by the State Department). However, the current export control regime for cryptography is an increasing impediment to the information security efforts of U.S. firms competing and operating in world markets, developing strategic alliances internationally, and forming closer ties with foreign customers and suppliers. Export controls also have had the effect of reducing the domestic availability of products with strong encryption capabilities. Looking to the future, both U.S. and foreign companies have the technical capability to integrate high-quality cryptographic features into their products and services. U.S. export controls may stimulate the growth of significant foreign competition for U.S. vendors to the detriment of both U.S. national security interests and U.S. business and industry.

Some relaxation of today's export controls on cryptography is warranted. Relaxation would create an environment in which U.S. and multinational firms and individuals could use the same security products in the United States and abroad, thereby supporting better information security for U.S. firms operating internationally. It would also increase the availability of good cryptography products in the United States. Finally, it would help to solidify U.S. leadership in a field critical to national security and economic competitiveness.

At the same time, cryptography is inherently dual-use in character, with important applications to both civilian and military purposes. Because cryptography is a particularly critical military application for which few technical alternatives are available, retention of some export controls on cryptography will mitigate the loss to U.S. national security interests in the short term, allow the United States to evaluate the impact of relaxation on national security interests before making further changes, and "buy time" for U.S. national security authorities to adjust to a new technical reality.

Recommendation 4: Export controls on cryptography should be progressively relaxed but not eliminated.

Recommendation 4.1—Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable.¹ Today, products with encryption capabilities that incorporate the 56-bit DES algorithm provide this level of confidentiality and

¹For purposes of Recommendation 4.1, a product that is "easily exportable" will automatically qualify for treatment and consideration (i.e., commodity jurisdiction, or CJ) under the Commerce Control List (CCL). Automatic qualification refers to the same procedure under which software products using RC2 or RC4 algorithms for confidentiality with 40-bit key sizes currently qualify for the CCL.

should be easily exportable. As a condition of export, vendors of products covered under this Recommendation 4.1 (and 4.2 below) would be required to provide to the U.S. government full technical specifications of their product and reasonable technical assistance upon request in order to assist the U.S. government in understanding the product's internal operations.

Recommendation 4.2—Products providing stronger confidentiality should be exportable on an expedited basis to a list of approved companies if the proposed product user is willing to provide access to decrypted information upon legally authorized request. Firms on the list would agree to abide by a set of requirements described in Chapter 8 that would help to ensure the ability of the U.S. government to obtain the plaintext of encrypted information upon presentation of a proper law enforcement request. (Plaintext is the information that was initially encrypted.)

Recommendation 4.3—The U.S. government should streamline and increase the transparency of the export licensing process for cryptography. Greater efforts in this area would reduce uncertainty regarding rules, time lines, and the criteria used in making decisions about the exportability of particular products. Chapter 8 describes specific possible steps that might be taken.

ADJUSTING TO NEW TECHNICAL REALITIES

As noted above, cryptography is helpful to some dimensions of law enforcement and national security and harmful to others. The committee accepts that the onset of an information age is likely to create many new challenges for public safety, among them the greater use of cryptography by criminal elements of society. If law enforcement authorities are unable to gain access to the encrypted communications and stored information of criminals, some criminal investigations and prosecutions will be significantly impaired. For these reasons, specific steps should be taken to mitigate these difficulties. In the realm of national security, new capabilities are needed to better cope with the challenges that cryptography presents.

Since 1993, the approach of the U.S. government to these problems has been an aggressive promotion of escrowed encryption (see Chapter 5) as a pillar of the technical foundation for national cryptography policy, primarily in response to the law enforcement concerns described above. Initiatives promoted by the U.S. government include the Escrowed Encryption Standard (a voluntary Federal Information Processing Standard

for secure voice telephony), the Capstone/Fortezza initiative that provides escrowed encryption capabilities for secure data storage and communications, and a recent proposal to liberalize export controls on certain encryption products if the keys are “properly escrowed.”

The committee understands the Administration's rationale for promoting escrowed encryption but believes that escrowed encryption should be only one part of an overall strategy for dealing with the problems that encryption poses for law enforcement and national security. The committee's view of an appropriate overall strategy is described below, and escrowed encryption is the focus of Recommendation 5.3.

Recommendation 5: The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age. Over the past 50 years, both law enforcement and national security authorities have had to cope with a variety of changing technological circumstances. For the most part, they have coped with these changes quite well. Today, however, “business as usual” will not suffice to bring agencies responsible for law enforcement and national security into the information age. At the same time, both law enforcement and national security have demonstrated considerable adaptability to new environments; this record of adaptability provides considerable confidence that they can adapt to a future of digital communications and stored data as well.

The specific subrecommendations that follow attempt to build on this record. They are intended to support law enforcement and national security missions in their totality—for law enforcement, in both crime prevention and crime prosecution and investigation; and for national security, in both the defense of nationally critical information systems and the collection of intelligence information.

Recommendation 5.1—The U.S. government should actively encourage the use of cryptography in nonconfidentiality applications such as user authentication and integrity checks. These applications are particularly important in addressing vulnerabilities of nationally critical information systems and networks. Furthermore, these applications of cryptography are important crime-fighting measures. To date, national cryptography policy has not fully supported such nonconfidentiality uses. Some actions have been taken in this area, but these actions have sometimes conflicted with government concerns about confidentiality. As importantly, government has expressed considerably more concern in the public debate regarding the deleterious impact of widespread cryptography used for confidentiality than over the deleterious impact of not deploying cryptographic capabilities for user authentication and data integ-

urity. Chapter 8 provides a number of illustrative examples to demonstrate what specific actions government can take to promote nonconfidentiality applications of cryptography.

Recommendation 5.2—The U.S. government should promote the security of the telecommunications networks more actively. At a minimum, the U.S. government should promote the link encryption of cellular communications² and the improvement of security at telephone switches. Such steps would not diminish government access for lawfully authorized wiretaps through the requirements imposed on carriers today to cooperate with law enforcement in such matters. Furthermore, by addressing public demands for greater security in voice communications that are widely known to be nonsecure through the telecommunications service providers, these measures would also reduce the demand for (and thus the availability of) devices used to provide end-to-end encryption of voice communications. Without a ready supply of such devices, a criminal user would have to go to considerable trouble to obtain a device that could thwart a lawfully authorized wiretap.

Recommendation 5.3—To better understand how escrowed encryption might operate, the U.S. government should explore escrowed encryption for its own uses. To address the critical international dimensions of escrowed communications, the U.S. government should work with other nations on this topic. Escrowed encryption has both benefits and risks. The benefits for law enforcement and national security are that when escrowed encryption is properly implemented and widely deployed, law enforcement and national security authorities will be able to obtain access to escrow-encrypted data in specific instances when authorized by law. Escrowed encryption also enables end users to recover encrypted stored data to which access has been inadvertently lost. The risk to end users is that escrowed encryption provides a potentially lower degree of confidentiality because it is specifically designed to permit exceptional access by parties not originally intended to have access to the encrypted data.

Aggressive government promotion of escrowed encryption is not appropriate at this time for several reasons: the lack of operational experi-

²“Link encryption” refers to the practice of encrypting information being communicated in such a way that it is encrypted only in between the node from which it is sent and the node where it is received; while the information is at the nodes themselves, it is unencrypted. In the context of link encryption for cellular communications, a cellular call would be encrypted between the mobile handset and the ground station. When carried on the landlines of the telephone network, the call would be unencrypted.

ence with how a large-scale infrastructure for escrowed encryption would work; the lack of demonstrated evidence that escrowed encryption will solve the most serious problems that law enforcement authorities face; the likely harmful impact on the natural market development of applications made possible by new information services and technologies; and the uncertainty of the market response to such aggressive promotion. At the same time, many policy benefits can be gained by an operational exploration of escrowed encryption by the U.S. government for government applications; such exploration would enable the U.S. government to develop the base of experience on which to build a more aggressive promotion of escrowed encryption should circumstances develop in such a way that encrypted communications come to pose a significant problem for law enforcement.

Recommendation 5.4—Congress should seriously consider legislation that would impose criminal penalties on the use of encrypted communications in interstate commerce with the intent to commit a federal crime. The purpose of such a statute would be to discourage the use of cryptography for illegitimate purposes, thus focusing the weight of the criminal justice system on individuals who were in fact guilty of criminal activity rather than on law-abiding citizens and criminals alike. Any statute in this area should be drawn narrowly.

Recommendation 5.5—High priority should be given to research, development, and deployment of additional technical capabilities for law enforcement and national security for use in coping with new technological challenges. Such R&D should be undertaken during the time that it will take for cryptography to become truly ubiquitous. These new capabilities are almost certain to have a greater impact on future information collection efforts than will aggressive attempts to promote escrowed encryption to a resistant market.

THE POLICY RELATIONSHIP BETWEEN INFORMATION SECURITY AND CRYPTOGRAPHY

Although this report is concerned primarily with national cryptography policy, any such policy is only one component of a national information security policy. Without a forward-looking and comprehensive national information security policy, changes in national cryptography policy may have little operational impact on U.S. information security.

Recommendation 6: The U.S. government should develop a mechanism to promote information security in the private sector. As is widely

EXECUTIVE SUMMARY

13

acknowledged, the U.S. government is not well organized to meet the challenges presented by an information society, and no government agency has the responsibility to promote information security in the private sector. Absent a coordinated approach to promoting information security, the needs of many stakeholders may well be given inadequate attention and notice; those who are pursuing enhanced information security and those who have a need for legal access to stored or communicated information must both be included in a robust process for managing the often-competing issues and interests that will inevitably arise over time. Government has an important role in actively promoting the security of information systems and networks critical to the nation's welfare (e.g., the banking and financial system, the public switched telecommunications network, the air traffic control system, the electric power grid). In other sectors of the economy, the role of the U.S. government should be limited to providing information and expertise. Chapter 8 provides some illustrative examples of what the government might do to promote information security in the private sector.

CONCLUSION

The committee believes that its recommendations will lead to enhanced confidentiality and protection of information for individuals and companies, thereby reducing economic and financial crimes and economic espionage from both domestic and foreign sources. In addition, they will result in improved security and assurance for the information systems and networks used by the nation—a more secure national information infrastructure. While the recommendations will in these ways contribute to the prevention of crime and enhance national security, the committee recognizes that the spread of cryptography will increase the burden of those in government charged with carrying out certain specific law enforcement and intelligence activities. It believes that widespread commercial and private use of cryptography in the United States and abroad is inevitable in the long run and that its advantages, on balance, outweigh its disadvantages. Thus, the committee concluded that the overall interests of the government and the nation would best be served by a policy that fosters a judicious transition toward the broad use of cryptography.

[CYBERSECURITY](#)

Making Progress on the Encryption Debate

By [Herb Lin](#) Tuesday, February 24, 2015, 1:24 PM

[In a recent debate](#) between NSA director Mike Rogers and Yahoo Chief Information Security Officer Alex Stamos, the topic of law-enforcement restricted access to encrypted communications once again came up.

To summarize the debate as it has been expressed to date, one side believes in encryption that only the user can decrypt. Those on this side of the debate (call it Side A) include large technology companies such as Apple, Yahoo, Google, and Microsoft and also privacy advocates such as the ACLU and EFF. Those on the other side of the debate (call it Side B) acknowledge the value of strong encryption to protect confidential information, but want to be able to decrypt to the underlying information without the user's knowledge or consent when they are legally authorized for such access. Those on Side B include the FBI and the Justice Department.

Side B proposes a technological solution to the problem—a mechanism to decrypt the information that can be accessed by law enforcement authorities and no one else—this is often known as a NOBUS solution, where “nobody but us” (NOBUS) can gain access. (According to the report of the debate referenced above—the NSA believes in the technological feasibility of a NOBUS solution.)

Side A argues that it's already hard enough to build secure systems and that introducing a NOBUS solution will inevitably make the system vulnerable to unauthorized access to the decrypting mechanism. That is,

they argue that technological impossibility of having access that is limited only to law enforcement authorities, and thus that NOBUS is not an appropriate feature (or bug, depending on how you see it) to introduce into any encryption system.

The debate—now 20 years old (think Clipper chip)—is entirely polarized, because there is no common ground in the middle. But when I unpack the claims on both sides, I find a real conceptual mess. No one taking Side A can provide a **proof** that the NOBUS mechanism will eventually become available to unauthorized parties. No one taking Side B can provide a proof that it **is** possible to build a tamperproof mechanism for NOBUS access. And so the argument continues to rage, as a clash of absolutes.

But the real technological issue is one of time scale. It is probably true that NOBUS access can't be kept secure forever. But it doesn't need to be kept forever. If a way to break NOBUS access takes 1000 years to develop, then it doesn't matter. If NOBUS access lasts for 1 minute, then it's clearly not workable. So somewhere between 1000 years and 1 minute, there's a threshold (a fuzzy threshold with big error bars, to be sure) where the idea of NOBUS making sense technically changes over to not making sense.

Viewed in these terms, it seems to be a problem of risk management, namely "For any given NOBUS mechanism, how might one estimate the period that it might plausibly remain secure, and what are the error bars around that estimate?" If we had such numbers, we might be able to make reasonable decisions about whether a given NOBUS mechanism might be technologically feasible or not.

Taking this approach has the virtue of separating the values issue from the technical issue. Some (maybe many) on Side A are opposed **in principle** to the idea of any access to encrypted communications that

are not authorized by the user. Others may favor Side A primarily because they do not believe that NOBUS is a viable technical approach, but would go along with Side B if it were.

[Note added after initial post.] I should also point out that NOBUS access does not necessarily presume that the holders of the encrypted data will have the ability to decrypt it. Thus, the tech companies will not themselves be able to decrypt data if and when other countries demand access.]

So I would propose that the debate move forward in the following way. Side B proponents should propose a specific NOBUS mechanism, much as they once did in the 1990s with the Clipper chip. And they should present an analysis that says why the mean time to compromise is closer to 1000 years than to one minute. Once that proposal is in hand for public scrutiny, Side A should show why the mean time to compromise is closer to one minute than to 1000 years. The analyses of Sides A and B can thus be compared. If it turns out that A's analysis is more plausible than B's, we can refrain from considering that mechanism further. If it turns out that B's analysis is more plausible than A's, then we can have an argument that is centered on the values proposition and not obscured by a technical smokescreen.

From my perspective, this would be progress.

Topics: [Cybersecurity](#), [Privacy: Technology](#), [Surveillance](#), [Privacy](#)



Dr. Herb Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Research Fellow at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cybersecurity and

cyberspace, and he is particularly interested in and knowledgeable about the use of offensive operations in cyberspace, especially as instruments of national policy. In addition to his positions at Stanford University, he is Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served from 1990 through 2014 as study director of major projects on public policy and information technology, and Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

[MORE ARTICLES >](#)

RELATED ARTICLES

Director Comey and the Real Threats

Susan Landau Fri, Jul 3, 2015, 10:01 AM

Breach of Trust, OPM, and the Intelligence Community

Benjamin Wittes Tue, Jun 30, 2015, 4:00 PM

Whose Fault is the OPM Hack, Really? Part II

Benjamin Wittes Tue, Jun 30, 2015, 12:36 PM

Whose Fault is the OPM Hack Really?

Benjamin Wittes Thu, Jun 25, 2015, 1:24 PM

What is the DoD's Position on Backdoors in Security Systems?

Bruce Schneier Wed, Jun 24, 2015, 10:54 AM

SUPPORT LAWFARE

Learn how to support to the publication of this site

[CYBERSECURITY](#)

Echoes From the Past on Encryption

By [Herb Lin](#) Wednesday, February 18, 2015, 3:44 PM

[President Obama's recent comments](#) calling for a public debate on encryption are, as [Susan Landau recently pointed out](#), some much-needed straight talk about the issue. In Susan's words, "the debate is not about perfect security versus privacy and civil liberties; it is about our society's willingness to accept risk."

What's striking about this debate is that it's nearly 2 decades old. [Here's the words of Louis Freeh](#), then director of the FBI:

"The looming spectre of the widespread use of robust, virtually uncrackable encryption is one of the most difficult problems confronting law enforcement. . . . At stake are some of our most valuable and reliable investigative techniques, and the public safety of our citizens. . . . Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity."

Director Freeh and others predicted disaster if the encryption problem was not solved, but their prediction was wrong. Even the horrific events of September 11, 2001 were the result of organizational failures in the U.S. government, and not because of encryption.

But are things different today? It's certainly true that the number of ways to communicate and store information electronically has gone up, and we are all more dependent on technology for our daily activities. And for

everyone, there's more awareness of security issues. But many things are the same, such as the unchanging reality that encryption can be used to conceal crime and terrorist activities and to protect against them.

Another important but overlooked point is that criminals are not generally smarter than the rest of us. Most of us have forgotten our password and had to ask for help from our employer or our service provider. If I'm on my own to remember my password, I will make sure I have continuing access to it—which means I am likely to record it somewhere that I can still get it. If I can get it, so can law enforcement officials. Criminals forget their passwords too, and if they have not written them down somewhere, certain crimes will not happen because the would-be perpetrators will not be able to access the information needed to commit them. Remember also that copies of data often exist in places other than on personal devices, as people back up and synchronize their data across computers in several locations.

Apple and Google have promised to deliver encryption that only their customers will be able to unlock. But some customers will soon demand that these vendors be able to unlock the encryption when they have forgotten or lost their keys. Thus, subsequent versions of Apple and Google products may well offer key recovery capabilities to customers, and law enforcement authorities will have access to those capabilities as well. [Louis Freeh made just such an argument in 1997](#) when he noted that “rational thinking corporations will . . . insist on using key recovery encryption for electronically stored information.” When (as I predict) Apple and Google start to offer key recovery services to their customers, law enforcement authorities will have yet another path to pursue.

Do new encryption capabilities pose problems for law enforcement? In some cases, they surely will, just as criminal investigations have surely been stymied by an inability to find evidence that was safely hidden in

unknown safe deposit boxes. But our law enforcement agencies are dedicated, hardworking, and smart, and the evidence from the first round of the crypto wars suggests that they will be able to adapt a new technological environment without the difficulties of legislation interfering with the market-based decisions of the nation's information technology companies.

Topics: [Cybersecurity](#)

0 Comments

Sort by Newest



Add a comment...

 Facebook Comments Plugin



Dr. Herb Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Research Fellow at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, and he is particularly interested in and knowledgeable about the use of offensive operations in cyberspace, especially as instruments of national policy. In addition to his positions at Stanford University, he is Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served from 1990 through 2014 as study director of major projects on public policy and information technology, and Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services

Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

[MORE ARTICLES >](#)

RELATED ARTICLES

Director Comey and the Real Threats

Susan Landau Fri, Jul 3, 2015, 10:01 AM

Breach of Trust, OPM, and the Intelligence Community

Benjamin Wittes Tue, Jun 30, 2015, 4:00 PM

Whose Fault is the OPM Hack, Really? Part II

Benjamin Wittes Tue, Jun 30, 2015, 12:36 PM

Whose Fault is the OPM Hack Really?

Benjamin Wittes Thu, Jun 25, 2015, 1:24 PM

What is the DoD's Position on Backdoors in Security Systems?

Bruce Schneier Wed, Jun 24, 2015, 10:54 AM

SUPPORT LAWFARE

Learn how to support to the publication of this site

[PRIVACY](#)

The Encryption Wars Continue

By [Paul Rosenzweig](#) Saturday, September 20, 2014, 12:31 PM

For quite a while it has been the case [that properly implemented encryption will defeat efforts to crack it](#) (at least using current technology). Yet it has been the case for an equally long time that very few people actually use encryption to protect their vital secrets – not journalists, not criminals, and most assuredly not the (perhaps mythical) “average layman user.”

Why is that the case? Nobody knows for sure of course, but speculation reasonably focuses on a range of possibilities: ignorance; complexity; laziness and hubris lead the list. User error is a frequent issue. Of all of these, I tend to think complexity and laziness lead the list – that is, most encryption programs are difficult to use and need to be installed. They don’t have “one button” applications and they are not “on” by default.

That seems to be changing. And the reason is, as many have predicted, less about the utility of encryption and more about the business necessity of appearing resistant to government surveillance. That explains Apple’s recent decision [to make encryption the default in its new operating system iOS8](#), that is being delivered in the new iPhone6. For data stored on a device the user (and only the user) will have the passphrase to unlock the data. The move is so widely lauded that [Google moved quickly to follow with its own Android operating system](#).

There are a number of legal and practical implications of this transition, almost all of which reset the balance between security and liberty in a way that tends to favor more libertarian impulses:

- The transition will essentially render moot last terms decision in [*Riley v. California*](#) (proving once again that by the time the Supreme Court addresses a technological issue the issue is irrelevant!). *Riley* held that, as a general matter, law enforcement will need a search warrant to access data on a cell phone. While that certainly raises the bar for access, it does not do so to an impossible degree. Probable cause is, after all, a standard that law enforcement establishes every day around the country.
- By contrast, however, the new operating systems act technologically to divest Apple and Google of any ability to respond to a warrant – they can't produce what they don't have. So this Fourth Amendment question now becomes converted to a Fifth Amendment question – whether or not the owner of the cell phone can be compelled to unlock his phone by providing the passphrase. Unlike the Fourth Amendment context, this privilege is absolute. If courts recognize the Fifth Amendment protection then the data on the phone is absolutely unavailable to law enforcement – which would be a significantly greater crimp in law enforcement (or counter-terrorism) investigations.
- That makes the growing debate over the extent of a Fifth Amendment privilege even more salient. When last I wrote about it, the latest word was an Eleventh Circuit case [*In Re: Grand Jury Subpoena \(US v. Doe\)*](#), which held that disclosure of the passphrase could not be compelled. That debate is not, however, over. Earlier this year, the Massachusetts Supreme Judicial Court ruled to the contrary. In [*Commonwealth v. Gelfgatt*](#), the Court held that disclosing the passphrase disclosed only the capacity to decrypt, which was a

“foregone conclusion” and did not implicate any proof of authenticity, control, or knowledge. That seems to me a highly suspect conclusion – but it is evidence that the legal question is not settled in the least.

- Notwithstanding all of the *strum und drang* there may actually be less to these announcements than meets the eye. Why? Because the encryption default lock applies =only= to data on the phone itself. As [we’ve noted before](#), unless you encrypt data before you store it with a cloud service provider then it is the provider’s encryption, not the user’s, that matters. And, of course, most Apple users store data in the iCloud (they like to synchronize data across all their devices) and Android users store their data in Google’s cloud storage for the same reason. And that sort of synchronicity remains the default “on” function in both operating systems. So, all that data stored behind a hard encryption lock on your phone is accessible from your cloud storage provider as a back up. And that [data may sometimes be accessed with a subpoena](#) – that is, on a basis requiring less than probable cause. So the only way to be completely privacy protective is to turn off the cloud storage portions of your new iPhone or Android tablet – hardly a way to advance efficiency and productivity (and also, perhaps, a sign that law enforcement fears are overstated).
- Meanwhile the same business reasons that are driving the adoption of encryption are likely to frustrate any effort to end the synchronicity default. Apple makes its money by offering you the seamless cross-platform product. And Google’s business model involves its access to your data for advertising purposes. So don’t expect a default “off” switch for cloud storage anytime soon.
- Finally, it is worth pondering the larger individual trade-off question. While I certainly respect the opinion of those who perceive government surveillance as a threat, I sometimes wonder if they are

forgoing too many technological advantages in the pursuit of personal privacy. Encrypting your data and turning off your synchronization means that if you forget your passphrase your data is gone ... totally gone. It means that you can't automatically see a picture you took on your iPhone when you go to create a family newsletter on your Mac. One answer, of course, is differential encryption (protecting only sensitive data), which is what I do with my client files. But overall, we sometimes don't recognize, I think, the efficiency/security tradeoff.

Topics: [Privacy](#), [Cybersecurity](#), [Privacy: Technology](#)



Paul Rosenzweig is the founder of Red Branch Consulting PLLC, a homeland security consulting company and a Senior Advisor to The Chertoff Group. Mr. Rosenzweig formerly served as Deputy Assistant Secretary for Policy in the Department of Homeland Security. He is a Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute. He also serves as a Professorial Lecturer in Law at George Washington University, a Senior Editor of the Journal of National Security Law & Policy, and as a Visiting Fellow at The Heritage Foundation.

[@RosenzweigP](#)

[MORE ARTICLES >](#)

RELATED ARTICLES

Surveillance State -- The Case of Germany

Paul Rosenzweig Wed, Jul 1, 2015, 9:00 AM

David E. Pozen on "Privacy-Privacy Tradeoffs"

Benjamin Wittes Mon, Jun 29, 2015, 2:22 PM

Did the 702 Suit Just Get Easier?

Paul Rosenzweig Sat, Jun 27, 2015, 11:27 AM

Patel Decided

Paul Rosenzweig Mon, Jun 22, 2015, 12:15 PM

Waiting for Patel

Paul Rosenzweig Thu, Jun 18, 2015, 8:30 AM

SUPPORT LAWFARE

Learn how to support to the publication of this site

Testimony by Peter Swire
Huang Professor of Law and Ethics
Scheller College of Business
Georgia Institute of Technology

Senate Judiciary Committee Hearing
“Going Dark: Encryption, Technology, and the Balance
Between Public Safety and Privacy”
July 8, 2015

Chairman Grassley, Ranking Member Leahy, and Members of the Committee, thank you for the opportunity to testify today on “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy.” I am Peter Swire, the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business. I have worked on encryption issues as a government official and scholar for two decades, including recently as a member of President Obama’s Review Group on Intelligence and Communications Technology. A more detailed biography is attached to the end of this testimony.

My testimony today is in three parts. First, the Review Group report concluded that strong cybersecurity and strong encryption should be vital national priorities. Our Recommendation 29 stated:

“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.”

The Review Group unanimously and clearly recommended that the U.S. Government vigorously encourage the use of strong encryption. With full awareness of the “going dark” concerns, we sharply criticized any attempt to introduce vulnerabilities into commercially available products and services, and found that even temporary vulnerabilities should be authorized only after administration-wide scrutiny. Based on the top-secret briefings and our experience, we found these policies would best fight cyber-crime, improve cybersecurity, build trust in the global communications infrastructure, and promote national security.

Second, it is more accurate to say that we are in a “Golden Age of Surveillance” than for law enforcement to assert that it is “Going Dark.” In previous writings,¹ I have agreed that there are indeed specific ways that law enforcement and national security agencies lose specific previous capabilities due to changing encryption technology. These specific losses, however, are more than offset by massive gains, including: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create digital dossiers about individuals’ lives.

The testimony specifically shows the enormous gains to law enforcement resulting from adoption in the past twenty years of digital smartphones and text messaging, the two areas most highlighted by law enforcement as examples of “going dark.” Although relatively few text messages were sent twenty years ago, by 2010 the number exceeded 6 trillion texts per year. For the predominant share of those messages, the content is available from the provider. Even for the subset where the content is encrypted, law enforcement can gain access to the meta-data, linking suspects and witnesses to their entire social graphs.

For text messages, it might be tempting to say that law enforcement could call the glass half-empty (some texts are encrypted) or half-full (some texts are in the clear). With over six trillion messages filling the cup, though, it takeschutzpah to say the glass is empty. Text messages are a prime example of a golden age of surveillance, and not of going dark.

Third, government-mandated vulnerabilities would threaten severe harm to cybersecurity, privacy, human rights, and U.S. technological leadership, while not preventing effective encryption by adversaries.

As occurred in the 1990’s, a diverse coalition of cybersecurity experts, technology companies, privacy experts, human rights activists, and others has expressed vociferous and united opposition to government-mandated encryption vulnerabilities.² My testimony highlights some of these concerns:

- Technology companies, even before Snowden, had multiple reasons to deploy strong encryption to enhance cybersecurity and customer trust. The ongoing development of encryption should thus not be seen primarily as a short-term response to Snowden’s revelations.
- Overwhelming technical problems and costs result from mandates to create vulnerabilities in encryption. A new report issued on July 7 is just the most recent, credible explanation of these technical issues.

¹ Peter Swire & Kenesa Ahmad, ‘Going Dark’ Versus a ‘Golden age for Surveillance’, CENTER FOR DEMOCRACY AND TECHNOLOGY, Nov. 28, 2011 (available at <https://cdt.org/blog/going-dark-versus-a-golden-age-for-surveillance/>).

² For one coalition letter, see https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf.

- U.S. Government support for encryption vulnerabilities increases cybersecurity problems in the “least trusted countries” and globally, and undermines U.S. human rights policies. The United States should be a strong example for cybersecurity and human rights, rather than an excuse used by repressive regimes to surveil U.S.-based businesses and individuals and clamp down on political dissent.
- Mandated vulnerabilities are bad industrial policy – they threaten U.S. technological leadership without preventing bad actors from using strong encryption.

In conclusion, providing access exceptions for U.S. law enforcement and intelligence agencies will be harmful, rather than helpful, to national security. Despite concerns of “going dark,” the steady increase of electronic communications worldwide provides these agencies with an ever-growing amount of valuable data and meta-data to use in identifying and pursuing targets of investigations. The inability to directly access the content of a small fraction of these communications does not warrant the subsequent damage that would result to privacy and to U.S. economic, diplomatic, and security interests.

I. Review Group: Strong Cybersecurity and Strong Encryption are Vital to National Security

In August, 2013 President Obama named me as one of five members of the Review Group on Intelligence and Communications Technology, to recommend policies in the wake of the Snowden revelations. Our report emphasized in strong terms the need for strong cybersecurity and strong encryption, without creating vulnerabilities for government access.³ The Review Group unanimously found these issues essential to achieving national security and other national goals in globalized information networks.

Multiple kinds of evidence support giving credence to the Review Group recommendations. The President’s tasking to the group made national security the first priority, along with other considerations such as relations with allies, economic effects, privacy and civil liberties, maintaining public trust, and addressing insider threats. The make-up of the group, along with my own role, showed a commitment to national security, informed by expertise in meeting each of these goals: Richard Clarke has served as cybersecurity coordinator and also anti-terrorist coordinator to Presidents of both political parties; Michael Morell has thirty years of experience in the intelligence community, including serving as acting Director of the CIA; both Cass Sunstein and Geoffrey Stone are eminent legal scholars, with particular

³ “Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technology” (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

expertise, respectively, in cost/benefit policy analysis⁴ and how to trade off security and civil liberties in times of crisis.⁵

The Review Group, in addition to the expertise of the members, received detailed briefings on encryption, cybersecurity, and related topics at the most highly classified levels. We met personally with top officials in meetings at the NSA, CIA, FBI, and elsewhere. We received particularly detailed briefings on national capabilities in encryption and decryption due to the NSA's leading role on encryption issues and also its Information Assurance Directorate's leading role in cybersecurity defense.⁶

Clear evidence establishes positive recognition of the Review Group's report and recommendations. Along with widespread coverage in the press, the Princeton University Press re-issued the Report in a paperback edition – the first time a federal report has received such treatment since the 9/11 Commission Report. President Obama and his administration have adopted numerous of our 46 recommendations; we have been told that the administration has adopted at least 70% of the recommendations in letter or in spirit. In addition, Congress has found the Report helpful. Each of the major provisions of the USA FREEDOM Act is consistent with one or more of the Review Group's recommendations.⁷

Based on the top-secret briefings and the knowledge of the members, the Review Group unequivocally recommended the following: strong encryption, without backdoors, is essential to cybersecurity, national security, and the prevention of cyber-crime. The Review Group was aware of law enforcement and intelligence agency concerns about “going dark.” We simply found no basis for weakening cybersecurity due to the going dark arguments.

Our discussion highlighted the central role of effective encryption for our global communications infrastructure generally, and specifically to address the “massive increase in cyber-crime”:

“Encryption is an essential basis for trust on the Internet; without such trust, valuable communications would not be possible. For the

⁴ Cass Sunstein, along with his numerous publications, served as Administrator for five years for the Office of Information and Regulatory Affairs of the U.S. Office of Management and Budget, which oversees cost/benefit analyses of federal regulations.

<http://hls.harvard.edu/faculty/directory/10871/Sunstein>.

⁵ Geoffrey R. Stone, *Perilous Times: Free Speech in Wartime from The Sedition Act of 1798 to The War on Terrorism* (2004), *Top Secret: When Our Government Keeps Us in the Dark* (2007), *War and Liberty: An American Dilemma* (2007).

⁶ See <https://www.nsa.gov/ia> for information on the IAD's role and activities.

⁷ Peter Swire, *The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years*, IAPP PRIVACY PERSPECTIVES, Jun. 8, 2015 (available at <https://privacyassociation.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years>).

entire system to work, encryption software itself must be trustworthy. Users of encryption must be confident, and justifiably confident, that only those people they designate can decrypt their data.

“The use of reliable encryption software to safeguard data is critical to many sectors and organizations, including financial services, medicine and health care, research and development, and other critical infrastructures in the United States and around the world. Encryption allows users of information technology systems to trust that their data, including their financial transactions, will not be altered or stolen. Encryption-related software, including pervasive examples such as Secure Sockets Layer (SSL) and Public Key Infrastructure (PKI), is essential to online commerce and user authentication. It is part of the underpinning of current communications networks. Indeed, in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud.”

Based on this analysis of the problem, we recommended vigorous U.S. government support for effective encryption, including a ban on subverting the security of generally available commercial products and services:

“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.”

Our concern with cyber-crime and cybersecurity extended to our discussion of cyber-vulnerabilities, including “Zero Day” attacks, defined as attacks where developers have had zero days to address the vulnerability. Review Group Recommendation 30 emphasized that vulnerabilities should be “quickly blocked, so that the underlying vulnerabilities are patched on US Government or other networks.” The Review Group recommended that, “when an urgent and significant national security policy can be addressed” by leaving a vulnerability unpatched, an agency of the US Government may be authorized to use the vulnerability “temporarily,” instead of “immediately fixing the underlying vulnerability.” Allowing the vulnerability to remain unpatched should be subject to “a senior-level, interagency approval process,” chaired by the National Security Council. To ensure that multiple perspectives are included before allowing such vulnerabilities, we

wrote that the process should involve “all offices and departments with relevant concerns, generally including the National Economic Council, State, Commerce, Energy, and Homeland Security.”

In conclusion on the Review Group, we unanimously and clearly recommended that the U.S. Government vigorously encourage the use of strong encryption. With full awareness of the “going dark” concerns, we sharply criticized any attempt to introduce vulnerabilities into commercially available products and services, and found that even temporary vulnerabilities should be authorized only after administration-wide scrutiny. Based on the top-secret briefings and our experience, we found these policies would best fight cyber-crime, improve cybersecurity, build trust in the global communications infrastructure, and promote national security.

II. Going Dark vs. a Golden Age of Surveillance

In 2011, I co-authored an article that has been widely cited in the encryption debates: “Going Dark vs. a Golden Age for Surveillance.”⁸ We did not agree that the FBI and other agencies are “going dark.” We acknowledged that, “due to changing technology, there are indeed specific ways that law enforcement and national security agencies lose specific previous capabilities.” We continued: “These specific losses, however, are more than offset by massive gains. Public debates should recognize that we are truly in a golden age of surveillance. By understanding that, we can reject calls for bad encryption policy.” The four years since writing that article, including my experience in the Review Group, have reinforced my confidence in these conclusions. The “going dark” claim is fundamentally incorrect; instead, government agencies are operating in a “golden age of surveillance.”

In this part of the testimony, I critically examine law enforcement statements about how common the “going dark” problem is. I then explain the basis for concluding that we are instead in a “golden age of surveillance,” and apply the analysis to encrypted text messaging and encrypted smartphones.

A. Challenges facing law enforcement access. FBI Director Comey’s article this week in LawFare highlights law enforcement concerns about “going dark.” Notably, Director Comey says that “our conversations and our ‘papers and effects’ will be locked in such a way that permits access only by participants to a conversation or the owner of the device holding the data.”⁹ Although I agree that there are certain subsets of communications that may not be reachable with a court order, Director Comey’s statement is so over-broad that policymakers should be

⁸ Peter Swire & Kenesa Ahmad, ‘Going Dark’ Versus a ‘Golden age for Surveillance’, CENTER FOR DEMOCRACY AND TECHNOLOGY, Nov. 28, 2011 (available at <https://cdt.org/blog/'going-dark'-versus-a-golden-age-for-surveillance/>).

⁹ James Comey, “Encryption, Public Safety, and “Going Dark,” July 6, 2015, <http://www.lawfareblog.com/encryption-public-safety-and-going-dark>.

extremely cautious about drawing policy conclusions from the assertion. Notably, Director Comey's statement essentially ignores the pervasive fact of cloud backup of content, and also greatly over-states the extent to which emails or other relevant content is or will be "dark" to law enforcement.

Before looking at the factual details, I pause to emphasize my support for highly effective law enforcement and intelligence activities to promote public safety and national security. My previous government work and other experience have given me considerable sympathy and, I believe, insight about the challenges facing law enforcement and intelligence agencies. During my time on the Review Group, for instance, one of my sons was serving as platoon leader for a motorized infantry unit in Kandahar. I can assure you that I wanted our signals intelligence to be absolutely outstanding to prevent an IED or other remote-control threat from harming his patrol. In 2000, the President's Chief of Staff entrusted me to serve as Chair of a White House Working Group on how to update wiretap laws for the Internet. That process included all of the major law enforcement and intelligence agencies, and resulted in a cleared administration bill, accepted by those agencies, that was later introduced in the Senate by Senator Leahy. Along with these years of experience working on law enforcement issues, I note that as a law student I worked for the Manhattan District Attorney's office, represented today by its leader, Mr. Vance. Doing a police ride-along for a night in Harlem is one of many experiences that has given me a vivid appreciation for how our police officers put themselves in harm's way as they face criminals and other threats to our public safety.

I have written previously about the central importance of cloud back-up and other stored records as a feature of law enforcement access to communications.¹⁰ There are numerous reasons why content on a modern smartphone or computer is very typically stored on the cloud, including the need for back-up and the ability for individuals or enterprises to access important information from different devices. In addition, the standard operation of a huge portion of apps on a smartphone includes automatic reporting of information to the app developer or others. For information stored in such cloud settings, standard functionality by the cloud provider means for a very wide range of applications that information is viewable by the cloud provider and not encrypted for access only by the user.

Despite concerns from law enforcement about end-to-end encryption (where content can be viewed only by the sender and recipient), my view is that the government in the vast majority of cases has retained and will retain access to plaintext of the content. For corporate accounts, the government can readily submit a court order to the corporate IT department, which will then turn over the content on pain of contempt of court. For individual email accounts, the government remains in a similarly strong position. The portion of individuals who use who end-to-end encryption remains vanishingly small. All of the largest email providers

¹⁰ "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," *International Data Privacy Law* (2012), doi: 10.1093/idpl/ips025.

today retain the ability to access the plaintext of emails when served a court order. Individuals who use smaller providers can choose end-to-end encryption (where the contents are available only to the sender and recipient), but few do so due to the high risk of problems – users who lose their keys lose access to all of their emails. How many of us would manage access to our bank accounts or other important accounts without the possibility of assistance if we forget the password? The risk of losing all access to one's communications is an enormous barrier to adoption. That is the single biggest reason in my view that I continue to doubt that we will see widespread adoption of end-to-end encryption.

In short, law enforcement may face small subsets of circumstances that match Director Comey's stated concern: locked devices or end-to-end encryption ("access only by the participants to a conversation"). At a factual level, however, we should remain highly alert to over-broad assertions about the pervasiveness of such "going dark."

B. Greater recent gains for lawful access.

The discussion here highlights 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. This information about any individual suspect is made even more useful because of the way that Big Data and data mining can help identify suspects.

1. Location information. Knowing the location over time of a suspect or witness is an enormous boon to law enforcement. For the first time in human history, we live in an age where most people carry a tracking device, the mobile phone. Location information comes standard with a wireless network – the phone company needs to know where your phone is to send you the call. A specific cell handles the call, so the network knows what cell you are in. Location information is tremendously useful for law enforcement and national security agencies. It can put a suspect at the scene of a crime, or establish an alibi. It can act as a "bug" without the need for the agency to place a bug on the suspect's person or property.

Even for the few who don't carry a phone, location is getting far more difficult to hide. Video surveillance cameras exist in stores, gas stations, and a proliferating variety of other places. Our cars' locations are tracked by EZ Pass, parking garages, and many more. Going forward, as the Internet of Things multiplies the sensors in daily life, we will see an exponential increase in the density of records about our individual location. When it comes to location, the maps are increasingly lit up for law enforcement, and emphatically not dark.

2. Meta-data reveals confederates and co-conspirators. The debates since Snowden have sensitized us all to the power and importance of meta-data. Congress, in the USA-FREEDOM Act, recently set important new limits on

government bulk collection of meta-data, precisely out of recognition of how much meta-data reveals.

The explosive increase in meta-data provides unprecedented information to law enforcement and intelligence agencies about a suspect or witness' confederates and co-conspirators. For many investigations, *who* is called is at least as important as *what* is said in the call. The investigator gets leads on whom else to investigate and can follow those leads to the contact's contacts, and so on. Nothing in the USA-FREEDOM Act limited the ongoing expansion of meta-data held by the private sector.

The importance of confederates has become famous in social networking. The term "social graph" was coined in connection with social networks to describe the phenomenon of "the global mapping of everybody and how they're related."¹¹ For investigatory agencies, mapping everybody and how they are related is extremely useful.

At some level, all of us realize the rapid increase in the density of our communications in recent years. The Pew Foundation, for instance, reports that 8% of Internet users were on social media in 2005, compared with 61% in 2010 and 74% in 2014.¹² With wireless phones and unlimited calling plans, the volume of our phone calls has skyrocketed, documenting in detail whom we speak with. VoiP calls through services such as Skype and Facetime similarly document the to/from information. E-mails have become a pervasive feature of life for many people; the emergence of global web mail providers, and nationwide service of process provided in the USA PATRIOT Act, gives agencies the convenience of serving many lawful requests to a small number of providers. Techniques for masking meta-data enormously lag behind current encryption techniques for content.

Our wireline, wireless, and VoiP calls, along with texts and social networking records are treasure troves of information for investigatory agencies. In the bygone era of face-to-face communications, no trace was usually left regarding whom a suspect had talked with. Today, by contrast, an individual would need to abstain from many everyday activities, over a period of years, to prevent the government from obtaining information about his or her contacts. The identity of those contacts helps lead investigators to additional targets of interest, thereby painting a broader and more precise picture of potential criminal or national security activity.

3. Digital dossiers and Big Data. Information about location and a person's confederates, in turn, are simply examples of the larger trend towards detailed personal records. Privacy scholars and regulators such as the Federal Trade Commission have documented the multi-dimensional expansion of personal

¹¹ <http://www.cbsnews.com/stories/2010/04/21/tech/main6418458.shtml>.

¹² <http://www.pewinternet.org/data-trend/social-media/social-media-use-all-users/>

information in the hands of data brokers,¹³ banks, hospitals, online advertisers, government agencies, and other record holders.¹⁴ The new era of “Big Data” includes advanced analytics that are to mine the data in these numerous databases. Although a few people attempt to live “off the grid,” this is not a feasible option for the vast majority of citizens in developed countries. Once an individual is identified as a target, the government – via lawful process – can access information specific to that individual in unprecedented detail.

C. Going Dark vs. Golden Age for text messages. Two areas of concern that law enforcement has highlighted have been the possibility of end-to-end encryption for text messages and new policies for mobile devices that ensure there is no “master key” to allow law enforcement access to the device. For both of these examples, the law enforcement claims to “going dark” turn out, upon inspection, to validate the view that we are in a golden age of surveillance.

For text messages, law enforcement has expressed concerns that some software, such as iMessage and WhatsApp, provides end-to-end encryption of the content. The idea of “going dark” is that law enforcement has lost something – they used to be able to see something, and now it is dark. But that is not what has happened. Not so long ago, there were no text messages – in almost all instances, daily communications never created a record of content, because we spoke to someone in our presence, or called someone on a non-wiretapped phone.

A much more accurate comparison with past practice is that law enforcement has gained an inestimable boon – the recorded meta-data of text messages. The history of SMS (short message service) illustrates the point. According to one source, the number of SMS sent by a typical cell phone user in 1995 was .4 per month, rising to 35 per user per month by 2000. By 2010, when per-text charges for text messaging were becoming obsolete, an estimated *6.1 trillion* SMS text messages were sent, in addition to the enormous quantity of text messages sent through Facebook Messenger, WhatsApp, and other data text services.¹⁵

For text messaging, therefore, law enforcement has experienced the new brightness of literally trillions of text messages per year. For the predominant share of those messages, the content is available from the provider. Even for the subset where the content is encrypted, law enforcement can gain access to the meta-data, linking suspects and witnesses to their entire social graphs.

¹³ FED. TRADE COMM’N, DATA BROKERS A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014) (available at <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>).

¹⁴ Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313301).

¹⁵ The statistics here are taken from https://en.wikipedia.org/wiki/Short_Message_Service; ITU, THE WORLD IN 2010 ICT FACTS AND FIGURES (2010) (available at <http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf>).

For text messages, it might be tempting to say that one can call the glass half-empty or half-full for law enforcement. With over six trillion messages filling the cup, though, it takeschutzpah to say the glass is empty. Text messages are a prime example of a golden age of surveillance, and not of going dark.

D. Going Dark vs. Golden Age for device encryption. Historical perspective similarly helps us understand going dark vs. a golden age of surveillance for smartphones. Two decades ago, a typical arrest rarely resulted in police access to a cell phone – mobile phones were fairly rare. A decade ago, a typical arrest might turn up a flip phone, with small amounts of meta-data about who had sent and received recent calls. Today, many users carry smart-phones with gigabytes of data, an almost unimaginable cornucopia of investigative detail in texts, emails, photos, and other apps. It is essentially impossible to describe this historical trajectory as the police “going dark.” Before, they had little or nothing. Today, they often have a cornucopia.

The law enforcement response is basically that they don’t always get the cornucopia, or sometimes they only get most of the cornucopia. Let’s begin with the basics, whether law enforcement gets any access to what is in the device. First, many users today don’t even put a passcode on their phone – anyone who picks it up can access the information. Second, if a suspect does use a passcode, many users have no encryption of data on the phone or there are technical ways to evade the encryption implementation. Third, especially in our world where confederates and co-conspirators are so easy to identify, the prosecutors only have to grant immunity to one co-conspirator in order to gain entry into the content shared with the other suspects. Fourth, the courts have yet to resolve how the Fifth Amendment privilege against self-incrimination applies to opening an encrypted smartphone, especially in a “going dark” scenario; the courts may decide that the government can jail suspects for contempt if they refuse to open the phone. Biometric identification, which is increasingly used for smartphones, may be especially available to law enforcement without triggering the privilege. These four reasons may help explain why it has been so difficult for the FBI and other law enforcement officials to provide examples of where encryption has frustrated an investigation, and the most recent statistics actually show a decline in wiretaps encountering encryption in 2014 compared to 2013, hardly evidence of “going dark.”¹⁶

Even where law enforcement does not gain access to the device (the cornucopia), law enforcement can often get most or all of the relevant data (most of the cornucopia). I have already discussed much of the data that remains available to

¹⁶ According to the federal 2014 Wiretap Report: “The number of state wiretaps in which encryption was encountered decreased from 41 in 2013 to 22 in 2014. In two of these wiretaps, officials were unable to decipher the plain text of the messages. Three federal wiretaps were reported as being encrypted in 2014, of which two could not be decrypted. Encryption was also reported for five federal wiretaps that were conducted during previous years, but reported to the AO for the first time in 2014. Officials were able to decipher the plain text of the communications in four of the five intercepts.” <http://www.uscourts.gov/statistics-reports/wiretap-report-2014>

law enforcement without recourse to the device itself – location of the phone; plaintext of emails; meta-data and often plaintext for text messages; and social networking data showing confederates. In addition, as discussed above, cloud storage often exists for numerous other data-sets, such as cloud storage of photos and videos, location on apps such as Waze and Uber, banking and other financial apps showing purchases, and so on. Indeed the increasing norm is full-device backups to the cloud. Even for an inaccessible device, therefore, the full content may be available from an accessible cloud provider.

E. Summary on Going Dark vs. Golden Age. To summarize, law enforcement does confront important challenges as encryption and other effective cybersecurity mechanisms become more pervasive. There will be particular instances where a lawful court order will not generate the full text of a communication. Nonetheless, numerous other technical trends are moving sharply in the direction of unprecedented law enforcement access. If the agencies had the choice between 1990-era capabilities or capabilities today, they would choose the capabilities today.

III. Government-Mandated Vulnerabilities Would Threaten U.S. Technological Leadership, While Not Preventing Effective Encryption by Adversaries

While national security interests are, justifiably, the focus of the current discussion around encryption, any mandated vulnerabilities would have far reaching effects in other sectors of U.S. interest as well. The first “Crypto Wars” in the 1990’s are illustrative of the futility of this approach: attempts to control the export of encryption negatively impacted U.S. business interests while other players entered to provide their own encryption solutions. Any mandated weakening of U.S. encryption today would create similar issues, as consumers both at home and abroad demand strong, independent encryption for a variety of reasons. Hamstringing U.S. companies from being able to meet this demand will only benefit foreign competitors who seek to fill the void while giving political cover for those countries who will demand similar access in order to further the suppression of targeted speech and oppression.

A. Technology companies, even before Snowden, had multiple reasons to use strong encryption to enhance cybersecurity and customer trust.

Although encryption issues have become the subject of greater public debate since the beginning of the Snowden revelations, there has been an ongoing trend to deploy effective encryption for consumer and business applications. The central importance of encryption to cybersecurity was a major theme in the Review Group report, as discussed above. Strong encryption is essentially the broadest-spectrum antibiotic against cyber-infections. In our era of pervasive cyber-attacks, encryption is crucial to preventing identity theft, reducing the harmful effects of data breaches, and providing myriad other protections against attacks.

The necessary and pervasive spread of encryption was the topic of my 2012 article why encryption drives the government to seek access to the cloud, cited above. That article gave a 2012 list of examples of widespread encryption:

- “Corporate and government users have widely adopted Virtual Private Networks (VPNs) for remote users. VPNs are strongly encrypted, thus protecting the organization’s emails and other communications.
- Electronic commerce, including credit card numbers, is overwhelmingly conducted today using SSL (Secure Sockets Layer).
- Facebook now supports SSL. If it enables SSL by default [which is true in 2015], then its social networking communications would not be readable at the ISP level.
- Research in Motion’s Blackberry products use strong encryption, and RIM itself does not have the keys for corporations who manage keys themselves.
- Major web locker services, such as Dropbox, use SSL by default.
- Skype, the leading VoIP provider, encrypts end-to-end. Many international calls are made using Skype. VoIP enables voice communications to be encrypted at scale.
- Many Internet games and other services use encryption, often with accompanying voice and chat channels.”¹⁷

This trend has continued since 2012, including for the device encryption of smartphones that the FBI has criticized.¹⁸ Although it might seem that the widespread use of encryption is a reason to mandate vulnerabilities in software to enable law enforcement access, my view is different. The growing and pervasive use of encryption is recognition of its centrality to defending against cyber-attacks – the ongoing debates about cybersecurity legislation in Congress show a consensus that customers need this protection, and companies need to supply it. In addition, CALEA II-style mandates run up against the pervasive use of encryption. Such

¹⁷ “From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud,” *International Data Privacy Law* (2012), doi: 10.1093/idpl/ips025.

¹⁸ Joe Miller, *Google and Apple to introduce default encryption*, BBC NEWS, Sep. 19, 2104 (available at <http://www.bbc.com/news/technology-29276955>), Clint Finley, *Encrypted Web Traffic More Than Doubles After NSA Revelations*, WIRED, May 16, 2014 (available at <http://www.wired.com/2014/05/sandvine-report/>), Peter Eckersley, *Launching in 2015: A Certificate Authority to Encrypt the Entire Web*, EFF, Nov. 18, 2014 (available at <https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web>), James Vincent, *Microsoft will encrypt Bing search traffic by default*, THE VERGE, Jun 16, 2015 (available at <https://www.theverge.com/2015/6/16/8788373/encrypted-search-microsoft-bing>), Kate Vinton, *Wikipedia Is Now Using HTTPS By Default To Prevent Snooping and Censorship*, FORBES, Jun. 12, 2015 (available at <http://www.forbes.com/sites/katevinton/2015/06/12/wikipedia-is-now-using-https-by-default-to-prevent-snooping-and-censorship/>), Alex Hern, *Facebook introduces PGP encryption for sensitive emails*, THE GUARDIAN, Jun. 1, 2015 (available at <http://www.theguardian.com/technology/2015/jun/01/facebook-introduces-pgp-encryption-for-sensitive-emails>), Micah Lee, *Microsoft Gives Details About Its Controversial Disk Encryption*, The Intercept, Jun. 4, 2015 (available at <https://firstlook.org/theintercept/2015/06/04/microsoft-disk-encryption/>).

mandates would be a regulatory nightmare, affecting so many applications and implementations as to be unmanageable and enormously costly.

B. Overwhelming technical problems and costs result from mandates to create vulnerabilities in encryption.

The technological hopes of law enforcement were expressed in House testimony this April by Amy Hess, Executive Assistant Director of the Science and Technology Branch of the FBI. She said:

“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 cyber crime 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 not lower the overall security.*” (emphasis supplied)¹⁹

The heart of the problem is this: the Review Group and the vast majority of technical experts do not think the FBI’s hopes are possible to achieve, for the sorts of access suggested in CALEA II proposals. Even if they assist law enforcement in some respects, the proposed lawful intercept and access solutions lower overall security.

Repeated blue-ribbon panels of technical experts have come to the same conclusion. In the 1990’s, Representative Bob Goodlatte summed up the lessons that Congress was learning:

“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.”²⁰

¹⁹ Amy Hess, *Statement Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology*, Apr. 29, 2015 (available at <https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices>).

²⁰ 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 Kenneth W. Dam and Herbert S. Lin, Editors, Committee to Study National Cryptography Policy, National Research Council, “Cryptography’s Role in Securing the Information

An influential group of encryption experts issued a 1997 report on “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption.”²¹ Among the key findings of this technical group: “The deployment of key-recovery-based encryption infrastructures to meet stated specifications will result in substantial sacrifices in security and greatly increased costs to end users.” The report made numerous, telling criticisms of key recovery approaches. From my participation in the policy debates of the era, there was no effective technical response by supporters of government key recovery approaches.

In May, 2013, just prior to the first Snowden revelations, the Center for Democracy and Technology gathered a different group of technical experts to write “CALEA II: Risks of Wiretap Modifications to Endpoints.”²² The conclusions about the harms of mandated vulnerabilities were clear:

“The U.S. government is proposing to expand wiretap design laws broadly to Internet services, including voice over Internet protocol (VoIP) services and other peer- to-peer tools that allow communications in real-time directly between individuals. This report explains how mandating wiretap capabilities in endpoints poses serious security risks. Requiring software vendors to build intercept functionality into their products is unwise and will be ineffective, with the result being serious consequences for the economic well-being and national security of the United States.”

An impressive new technical study by a group of experts was released on July 7, just before this hearing, entitled “Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications.”²³ It states:

“We have found that the damage that could be caused by law enforcement exceptional requirements would be even greater today than it would have been twenty years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today’s Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse “forward secrecy” design

Society,” *National Academies Press* (1996), available at <http://www.nap.edu/catalog/5131/cryptographys-role-in-securing-the-information-society>.

²¹ Hal Abelson, Ross N. Anderson, Steven Michael Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and others. <https://www.schneier.com/paper-key-escrow.html>.

²² <https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf>.

²³ “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communication.” Abelson, Harold; Anderson, Ross; Bellovin, Steven M.; Benaloh, Josh; Blaze, Matt; Diffie, Whitfield; Gilmore, John; Green, Matthew; Neumann, Peter G.; Landau, Susan; Rivest, Ronald L.; Schiller, Jeffrey I.; Schneier, Bruce; Specter, Michael; Weitzner, Daniel J.

practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally-connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws."

The new study highlights three general problems. First, providing mandated access "would force a U-turn from the best practices now being deployed to make the Internet more secure." For instance, best practices now incorporate "forward secrecy," where "decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications." If law enforcement requires key retention, then that directly undermines the protection against later attacks.

Second, building in exceptional access would substantially increase system complexity:

"Security researchers inside and outside government agree that complexity is the enemy of security — every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services... Features to permit law-enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious — making security testing difficult and less effective."

Third, exceptional access would create concentrated targets for bad actors to target:

"Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement's keys have guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement's stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple keyholders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the United States Government Office of Personnel Management show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data because OPM had insecure infrastructure. If service providers implement exceptional

access requirements incorrectly, the security of all of their users will be at risk.”

At a practical level, there are thousands of police departments spread across the United States. Providing online access to these police departments, while having iron-clad assurances that no hackers can get in, ignores the lessons of the recent OPM breach and the numerous other data breaches in the public and private sectors.

Let me add my personal observations on these studies about the technical obstacles to safe key recovery by law enforcement. I have engaged with a wide range of technical encryption experts for two decades, both inside and outside of government, often as the only person with legal training at a conference. I have an appointment in the College of Computing at Georgia Tech, and teach cybersecurity there, with a majority of the class in graduate studies in information security. Based on this engagement with technical experts, they say the same things in private as are written in the blue-ribbon reports. The passion that the most eminent technical experts show here is due to their conviction based on hard-fought experience, and not as a lobbying ploy.

Quite simply, the technical experts I trust believe that the FBI is asking for the impossible. CALEA II-style proposals hurt security.

C. U.S. Government support for encryption vulnerabilities increases cybersecurity problems in the “least trusted countries” and globally, and undermines U.S. human rights policies.

U.S. Government support for encryption vulnerabilities not only encounters the severe technical cybersecurity problems just discussed, but also increases the likelihood of cybersecurity threats originating from other countries. U.S. government support for such vulnerabilities harms both cybersecurity and human rights.

In 2012 I was the lead author of a 65-page law review article on “Encryption and Globalization,” a comprehensive examination of global effects of national encryption policies.²⁴ What we called the “least trusted country” problem is critical to understanding cybersecurity and encryption in our globalized setting. If one country sets limits on encryption, then cross-border communications that comply with that country’s laws will have that vulnerability. If one party to a communication uses compromised encryption as required in that country, then those globally who communicate with that country will have their communications compromised as well.

Key escrow provides a vivid example of the least trusted country problem.

²⁴ Peter Swire & Kenesa Ahmad, “Encryption and Globalization,” 13 *Colum. Sci. & Tech. L. Rev.* 416 (2012).

Consider whatever country in the world you trust the least. For India, that could be Pakistan, for Taiwan it could be China, for Israel it could be Iran. (I prefer not to pick one such country for the United States.) How secure would any of these countries be if their least trusted country had key escrow for their communications? We wrote: “Ultimately, laws that limit effective encryption create security holes. Communications that originate, end, travel through, or comply with the policies of those nations are systematically weakened —they are as secure as they would be in the hands of our least trusted country, whatever country that may be... Think about important communications in the hands of the country you trust least in the world. That is the Internet that would result from limits on strong encryption.”

In this globalized setting, the United States has a crucial leadership role to play concerning possible compromises in global communications security. I saw this personally when I met in India with senior officials in 2011, when India was considering a sweeping key escrow proposal. In these discussions, we explained the history of the crypto wars in the 1990's, and gave the technical and political reasons why the U.S. government had correctly decided to abandon a key escrow approach. After these discussions, and those with other American and global experts, the Indian government substantially cut back its legal proposal, and also has had far less than full implementation of the residual provisions. In short, the American example was useful in reducing the bad effects on global security, notably including for U.S. individuals and companies communicating abroad. If American policy becomes to mandate encryption vulnerabilities, either in law and practice, then our moral and policy authority to argue for strong cybersecurity is eroded.

The human rights implications of mandating vulnerabilities are also substantial and important. The Review Group Report discussed the importance of the U.S. Internet Freedom agenda, to bolster protections for journalist, religious minorities, and political dissenters around the world, especially in repressive regimes. In February, the U.S. government wrote a detailed statement about the importance of encryption to global free expression and human rights to David Kaye, Special Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression for the United Nations High Commissioner for Human Rights. Key statements included:

“As President Obama recently made clear, the United States firmly supports the development of robust adoption of strong encryption, which is a key tool to secure commerce and trade, safeguard private information, promote freedoms of expression and association, and strengthen cybersecurity. Encryption, as well as tools that assist with anonymity, are especially important in sensitive contexts where attribution could have negative political, social or personal consequences or when the privacy interests in the information are strong.... Consistent with this legal framework, as a matter of policy, the United States has long supported the development and use of

strong encryption and anonymity-enabling tools online.”²⁵

The importance of these anonymity-enabling tools has been underscored by financial support, especially from the U.S. State Department, for development of software and platforms to enable human rights activists and others abroad to communicate effectively notwithstanding local political regimes’ efforts to undermine such communications. The U.S. government support for its Internet Freedom agenda is broadly consistent with the June 17, 2015 Joint Civil Society Statement by 25 leading non-government organizations entitled “Promote Strong Encryption and Anonymity in the Digital Age.”²⁶

In conclusion on the “least trusted country” discussion, it is abundantly clear in our globalized world that decisions about U.S. law enforcement access to communications have important effects on how other countries decide to respond to similar issues in their own countries. The Information Technology Industry Council and Software & Information Industry Association made this point in a recent letter: “In addition to these security and trust concerns, the U.S. policy position on encryption will send a signal to the rest of the world. Should the U.S. government require companies to weaken encryption technology, such requirements will legitimize similar efforts by foreign governments. This would threaten the global marketplace as well as deprive individuals of certain liberties.”²⁷ The United States should be a strong example for cybersecurity and human rights, rather than an excuse used by repressive regimes to surveil U.S.-based businesses and individuals and clamp down on political dissent.

D. Mandated vulnerabilities are bad industrial policy – they threaten U.S. technological leadership without preventing bad actors from using strong encryption.

I next turn to why mandated vulnerabilities are bad as a matter of economic and industrial policy. Such vulnerabilities threaten U.S. technological leadership because they provide a ready excuse for foreign governments and purchasers to eschew American products and services. As we learned from the crypto battles of the 1990’s, they also are futile – they encourage non-U.S. suppliers to gain the technical edge in supplying effective encryption.

In April, 2015 House testimony, Kevin Bankston of the New America Foundation summarized key economic arguments:

“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

²⁵<http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/USA.pdf>

²⁶ <https://www.hrw.org/news/2015/06/17/promote-strong-encryption-and-anonymity-digital-age-0>

²⁷ <http://www.itic.org/dotAsset/58fbf8de-cd86-47a0-a114-43a55776d2e6.pdf>.

National Security Agency's programs, a loss of trust already predicted to cost our economy billions of dollars. 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."²⁸

The experience from the 1990's shows that foreign suppliers are eager to step into gaps left by U.S. restrictions on encryption. Under the export control regime then in existence, it was illegal to export strong encryption from the U.S. Other encryption suppliers, such as from Russia and Israel, became significant players precisely because U.S.-based companies could not supply effective software encryption from the U.S. In my experience, the futility of the encryption limits was an especially persuasive argument to members of Congress – why should we support an approach that undermined the U.S. tech sector and also didn't stop the spread of strong encryption? A related phenomenon, less well known, was the concern within the Pentagon about the rising competition from non-U.S. technology companies. For the Department of Defense, limits on U.S. encryption development meant that it faced the risk of relying on second-rate encryption for its own systems, while other countries could be developing state-of-the-art encryption that would benefit other militaries but not the United States.

Mandated vulnerabilities within the United States, to assist law enforcement, thus repeat the 1990's syndrome of harm to U.S. industry as well as futility. Much of the growth in encryption-related software and products could come from non-U.S. companies that serve the global market for secure communications and storage. Other growth would come from the already-flourishing free and open source sector. As Bankston wrote:

“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

²⁸ <http://oversight.house.gov/wp-content/uploads/2015/04/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston.pdf>.

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.”²⁹

Stanford cybersecurity research Jonathan Mayer sums up the futility of technology controls justified by “going dark” concerns:

“Cryptographic backdoors are, however, not a solution. Beyond the myriad other objections, they pose too much of a cost-benefit asymmetry. In order to make secure apps just *slightly* more difficult for criminals to obtain, and just *slightly* less worthwhile for developers, the government would have to go to *extraordinary* lengths. In an arms race between cryptographic backdoors and secure apps, the United States would inevitably lose.”³⁰

Conclusion

Much more could be added about why such a diverse coalition of cybersecurity experts, technology companies, privacy experts, human rights activists, and others are so passionately concerned about the “going dark” arguments made by law enforcement agencies.³¹ We can respect the heartfelt concerns of law enforcement officials facing new challenges while respectfully disagreeing with proposed policies. The policy debates in the 1990s ended in a clear verdict, accepted by Congress and the administration -- effective encryption is essential to our modern communications infrastructure, and mandated weaknesses in encryption are both futile and ultimately counter-productive.

Biography of Peter Swire

Peter Swire is the Huang Professor of Law and Ethics at the Georgia Tech Scheller College of Business. He has appointments by courtesy with the College of Computing and School of Public Policy. His courses include “Information Security Strategies and Policy” and “Privacy, Technology, Policy, and Law.”

In 2015, the International Association of Privacy Professionals, among its over 20,000 members, awarded him its Privacy Leadership Award. In 2013, he served as one of five members of President Obama’s Review Group on Intelligence and Communications Technology. Prior to that, he was co-chair of the global Do Not

²⁹ Bankston, at <http://oversight.house.gov/wp-content/uploads/2015/04/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston.pdf>, quoting 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>.

³⁰ Jonathan Mayer, “You Can’t Backdoor a Platform,” Apr. 28, 2015, <http://webpolicy.org/2015/04/28/you-cant-backdoor-a-platform>.

³¹ For one coalition letter, see https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf.

Track process for the World Wide Web Consortium.

Swire is Senior Counsel with Alston & Bird, LLP. He is Senior Fellow with the Future of Privacy Forum, a Policy Fellow with the Center for Democracy and Technology, and a Cybersecurity Fellow with the New America Foundation.

Under President Clinton, Swire was the Chief Counselor for Privacy, in the U.S. Office of Management and Budget, the first person to have U.S. government-wide responsibility for privacy policy. In that role, he chaired the White House Working Group on Encryption, and participated in the 1999 White House announcement enabling export of strong encryption. As Chief Counselor, his activities included being White House coordinator for the HIPAA medical privacy rule, chairing a White House task force on how to update wiretap laws for the Internet age, and helping negotiate the U.S.-E.U. Safe Harbor agreement for trans-border data flows. Under President Obama, he served as Special Assistant to the President for Economic Policy.

Swire's writings on encryption include: (1) "The Uses and Limits of Financial Cryptography: A Law Professor's Perspective," chapter in the *proceedings of Financial Cryptography '97* (Springer-Verlag, 1997); (2) "'Going Dark' vs. 'A Golden Age for Surveillance,'" *Center for Democracy and Technology*, Nov. 28, 2011 (with Kenesa Ahmad); (3) "Encryption and Globalization," 13 *Colum. Sci. & Tech. L. Rev.* 416 (2012) (with Kenesa Ahmad); (4) "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," *International Data Privacy Law* (2012), doi: 10.1093/idpl/ips025; (5) "Going Dark vs. Going Secure – New CDT Experts Report on CALEA II," *IAPP Privacy Perspectives*, May 16, 2013; (6) "The FBI Doesn't Need More Access: We're Already in the Golden Age of Surveillance," *Just Security*, Nov. 17, 2014.

Swire graduated from Princeton University, summa cum laude, and the Yale Law School, where he was an editor of the Yale Law Journal.

HEARING BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

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

JULY 8, 2015

QUESTIONS FOR THE RECORD
FROM CHAIRMAN GRASSLEY TO
JAMES B. COMEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION:

1. The 2014 Wiretap Report and the “Data-in-Motion” Problem

The Administrative Office of the United States Courts releases an annual “Wiretap Report,” concerning intercepted communications pursuant to Title III of the Omnibus Crime Control and Safe Streets Act. The most recent Wiretap Report for 2014 showed that law enforcement confronted encryption in a very small fraction of wiretap applications and was unable to decipher encrypted communications in only a few of those cases. Some commentators, including Professor Swire at the hearing, have asserted that this report contradicts law enforcement’s claim that it is “Going Dark” and instead proves that encryption is not harming its ability to investigate crime by intercepting “data-in-motion.” Regardless, there is no doubt that Congress would benefit from concrete statistical information about the scope of the “Going Dark” problem and how it is affecting law enforcement.

- a. Does the Wiretap Report provide helpful data for evaluating the “Going Dark” problem faced by law enforcement, at least in the “data-in-motion” context? Or, as Deputy Attorney General Yates suggested in her testimony, does the Wiretap Report only reflect the number of applications that are sought and impacted by encryption, not the number of applications that are never sought because of encryption?

Response: Please see the response to Chairman Grassley’s question 2 to Deputy Attorney General Yates, *infra*.

- b. If the Wiretap Report is not a good benchmark for the “data-in-motion” problem, can the Federal Bureau of Investigation work to develop a better mechanism to keep track of the number of investigations that are negatively

impacted by strong encryption and share that information with Congress so that Congress can better evaluate the issue?

Response: Yes. The FBI is currently working on improving enterprise-wide quantitative data collection to better explain the “data-in-motion” problem. The objectives are to improve and streamline data collection metrics and ensure that the FBI has access to timely and accurate quantitative data to capture and convey the problem.

2. The Impact of Encryption and the “Data-at-Rest” Problem

Regarding the “data-at-rest” problem, District Attorney Vance stated in his written testimony to the Committee that “when smartphone encryption is fully deployed by Apple and Google, 71% of all mobile devices examined – at least by my Office’s lab -- may be outside the reach of a search warrant.”

a. Does the Federal Bureau of Investigation have similar information regarding the potential impact of encryption on the “data-at-rest” problem?

Response: Yes. The FBI encounters many of the same brands and models of electronic devices as the New York District Attorney’s crime lab, and we utilize many of the same commercial forensic tools. The two companies that you reference share a large percentage of the smart phone operating system marketplace in the United States. As with the New York District Attorney’s Office, the devices we encounter during investigations are generally representative of what is popular in the commercial marketplace. Some companies have advertised their intention to fully implement encryption methodologies that they are unable to bypass, even with lawful court order. As a consequence, the data on the vast majority of the devices seized in the United States may no longer be accessible to law enforcement even with a court order or search warrant.

b. For instance, does the FBI have any similar statistical information on how often it has obtained a judicially authorized search warrant for the digital contents of a device but was nonetheless unable to execute the warrant due to encryption? Similarly, does the FBI have any similar statistical information on how often it has obtained a judicially authorized search warrant to obtain the contents of an email account but was unable to execute the warrant due to encryption?

Response: No. As with the “data-in-motion” problem, the FBI is working on improving enterprise-wide quantitative data collection to better explain the “data-at rest” problem. Before the recent introduction of encrypted-by-default electronic devices into the marketplace, the challenges posed by encrypted “data at rest” were encountered intermittently in investigations. Prior to 2014, the FBI’s Going Dark Initiative focused primarily on the data-in-motion

challenges. The technology industry's shift toward fully encrypted-by-default devices has been extremely rapid and the FBI has been working to shift our business practices to address these new challenges. Our ability to rely on commercial forensic tools has diminished, we can no longer reliably obtain critical information from certain manufacturers, and we have found ourselves relying on self-initiated efforts to solve these extremely complex challenges.

As noted above, the FBI is currently working on improving enterprise-wide quantitative data collection to better understand and explain the "data at rest" problem. This process includes adopting new business processes to help track when devices are encountered that cannot be decrypted, and when we believe leads have been lost or investigations impeded because of our inability to obtain data. As we adjust business practices to capture this information, one thing we know for certain is that, even with a court order or warrant, we increasingly cannot obtain the communications, transactions, documents, records, and contact lists of criminals that are contained within devices. We agree that the FBI must institute better methods to measure these challenges when they occur.

- c. If the FBI does not have such information, can it develop a mechanism to keep track of the number of investigations that are negatively impacted by smartphone encryption and share that information with Congress so that Congress can better evaluate the issue?**

Response: Yes. The FBI is working to identify new mechanisms to better capture and convey the challenges encountered with lawful access to both data-in-motion and data-at-rest.

3. CALEA

In prior testimony before Congress, the Federal Bureau of Investigation suggested that the "data-in-motion" problem was associated with limitations on the enforceability and scope of the Communications Assistance for Law Enforcement Act (CALEA).

- a. How much of the "data-in-motion" side of the problem is attributable to problems with the enforceability of CALEA – i.e., providers or services that are covered by CALEA but that do not or are unable to comply with CALEA? Alternatively, how much is attributable to problems with the scope of CALEA – i.e., providers or services that are not covered by CALEA, either by statute or by FCC regulation?**

Response: There are several constraints inherent to CALEA that limit certain provisions of the statute. Many of these constraints have become more pronounced over time as new communications services have been introduced. At the time of enactment, the portion of the

communications infrastructure covered by CALEA was significant — i.e., landline and cellular telecommunications carriers. In 2005, the scope was expanded through a decision from the Federal Communications Commission (FCC) to include interconnected Voice over Internet Protocol (VoIP) service providers and providers of broadband Internet access services. However, services and networks evolve very quickly and systems are frequently updated. Indeed, there have been instances where companies upgraded equipment or altered their architectures and they no longer have the capability to isolate the communications of the subject of a court order.

In some cases, law enforcement agencies may be able to install or provide equipment to facilitate the implementation of a court order. However the installation of law enforcement equipment tends to yield incomplete results, is resource intensive, and is not available to all of law enforcement — the very situation CALEA was intended to remedy.

As traditional telecommunications services become less popular, users have migrated to Internet-based communications services that are presently outside the scope of CALEA, and therefore are not subject to the CALEA requirement to have a lawful intercept capability. For example, pursuant to technical standards adopted under CALEA, telecommunications carriers maintain an interception capability for traditional text messages (“Short Message Service,” or “SMS”). There are no analogous CALEA-based standards or requirements for Internet-based instant messages. This is true even though both types of messages are carried over connections made available by telecommunications carriers and seamlessly integrated within some popular Internet-based instant messaging applications.

b. How many providers or services have refused to comply with court orders on the basis that they are not subject to CALEA? Please identify each instance and each provider or service that has refused to comply with a court order in this area.

Response: Today’s Internet-based service providers are generally not required to develop and maintain technical capabilities for intercepting communications. In many instances, providers that are not subject to the requirements imposed by CALEA are often unprepared to assist law enforcement when served with a court order. These providers may leverage internal systems not designed for interception purposes in an attempt to comply with lawful interception orders. As a result of this ad-hoc approach, court ordered compliance can be affected in a number of different ways, including: providing incomplete or unintelligible information that requires additional troubleshooting and support from both the provider and law enforcement; and delaying the delivery of the information as the provider manually retrieves data from its systems with a frequency that can vary between hours, days, and weeks. Ultimately, it has been the FBI’s experience that none of the providers offering application-based communication services outside of CALEA are able to provide all of the information law enforcement is authorized by court order to collect.

For more information, please also see the response to Senator Whitehouse's question 1 to Director Comey, *infra*.

4. Spyware

In June, I wrote to you to ask for details about the FBI's use of spyware. According to press reports, some types of spyware programs can be remotely deployed to a targeted computer to surreptitiously activate the computer's camera and microphone; collect passwords; search the computer's hard drive, random-access memory, and other storage media; generate latitude and longitude coordinates for the computer's location; and intercept phone calls, texts, and social media messages. Some have argued that spyware is a potential solution to the Going Dark problem because it allows law enforcement to forgo trying to break strong encryption and instead lets law enforcement see the same decrypted version of the communication that the sender or receiver sees on his or her device. In fact, in 2013 the Wall Street Journal ran an article entitled: "FBI Taps Hacker Tactics to Spy on Suspects: Law-Enforcement Officials Expand Use of Tools Such as Spyware as People Under Investigation 'Go Dark,' Evading Wiretaps."

In your testimony, you stated: "what I'm confirming here is we cannot break strong encryption. We have not found that tool. I don't think it exists. But we look for other ways around the margins if a judge gives us permission to be able to get into a room or get into a device."

- a. Does the FBI possess or deploy spyware that allows it to see decrypted versions of messages on a targeted device that were transmitted using strong encryption?
- b. If so, has the FBI evaluated to what extent the use of such spyware could mitigate or resolve the problems of "Going Dark" without requiring companies to provide back doors or otherwise limit strong encryption? If so, what were the conclusions of that evaluation?
- c. If current spyware technology does not have the capability to see decrypted versions of communications sent with strong encryption, has the FBI considered increasing its research and development of spyware tools in pursuit of this capability?

Response: The responses to these inquiries are classified and are, therefore, provided separately. In addition to the classified annex accompanying this document, we note that the Department of Justice has previously responded to the Committee's letters on this topic. Specifically, on July 14, 2015, the Department of Justice responded to the Committee's letter to the Deputy Attorney

General, dated April 27, 2015. The Committee submitted a follow-up letter to the FBI and the Drug Enforcement Administration (DEA) on July 15, 2015. On January 14, 2016, the FBI provided an unclassified response with a classified annex to the Committee in response to its letters of June 12, July 15, and December 16, 2015. Further, DEA responded to the July 15, 2015, letter on January 14, 2016.

**QUESTIONS FROM CHAIRMAN GRASSLEY TO
SALLY QUILLIAN YATES, DEPUTY ATTORNEY GENERAL**

1. Legislative Proposals Timeline

At the hearing, I asked you whether the Obama Administration planned to come forward with a proposed legislative solution to the “Going Dark” problem, as well as the fate of its reported 2012 proposal. You told me that the Department of Justice is not seeking a legislative fix at this time, but wanted to work with the technology companies to find solutions that will work for each individual company. However, you acknowledged that the Department was “not ruling out a legislative solution” should one prove necessary. I also asked whether there was a process in place or a target timeline within the Administration to find solutions, but I didn’t get an answer to that question.

- a. Does the Department of Justice have any formal process or any timeline in place to work with technology companies to find solutions to the “Going Dark” problem? If so, please provide as much detail about that process or timeline as possible. If not, why does the Department not have such a process or timeline?
- b. Given the testimony at the hearing that “Going Dark” is a significant problem and is only getting worse, is there a date certain by which, if a solution to the problem has not been reached through dialogue with the technology companies, the Department of Justice will come forward with a legislative proposal?

Response: The Department of Justice continues to work with companies and industry groups to address these issues, and those efforts have intensified in the last few months. In fact, the United States Government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors’ use of their encrypted products and services. The Administration is not seeking legislation at this time. The United States Government is seeking voluntary cooperation from U.S. companies on a case-by-case basis, in order to address incidents or cases of concern. We will continue to pursue this cooperation, but note that solutions to particular issues may vary based on the technology

involved, the responsiveness of the company, and other factors. For this reason, we do not have a deadline in mind for any particular action.

2. The “Data-in-Motion” Problem and the Wiretap Report

The Administrative Office of the United States Courts releases an annual “Wiretap Report,” concerning intercepted communications pursuant to Title III of the Omnibus Crime Control and Safe Streets Act. The most recent Wiretap Report for 2014 showed that law enforcement confronted encryption in a very small fraction of wiretap applications and was unable to decipher encrypted communications in only a few of those cases. Some commentators, including Professor Swire at the hearing, have asserted that this report contradicts law enforcement’s claim that it is “Going Dark” and instead proves that encryption is not harming its ability to investigate crime by intercepting “data-in-motion.” Regardless, there is no doubt that Congress would benefit from concrete statistical information about the scope of the “Going Dark” problem and how it is affecting law enforcement.

- a. Does the Wiretap Report provide helpful data for evaluating the “Going Dark” problem faced by law enforcement, at least in the “data-in-motion” context? Or, as you suggested in your testimony, does the Wiretap Report only reflect the number of applications that are sought and impacted by encryption, not the number of applications that are never sought because of encryption?
- b. If the Wiretap Report is not a good benchmark for the “data-in-motion” problem, can the Department of Justice work to develop a better mechanism to keep track of the number of investigations that are negatively impacted by strong encryption and share that information with Congress so that Congress can better evaluate the issue?

Response: Encryption presents a significant and growing challenge for law enforcement in the context of “data in motion.” Billions of communications occur each day over services that, because of encryption, lack a meaningful interception capability. Unfortunately, the Wiretap Report cannot present a complete or accurate picture of this challenge. Pursuant to 18 U.S.C. § 2519, the Department of Justice, State prosecutors, and judges provide information to the Administrative Office of the United States Courts for inclusion in the Wiretap Report. The Wiretap Report only reflects the number of criminal applications that are sought, and not the many instances in which an investigator is dissuaded from pursuing a court order by the knowledge that the information obtained will be encrypted and unreadable. That is, the Wiretap Report does not include statistics on cases in which the investigator does not pursue an interception order because the provider has asserted that an intercept solution does not exist. Obtaining a wiretap order in criminal investigations is extremely resource-intensive as it requires

a huge investment in agent and attorney time, and the review process is extensive. It is not prudent for agents and prosecutors to devote resources to this task if they know in advance that the targeted communications cannot be intercepted. The Wiretap Report, which applies solely to approved wiretaps, records only those extremely rare instances where agents and prosecutors obtain a wiretap order and are surprised when encryption prevents the court-ordered interception. It is also important to note that the Wiretap Report does not include data for wiretaps authorized as part of national security investigations.

Because it does not capture the effect of the Going Dark problem on the choice of investigative tools, the Report is of limited utility in quantifying the challenges posed by encryption. Accordingly, the statistics in the Wiretap Report are not a reliable measure of the scope of the Going Dark problem. The Department of Justice is exploring ways to more accurately measure the impact of encryption in the context of “data in motion,” and we look forward to sharing the results with the Committee.

3. The “Data-at-Rest” Problem and the Impact of Encryption

Regarding the “data-at-rest” problem, District Attorney Vance stated in his written testimony to the Committee that “when smartphone encryption is fully deployed by Apple and Google, 71% of all mobile devices examined – at least by my Office’s lab – may be outside the reach of a search warrant.”

- a. Does the Department of Justice have similar information regarding the potential impact of encryption on the “data-at-rest” problem?

Response: Please see the response to Chairman Grassley’s question 2(a) to FBI Director Comey, *supra*.

- b. For instance, does the Department of Justice have any similar statistical information on how often it has obtained a judicially authorized search warrant for the digital contents of a device but was nonetheless unable to execute the warrant due to encryption? Similarly, does the Department of Justice have any similar statistical information on how often it has obtained a judicially authorized search warrant to obtain the contents of an email account but was unable to execute the warrant due to encryption?

Response: Please see the response to Chairman Grassley’s question 2(b) to FBI Director Comey, *supra*.

- c. If the Department of Justice does not have such information, can it develop a mechanism to keep track of the number of investigations that are negatively impacted by smartphone encryption and share that information with Congress so that Congress can better evaluate the issue?

Response: Please see the response to Chairman Grassley's question 2(c) to FBI Director Comey, *supra*.

4. CALEA

In prior testimony before Congress, the Federal Bureau of Investigation suggested that the "data-in-motion" problem was associated with limitations on the enforceability and scope of the Communications Assistance for Law Enforcement Act (CALEA).

- a. How much of the "data-in-motion" side of the problem is attributable to problems with the enforceability of CALEA – i.e., providers or services that are covered by CALEA but that do not or are unable to comply with CALEA? Alternatively, how much is attributable to problems with the scope of CALEA – i.e., providers or services that are not covered by CALEA, either by statute or by FCC regulation?

Response: Please see the response to Chairman Grassley's question 3(a) to FBI Director Comey, *supra*.

- b. How many providers or services have refused to comply with court orders on the basis that they are not subject to CALEA? Please identify each instance and each provider or service that has refused to comply with a court order in this area.

Response: Please see the response to Chairman Grassley's question 3(a) to FBI Director Comey, *supra*.

5. Department of Justice's Discussions with Technology and Communication Companies

You testified that the Department of Justice is working with technology and communications companies to try to find solutions to the "Going Dark" problem.

- a. Please provide as much information as possible about the Department of Justice's engagement with these companies, including the specific companies

that are part of the discussions, when the discussions on this topic began, and whether the discussions with each company remain ongoing.

- b. Have any companies refused to productively engage with the Department of Justice on this issue? If so, please identify them.
- c. Will you commit to providing the Committee with quarterly updates about the status of the Department's engagement with these companies to find solutions to this problem?

Response: The Department of Justice regularly works with companies in connection with the need for lawful access to customer data to protect public safety and national security. This often occurs in connection with specific court orders or search warrants, but also involves broader engagement about a company's technical capabilities concerning compliance with legal process. We use this broader engagement, which also extends to industry groups and organizations, to exchange information regarding Going Dark challenges and to hear the companies' perspectives. Most are willing to engage on the Going Dark problem, though some prefer that this engagement take place in one-on-one discussions regarding their capabilities. These discussions occur frequently with a variety of companies, groups, and organizations. We would welcome the opportunity to offer the Committee regular updates about our continuing efforts to attain individualized solutions.

6. Contempt as a Solution

Some critics of the "Going Dark" problem argue that law enforcement has other options available to them, such as the use of contempt to force a defendant to provide law enforcement with access to his or her encrypted information. Is this a viable option in most investigations? Why or why not?

Response: This is not a viable option in most investigations. Courts thus far have held that the compelled production of a password violates the defendant's Fifth Amendment privilege against self-incrimination in most circumstances. Moreover, even if courts were to hold otherwise on the Fifth Amendment question, many offenders would choose to accept a punishment for contempt rather than risk a lengthy sentence for the underlying crime. In addition, in some cases, especially those involving real-time interception pursuant to a court order, it is not feasible to compel an individual because doing so would alert them to the surveillance. And, finally, regardless of the legal landscape, compelling disclosure of passwords is not a useful solution in many national security surveillance contexts, such as those involving spies and terrorists.

QUESTION FROM SENATOR WHITEHOUSE TO
JAMES B. COMEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION:

1. During your testimony, you mentioned that there are companies that have the technical capability to comply with requests issued by law enforcement but have declined to do so. Please provide all available information about these declinations, including the name and address of the company and the type of request issued by law enforcement.

Response: In the current legal and technological environment, there are several circumstances in which companies may decline to comply with requests issued by law enforcement authorities. In some instances, a company may have the technical capability to comply but it declines to do so based on a legal argument that applies in that narrow case (these arguments may relate to jurisdiction, the form of the request, or other factors). As a separate matter, some companies may decide not to fully develop the capability to comply because there is no legal mandate to do so. Companies may also decide not to comply because they assert that doing so would cause reputational harm. *See, e.g.,* Response Brief of Apple, Inc., *In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued By this Court*, No. 15 MISC 1902 (JO) (E.D.N.Y. Oct. 19, 2015). Although the FBI does not retain information regarding these various circumstances, we would be pleased to provide anecdotal information to the Committee regarding our efforts and results in an appropriate setting.

QUESTION FROM SENATOR WHITEHOUSE TO
SALLY QUILLIAN YATES, DEPUTY ATTORNEY GENERAL:

2. Has the Department of Justice explored whether there is any potential civil liability for companies that choose to encrypt customer data in a manner that they cannot decrypt, even when presented with a valid search warrant? If the Department has not explored this issue, would it be willing to do so?

Response: The Department of Justice has not undertaken a detailed analysis of that issue, but we would be willing to work with you and your staff to understand the exact scope and contours of any such analysis.

Our efforts have focused on preventing the type of harm that might give rise to civil liability by ensuring that companies retain the ability to comply with lawful court orders. Indeed, many companies maintain that ability while simultaneously guarding individual security and privacy through the use of strong encryption. We look forward to working with the industry to find other ways to implement strong data protection while preserving the ability to protect public safety and national security.

Senate Committee on the Judiciary
Questions for the Record from Senator Grassley
To: Dr. Herbert Lin
Senior Research Scholar, Center for International Security and Cooperation
The Hoover Institution
Stanford University

1. **Massachusetts Institute of Technology Report: “Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications”**

As you know, days before our Committee hearing, the above report was issued by a number of security technologists. The report was highly skeptical of the government’s ability to mandate special access to encrypted communications without doing great harm to internet security. If you have had a chance to review it thoroughly, please comment on what effect, if any, it has on the views expressed in your written and oral testimony before the Committee.

Answer:

I have indeed read the report in detail, and I think the report has great value to the debate. In my testimony, I called attention to two aspects of the report that are worth repeating for the record here.

First was the report’s call for more specifics. Quoting from the report – law enforcement needs to “develop genuine, detailed specifications for what they expect exceptional access mechanisms to do.” That is absolutely correct – only with real specifics is a serious technical debate possible, and only with such a debate is it possible to assess the nature and extent of the actual security impact of any such mechanism. The report does describe some general risks of exceptional access, and these must be taken seriously, but they do not speak directly to any specific mechanism because no specific mechanism has been introduced publicly for consideration.

The second important aspect of the report was its list of key questions that would have to be addressed satisfactorily before government goes down the path of mandated exceptional access. In the strongest of terms, I endorse these questions as being critical—and I believe the Congress should require **written** answers to these questions from whatever Administration, if any, that decides in favor of mandated exceptional access.

Senate Committee on the Judiciary
Questions for the Record from Senator Grassley
To: Peter Swire
Huang Professor of Law and Ethics
Scheller College of Business
Georgia Institute of Technology

1. Global Competitiveness

In my opening statement, one of the concerns I expressed was that, in considering solutions to the “Going Dark” problem, we carefully consider the impact on the global competitiveness of American technology companies. You testified that if U.S. companies were required to give U.S. law enforcement access to encrypted communications and devices, U.S. companies find themselves at a disadvantage in the global marketplace. Yet it appears that countries like the United Kingdom, France and China are considering laws that would move in this direction.

- a. Do you agree that these foreign governments may be moving in this direction? If so, how would the global competitiveness of U.S. companies be damaged if foreign governments mandate the same sort of access?

Swire: I agree that other countries have been considering laws concerning mandated access. My view is that the position of the United States government is highly relevant to the likelihood of other countries adopting such laws, especially for close allies such as the United Kingdom and France. If the United States were to mandate access legally, which I hope it will not, my view is that the U.S. decision would substantially increase the likelihood of such laws being enacted by our allies. By contrast, if the United States maintains the status quo of no such mandates, then that fact becomes an important and relevant precedent against enactment of such measures by our allies.

I believe the U.S. position would also have a large impact on other countries around the world, especially for authoritarian or dictatorial regimes that would like to use mandated access to clamp down on political dissent, religious activity, and other activities. If the U.S. resists mandates, then the U.S. based technology companies have a much greater ability to resist demands for mandated access in such countries. Being able to resist such demands will protect devices and sensitive data of Americans and American businesses in those countries. By contrast, if the U.S. requires access, then it will be much more difficult for U.S. based technology companies to push back against requests from China or other foreign governments.

My initial point, therefore, is that the U.S. actions in this area have a very important impact on whether other countries adopt mandated access. As I stated during the hearing, I also believe that mandates in the U.S. would harm U.S. based technology companies because of the suspicion around the world that their products and services are not secure and information is shared with U.S. government agencies.

In terms of mandates in another country, such as a U.S. ally, there would be multiple effects and the overall outcome depends on the circumstances. For instance, if a small market country mandates access, then that might aid local companies that comply with the local law while U.S. companies may decide not to take the reputational risk of doing business in that jurisdiction. In that event, U.S. companies might lose access to a small market but face less competition from companies based in there in other markets. If the country is seen globally as having a weak human rights record, mandated access may push the U.S. companies, consistent with the Global Network Initiative principles, not to continue doing business there, thus losing market access. Such company decisions to eschew a market, however, may send a strong signal globally about the importance of customer security to the U.S. based companies, with offsetting gains in other markets.

In addition, there is a crucial dynamic aspect to such mandates. The small country, or country with weak human rights, might find the consequences negative if they lose access to cutting edge technology from U.S. based companies. They thus might reconsider their decision to mandate access, in order to bring U.S. based companies back into the jurisdiction. In such an event, a clear U.S. policy of not requiring access is crucial – the good long-term outcome of U.S. company participation and no mandates occurs only if the U.S. retains its policy where no mandates are imposed.



Senate Committee on the Judiciary
Responses to Questions for the Record from Senator Grassley
Washington, D.C.

Cyrus Vance, Jr., District Attorney, New York County, New York

Question 1: Correspondence with Apple and Google

In your written testimony and during the hearing, you spoke about your interactions with Apple and Google, and follow-up letters that you sent to these companies containing a series of detailed questions about the “Going Dark” issue.

- a. Please describe in further detail your interactions with these companies.
- b. Have you received a response from either company? If so, please describe in detail the response. If not, have you contacted them about the timing of any response?
- c. If and when you receive a response, would you please forward a copy to the Committee?

Response to Question 1(a).

Given my deep concerns on the harm to local law enforcement caused by Apple’s and Google’s new policies that would render the information on smartphones effectively beyond the reach of search warrants, my Office contacted Apple and Google to set up separate meetings with each company. On March 19, 2015, I, along with two members of my Office, two representatives from the United States Secret Service, and two representatives from the

Alabama Office of Prosecution Services participated in separate meetings with Apple and Google at their headquarters in California.

The representatives from Apple who participated in the meeting included: i) Jane Horvath, Senior Director of Global Privacy; ii) Pat Burke, Privacy Counsel for Enforcement; iii) Cathy Foster, Corporate Government Affairs; and iv) Mike Foulkes, Director, State and Local Government Affairs. I shared my concerns about the impact of Apple's decision on my Office and other state and local law enforcement agencies, explaining that state and local law enforcement handles ninety percent of the criminal cases in the United States and that a huge percentage of them involve evidence derived from smartphones. I explained that the availability of information on the cloud is not an adequate substitute for information on smartphones for pursuing criminal investigations, exoneration efforts, or prosecutions.

Apple explained that its decisions regarding smartphone encryption were based principally on security and market considerations, with the latter relating in large part to growth in foreign markets. Apple offered that efforts by Congress or a state legislature that would cause United States-based technology companies to limit encryption in any way might cause those companies to re-locate outside of the United States.

Our second meeting was held with Google. The representatives from Google present at the meeting included: i) Kent Walker, Senior Vice President and General Counsel; ii) Richard Salgado, Legal Director, Law Enforcement and Information Security; iii) Nicole Jones, Sr. Law Enforcement and Security Counsel; iv) Betsy Masiello; and v) Eric Grosse. As we had done with Apple, we shared with Google our concerns about the impact on state and local law enforcement of policies that would render the information on smartphones

effectively beyond the reach of search warrants. As had Apple, Google raised concerns about how limits on encryption would be exploited by foreign governments, and noted that information on smartphones had been used by repressive governments to oppress human rights activists. Google also referred to harm to its “brand” allegedly caused by publicity surrounding activities of the National Security Agency.

On March 31, 2015, and April 1, 2015, I sent letters to Apple and Google, respectively, setting forth questions that arose from our meetings with them. I have attached a copy of both my letters. (Copies of the letters were also attached as exhibits to my written testimony before your Committee.) I had hoped that the letters would foster a dialogue, but neither company has responded. I remain hopeful that a dialogue and a solution are possible.

Response to Question 1(b).

As noted above, to date I have not received a response from either Apple or Google.

Response to Question 1(c).

I will promptly forward to the Committee a copy of any response to my letters should I receive one.

Question 2: Exonerations of the Innocent

In your testimony, you spoke about how the “Going Dark” problem seriously affects your ability to obtain evidence to prosecute criminals. Can you also describe how the “Going Dark” problem impacts law enforcement’s ability to exclude individuals suspected of criminal wrongdoing or otherwise exonerate innocent people? Do you have any real-world examples of this?

Response to Question 2.

As you are aware, any evidence that helps us to prosecute criminals also helps us to exonerate the innocent, including the wrongly suspected or accused. A case from my office that illustrates the point arose when the police discovered a person dead in his apartment with a gunshot wound to the head.

My office obtained a search warrant and an “unlock order” from a court for certain phones found at the scene of the crime. We sent the phones to Apple, which unlocked them. The phone data helped to establish that what we had initially thought to be the timeline of the events was wrong, and that a person whom we had initially suspected had not, in fact, been involved. A contact in one of the unlocked iPhones was eventually traced to another individual, who later confessed and pled guilty to the killing. He is currently serving a sentence of 17 years and 6 months imprisonment. *People v. Rosario*, Indictment 01859/2010, New York State Sup

LIBERTY AND SECURITY IN A CHANGING WORLD

12 December 2013

**Report and Recommendations of
The President's Review Group on Intelligence
and Communications Technologies**

Table of Contents

Preface

Executive Summary

Recommendations

Chapter I: Principles

Chapter II: Lessons of History

- A. The Continuing Challenge
- B. The Legal Framework as of September 11, 2001
- C. September 11 and its Aftermath
- D. The Intelligence Community

Chapter III: Reforming Foreign Intelligence Surveillance Directed at United States Persons

- A. Introduction
- B. Section 215: Background
- C. Section 215 and “Ordinary” Business Records

- D. National Security Letters
- E. Section 215 and the Bulk Collection of Telephony Meta-data
 - 1. The Program
 - 2. The Mass Collection of Personal Information
 - 3. Is Meta-data Different?
- F. Secrecy and Transparency

Chapter IV: Reforming Foreign Intelligence Surveillance Directed at Non-United States Persons

- A. Introduction
- B. Foreign Intelligence Surveillance and Section 702
- C. Privacy Protections for United States Persons Whose Communications are Intercepted Under Section 702
- D. Privacy Protections for Non-United States Persons

Chapter V: Determining What Intelligence Should Be Collected and How

- A. Priorities and Appropriateness
- B. Monitoring Sensitive Collection
- C. Leadership Intentions

- D. Cooperation with Our Allies

Chapter VI: Organizational Reform in Light of Changing Communications Technology

- A. Introduction
- B. The National Security Agency
 - 1. “Dual-Use” Technologies: The Convergence of Civilian Communications and Intelligence Collection
 - 2. Specific Organizational Reforms
- C. Reforming Organizations Dedicated to the Protection of Privacy and Civil Liberties
- D. Reforming the FISA Court

Chapter VII: Global Communications Technology: Promoting Prosperity, Security, and Openness in a Networked World

- A. Introduction
- B. Background: Trade, Internet Freedom, and Other Goals
 - 1. International Trade and Economic Growth
 - 2. Internet Freedom

- 3. Internet Governance and Localization Requirements
- C. Technical Measures to Increase Security and User Confidence
- D. Institutional Measures for Cyberspace
- E. Addressing Future Technological Challenges

Chapter VIII. Protecting What We Do Collect

- A. Personnel Vetting and Security Clearances
 - 1. How the System Works Now
 - 2. How the System Might be Improved
 - 3. Information Sharing
- B. Network Security
 - 1. Executive Order 13578
 - 2. Physical and Logical Separation
- C. Cost-Benefit Analysis and Risk Management

Conclusion

Appendix A: The Legal Standards for Government Access to Communications

Appendix B: Overview of NSA Privacy Protections Under FAA 702

Overview of NSA Privacy Protections Under EO 12333

Appendix C: US Intelligence: Multiple Layers of Rules and Oversight

Appendix D: Avenues for Whistle-blowers in the Intelligence
Community

Appendix E: US Government Role in Current Encryption Standards

Appendix F: Review Group Briefings and Meetings

Appendix G: Glossary

Chapter VII

Global Communications Technology: Promoting Prosperity, Security, and Openness in a Networked World

A. Introduction

An important goal of US policy is to promote prosperity, security, and openness in the predominant method of modern communication, the Internet. This chapter examines how to achieve that goal, consistent with other goals of US policy.

In 2011, the Obama Administration released a major report: “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.” In the letter introducing the report, President Obama wrote: “This strategy outlines not only a vision for the future of cyberspace, but an agenda for realizing it. It provides the context for our partners at home and abroad to understand our priorities, and how we can come together to preserve the character of cyberspace and reduce the threats we face.” The Strategy defined the overall goal: “The United States will work internationally to promote an **open, interoperable, secure, and reliable** information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation” (emphasis added).

We believe that this is an exceedingly important goal, and that it bears directly on efforts to engage in sensible risk management. In this chapter, we offer a series of recommendations designed to promote that

goal, and in the process to protect the central values associated with a free Internet.

B. Background: Trade, Internet Freedom, and Other Goals

The United States has a strong interest in promoting an open, interoperable, secure, and reliable information and communication structure. We focus our discussion on international trade, economic growth, and Internet freedom.

Throughout this report, we have stressed the need for a risk-management approach, balancing the imperatives for intelligence collection with the potential downsides. In the areas discussed in this chapter, prominent US policy goals run the risk of being undermined by the reports about US surveillance. We consider what measures will best achieve those goals for our global communications structure.

1. International Trade and Economic Growth

The US is committed to international economic competitiveness, to improvements in the international trade system, and to achievement of economic growth. The rules for international trade are crucial for the pervasively international conduct of commerce on the Internet, as well as for other sectors involved in international trade. Free trade agreements can contribute to economic growth. Unfortunately, foreign concerns about US surveillance threaten achievement of these various goals.

For example, the Transatlantic Trade and Investment Partnership (T-TIP) is a large and visible trade negotiation potentially affected by the

recent surveillance leaks. The T-TIP talks were launched in 2013 as “an ambitious, comprehensive, and high-standard trade and investment agreement” designed to eliminate all tariffs on trade, improve market access on trade in services, and address a wide range of other impediments to trade.¹⁶⁹ But strong concerns have been expressed about surveillance by European officials, as reflected in this statement by the EU Parliament Committee on Foreign Affairs: “With the damage to trust in the transatlantic relationship caused by NSA massive surveillance and lack of data privacy remedies for Europeans, the transatlantic economic relationship is at risk.”¹⁷⁰

European officials have similarly expressed doubt about whether to continue the existing Safe Harbor agreement for transfer of personal information to the US, under which companies are able to comply with the stricter EU privacy laws.¹⁷¹ Although the precise impact on such future negotiations is unclear, such statements show the linkage between intelligence collection decisions and international trade negotiations.

The effects of concern with US surveillance on US trade in cloud computing and other online activities have drawn particular attention. The public cloud computing market for enterprises is growing rapidly. By 2016, it is estimated to reach \$207 billion annually, more than double the

¹⁶⁹ White House Fact Sheet: *Transatlantic Trade and Investment Partnership (T-TIP)*, June, 2013, available at <http://www.ustr.gov/about-us/press-office/fact-sheets/2013/june/wh-ttip>.

¹⁷⁰ “Draft Working Document on Foreign Policy Aspect of the Inquiry on Electronic Mass Surveillance of EU Citizens,” European Parliament Committee on Foreign Affairs, Nov. 4, 2013, available at <http://www.statewatch.org/news/2013/nov/ep-nsa-surv-inq-working-document-fa-committee.pdf>.

¹⁷¹ “Bhatt Jaheen, “In Wake of PRISM, German DPAs Threaten to Halt Data Transfers to Non-EU Countries,” Bloomberg BNA, July 29, 2013, available at <http://www.bna.com/wake-prism-germann1717987502>.

2012 level.¹⁷² As a result, cloud computing vendors not only have to retain existing customers but also must recruit new customers to maintain market share. In the wake of press reports on US surveillance, two studies estimated large losses in sales for US cloud computing providers, due to concerns overseas about the security of US providers and possible legal measures to limit use of US-based cloud providers by other countries.¹⁷³ US-based information technology companies and trade associations have expressed strong concerns, fearing that Chinese, European, and other competitors will use the disclosures to promote their products over American exports.

Negative effects stemming from concern with US surveillance on trade and economic competitiveness may, in turn, have adverse effects on overall US economic growth. In recent years, the information technology sector has been a major source of innovation and growth. Foreign concerns about US surveillance can directly reduce the market share of US-based technology companies, and can in addition have an indirect effect of justifying protectionist measures. Addressing concerns about US Government surveillance would increase confidence in the US information technology sector, thus contributing to US economic growth.

¹⁷² "Garner Predict Cloud Computing Spending to Increase by 100% in 2016, says AppsCare," PRWEb.com, 2012, available at <http://prweb.com/releases/2012/7/prweb9711167.htm>.

¹⁷³ Daniel Castro, "How Much Will PRISM Cost the US Cloud Computing Industry," August, 2013 (estimating monetary impact on US cloud providers of \$21.5 billion by 2016, based on 10% loss in foreign market share), available at www2.itif.org/2013-cloud-computing-costs.pdf; Cloud Security Alliance, "CSA Survey Results: Government Access to Information", July 2013, available at https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-july-2013.pdf (losses up to \$180 billion by 2016).

2. Internet Freedom

US Internet freedom policy seeks to preserve and expand the Internet as an open, global space for free expression, for organizing and interaction, and for commerce. In recent years, the United States has highlighted Internet freedom as an important goal of US policy, including by pushing successfully in 2012 for the first United Nations resolution that confirms that human rights in the Internet realm must be protected with the same commitment as in the real world. The US has worked with the Dutch Foreign Ministry to establish the Freedom Online Coalition, currently a group of 21 governments from five regions committed to coordinating diplomatic efforts to advance Internet freedom. This Coalition has sought to broaden support for an approach based on universal human rights and the inclusive, multi-stakeholder model of Internet governance.

A central theme of US Internet freedom policy has been protection against intrusive surveillance and repression. The US Government has consistently spoken out against the arrest and persecution of bloggers and online activists in countries such as Azerbaijan, China, Cuba, Egypt, Ethiopia, Iran, Russia, Saudi Arabia, Thailand, Venezuela, and Vietnam. President Obama and Secretaries of State have publicly criticized restrictive Internet legislation designed to force companies to collaborate in censorship and pervasive surveillance of their users in order to chill expression and facilitate persecution. Since 2008, the Department of State and the United States Agency for International Development have invested over \$100 million in programs to enable human rights activists and

bloggers to exercise their human rights freely and safely online, including by distribution of strong encryption and other anti-censorship tools.

Revelations about US surveillance have threatened to undermine the US Internet freedom agenda. Countries that were previously criticized by the United States for excessive surveillance have accused the US of hypocrisy. In our view, these allegations lack force. US surveillance is subject to oversight by the multiple authorities shown in Appendix C, and the First Amendment protections under the US Constitution are an effective bulwark against censorship and political repression. Nonetheless, the reports about US surveillance have clearly made it more difficult to explain the key differences in international fora. As we have emphasized at several points in this Report, public trust is exceedingly important.

3. Internet Governance and Localization Requirements

The United States has strongly supported an inclusive multi-stakeholder model of Internet governance in order to maintain and expand a globally interoperable, open, and secure Internet architecture to which all people have access. This multi-stakeholder approach incorporates input from industry, governments, civil society, academic institutions, technical experts, and others. This approach has emphasized the primacy of interoperable and secure technical standards, selected with the help of technical experts.

A competing model, favored by Russia and a number of other countries, would place Internet governance under the auspices of the United Nations and the International Telecommunications Union (ITU).

This model would enhance the influence of governments at the expense of other stakeholders in Internet governance decisions, and it could legitimize greater state control over Internet content and communications. In particular, this model could support greater use of “localization” requirements, such as national laws requiring servers to be physically located within a country or limits on transferring data across borders.

The press revelations about US surveillance have emboldened supporters of localization requirements for Internet communications. Brazil, Indonesia, and Vietnam have proposed requiring e-mails and other Internet communications to be stored locally, in the particular country. Although generally favoring the multi-stakeholder approach to many Internet governance issues, the EU has also shifted in the direction of localization requirements. In the second half of 2013, the EU Parliament voted in favor of a proposal to limit international data flows; this provision would prohibit responding to lawful government requests, including from the US courts and government, until release of such records were approved by a European data protection authority.

Public debate has suggested a possible mix of motives supporting such localization requirements, including (1) concern about how records about their citizens will be treated in the US; (2) support for local cloud providers and other information technology companies with the effect of reducing the market share of US providers; and (3) use of the localization proposals as a way to highlight concerns about US intelligence practices and create leverage for possible changes in US policy. Whatever the mix of

motives, press reports about US surveillance have posed new challenges for the longstanding US policy favoring the multi-stakeholder approach to Internet governance as well as US opposition to localization requirements.

C. Technical Measures to Increase Security and User Confidence

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.**

Encryption is an essential basis for trust on the Internet; without such trust, valuable communications would not be possible. For the entire system to work, encryption software itself must be trustworthy. Users of encryption must be confident, and justifiably confident, that only those people they designate can decrypt their data.

The use of reliable encryption software to safeguard data is critical to many sectors and organizations, including financial services, medicine and health care, research and development, and other critical infrastructures in the United States and around the world. Encryption allows users of

information technology systems to trust that their data, including their financial transactions, will not be altered or stolen. Encryption-related software, including pervasive examples such as Secure Sockets Layer (SSL) and Public Key Infrastructure (PKI), is essential to online commerce and user authentication. It is part of the underpinning of current communications networks. Indeed, in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud.

We are aware of recent allegations that the United States Government has intentionally introduced “backdoors” into commercially available software, enabling decryption of apparently secure software. We are also aware that some people have expressed concern that such “backdoors” could be discovered and used by criminal cartels and other governments, and hence that some commercially available software is not trustworthy today.

Upon review, however, we are unaware of any vulnerability created by the US Government in generally available commercial software that puts users at risk of criminal hackers or foreign governments decrypting their data. Moreover, it appears that in the vast majority of generally used, commercially available encryption software, there is no vulnerability, or “backdoor,” that makes it possible for the US Government or anyone else to achieve unauthorized access.¹⁷⁴

¹⁷⁴ Any cryptographic algorithm can become exploitable if implemented incorrectly or used improperly.

Nonetheless, it is important to take strong steps to enhance trust in this basic underpinning of information technology. Recommendation 32 is designed to describe those steps. The central point is that trust in encryption standards, and in the resulting software, must be maintained. Although NSA has made clear that it has not and is not now doing the activities listed below, the US Government should make it clear that:

- NSA will not engineer vulnerabilities into the encryption algorithms that guard global commerce;
- The United States will not provide competitive advantage to US firms by the provision to those corporations of industrial espionage;
- NSA will not demand changes in any product by any vendor for the purpose of undermining the security or integrity of the product, or to ease NSA's clandestine collection of information by users of the product; and
- NSA will not hold encrypted communication as a way to avoid retention limits.

Although NSA is authorized to retain encrypted data indefinitely for cryptanalysis purposes, such as for encryption systems of nation-states or terrorist groups, NSA should not store generic commercial encrypted data, such as Virtual Private Network (VPN) or SSL data. If NSA is able to decrypt data years after it is collected, that data, once decrypted, should be sent to an analytic storage facility, where standard retention, minimization, and reporting rules would apply. Those rules should include minimization

of US person data and a prohibition on using data that is beyond authorized retention limits.

Recommendation 30

We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are often called “Zero Day” attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.

NSA and other US Government agencies, such as DHS, have important missions to assist US corporations in the protection of privately owned and operated critical infrastructure information networks. To do so, NSA, DHS, and other agencies should identify vulnerabilities in software widely employed in critical infrastructure and then work to eliminate those vulnerabilities as quickly as possible. That duty to defend, however, may sometimes come into conflict with the intelligence collection mission, particularly when it comes to what are known as “Zero Days.”

A Zero Day or “0 Day” exploit is a previously unknown vulnerability in software in a computer application or system – the developers or system

owners have had zero days to address or patch the vulnerability. Because the software attack technique has not been used or seen before, it enables a cyber attacker to penetrate a system or to achieve other malicious goals. In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities—“patching” them—strengthens the security of US Government, critical infrastructure, and other computer systems.

We recommend that, when an urgent and significant national security priority can be addressed by the use of a Zero Day, an agency of the US Government may be authorized to use temporarily a Zero Day instead of immediately fixing the underlying vulnerability. Before approving use of the Zero Day rather than patching a vulnerability, there should be a senior-level, interagency approval process that employs a risk management approach. The NSS should chair the process, with regular reviews. All offices and departments with relevant concerns, generally including the National Economic Council, State, Commerce, Energy, and Homeland Security, should be involved in that process.

D. Institutional Measures for Cyberspace

Recommendation 31

We recommend that the United States should support international norms or international agreements for specific measures that will increase confidence in the security of online communications. Among those measures to be considered are:

- (1) Governments should not use surveillance to steal industry secrets to advantage their domestic industry;**
- (2) Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems;**
- (3) Governments should promote transparency about the number and type of law enforcement and other requests made to communications providers;**
- (4) Absent a specific and compelling reason, governments should avoid localization requirements that (a) mandate location of servers and other information technology facilities or (b) prevent trans-border data flows.**

The US Government should encourage other countries to take specific measures to limit the possible negative consequences of their own intelligence activities, and increase public trust and user confidence in the security of online communications. Norms or agreements might be valuable for that purpose.

We suggest consideration of a series of specific steps. First, governments should not use their surveillance capabilities to steal industry secrets to advantage their domestic industries. Surveillance may take place against both foreign and domestic companies for a variety of reasons, such as to promote compliance with anti-money laundering, anti-corruption, and other laws, as well as international agreements such as economic sanctions against certain countries. The purpose of such surveillance,

however, should not be to enable a government to favor its domestic industry. Bolstering an international norm against this sort of economic espionage and competition would support economic growth, protect investment and innovation in intellectual property, and reduce costs to those innovators of protecting against nation-state cyber attacks.

Second, governments should abstain from penetrating the systems of financial institutions and changing the amounts held in accounts there. The policy of avoiding tampering with account balances in financial institutions is part of a broader US policy of abstaining from manipulation of the financial system. These policies support economic growth by allowing all actors to rely on the accuracy of financial statements without the need for costly re-verification of account balances. This sort of attack could cause damaging uncertainty in financial markets, as well as create a risk of escalating counter-attacks against a nation that began such an effort. The US Government should affirm this policy as an international norm, and incorporate the policy into free trade or other international agreements.

Third, governments should increase transparency about requests in other countries from communications providers. Elsewhere in this Report, we discuss the importance of such transparency, and recommend increasing reporting by both providers and the US Government. Transparency about the number and nature of such requests serves as a check against abuse of the lawful access process. Greater transparency can also encourage increased trust in the security of Internet communications

and reduce the risk that governments are obtaining widespread access to private communication records without the knowledge of users. Putting this sort of provision into free trade agreements or other international instruments can broaden the positive effects of greater transparency within the US.

Fourth, we support international efforts to limit localization requirements except where there is a specific and compelling reason for such actions. Global inter-operability has been a fundamental technical feature of the Internet; bits flow from one user to the next based on technical considerations rather than national boundaries. National efforts to tamper with this architecture would require pervasive technical changes and be costly in economic terms. A balkanized Internet, sometimes referred to as a “splinternet,” would greatly reduce the economic, political, cultural, and other benefits of modern communications technologies. The US Government should work with allies to reduce harmful efforts to impose localization rules onto the Internet.

Recommendation 32

We recommend that there be an Assistant Secretary of State to lead diplomacy of international information technology issues.

In the wake of recent disclosures, distortions, and controversies involving US Government intelligence collection, there is an increased need for vigorous, coordinated, senior-level US diplomacy across a broad range of inter-related information technology issues. We believe that the US should take the lead in proposing an agreement among multiple nations to

some set of Internet Norms for Cyberspace, such as a prohibition on industrial espionage, a protection of financial services and markets data standard, and others. To this end, we recommend a US diplomatic agenda to promote confidence-building measures for international cyber security, building on the Budapest Convention on Cyber Crime. The promotion of the Internet Freedom Agenda, the protection of intellectual property rights in cyber space, changes in Internet governance and the implementation of the President's International Cyber Strategy—all will necessitate agile diplomatic activity by the United States.

Currently, there is no single, senior US diplomat and no single Department of State Bureau, with lead responsibility across this broad set of issues. Just as other international, non-regional functional issues have in the past benefited from the creation of an Assistant Secretary of State position and of a State Department bureau (International Narcotics, Environmental Affairs, Counterterrorism, Human Rights), the interests of the United States would be served by the creation of a Department of State Bureau of Internet and Cyberspace Affairs, led by an experienced senior diplomat confirmed by the Senate as an Assistant Secretary of State. The Assistant Secretary would coordinate activity of the regional and functional bureaus on these issues and should, with NSS support, coordinate interagency activities with other governments.

Recommendation 33

We recommend that as part of its diplomatic agenda on international information technology issues, the United States should advocate for, and explain its rationale for, a model of Internet governance that is inclusive of all appropriate stakeholders, not just governments.

The United States Government should continue and strengthen its international advocacy for an Internet governance model that is inclusive of all appropriate stakeholders, not just governments. This recommendation builds on the administration's 2011 International Strategy for Cyberspace, which outlines multiple US Government goals with respect to global communications technologies. It articulates the need to protect national security, while also highlighting the importance of economic growth, openness, privacy protection, and a secure communications infrastructure. Other administration initiatives similarly emphasize the importance of multiple policy goals for online communications, such as the efforts led by the Department of State on the Internet Freedom agenda and the efforts led by the Department of Commerce on the Consumer Privacy Bill of Rights.

As part of the overall discussion of US policy concerning communications technology, we believe that the US Government should reaffirm that Internet governance must not be limited to governments, but should include all appropriate stakeholders. Inclusion of such stakeholders—including civil society, industry, and technical experts—is

important to ensure that the process benefits from a wide range of information and to reduce the risk of bias or partiality.

We are aware that some changes in governance approaches may well be desirable to reflect changing communications practices. For instance, the time may well be approaching for a hard look at the unique US relationship to the organization that governs the domain name system, the Internet Corporation for Assigned Names and Numbers (ICANN). The current US role is an artifact of the early history of the Internet, and may not be well suited to the broader set of stakeholders engaged in Internet governance today. The US Government and its allies, however, should continue to oppose shifting governance of the Internet to a forum, such as the International Telecommunications Union, where nation-states dominate the process, often to the exclusion of others. We believe that such a governance shift would threaten the prosperity, security, and openness of online communications.

Recommendation 34

We recommend that the US Government should streamline the process for lawful international requests to obtain electronic communications through the Mutual Legal Assistance Treaty process.

US efforts to obtain improved international cooperation on information technology issues of importance to us are undermined by the inability of the Department of Justice to provide adequate support to other nations when they request our assistance in dealing with cyber crime originating in the United States. The Justice Department has severely

under-resourced the so-called Mutual Legal Assistance Treaty (MLAT) support process.

The MLAT process essentially permits one country to seek electronic communication and other records held in other countries. For instance, non-US countries may seek e-mails held in the United States by web e-mail providers. Under the Electronic Communications Privacy Act, providers in the US can turn over the content of e-mails only through the required legal process, typically requiring probable cause that a crime has been committed.

The MLAT process creates a legal mechanism for non-US countries to obtain e-mail records, but the process today is too slow and cumbersome. Requests appear to average approximately 10 months to fulfill, with some requests taking considerably longer. Non-US governments seeking such records can face a frustrating delay in conducting legitimate investigations. These delays provide a rationale for new laws that require e-mail and other records to be held in the other country, thus contributing to the harmful trend of localization laws discussed above.

We believe that the MLAT process in the US should be streamlined, both in order to respond more promptly to legitimate foreign requests and to demonstrate the US commitment to a well-functioning Internet that meets the goals of the international community. Promising reform measures could include:

1. *Increase resources to the office in the Department of Justice that handles MLAT requests.* The Office of International Affairs (OIA) in the

Department of Justice has had flat or reduced funding over time, despite the large increase in the international electronic communications that are the subject of most MLAT requests.

2. Create an online submission form for MLATs. Today, there is no online form for foreign governments that seek to use the MLAT process. An online submission process, accompanied by clear information to foreign governments about the MLAT requirements, would make it easier for distant and diverse foreign governments to understand what is required under the US probable cause standard or other laws.

3. Streamline the number of steps in the process. Under the current system, the OIA first examines a request, and then forwards it to the US Attorney in the district where the records are held. That US Attorney's office then reviews the application a second time, and handles the request subject to the other priorities of that office. The Department of Justice should explore whether a single point of contact would be able to expedite the MLAT request.

4. Streamline provision of the records back to the foreign country. Under the current system, the provider sends the records to the Department of Justice, which then forwards the records to the requesting country. It may be possible to streamline this process by permitting the provider to send the records directly to the requesting country, with notice to the Justice Department of what has been sent.

5. Promote the use of MLATs globally and demonstrate the US Government's commitment to an effective process. Changing technology

has sharply increased the importance for non-US governments of gaining lawful access to records held in the United States. Web e-mail providers are largely headquartered in the United States, and today's use of secure encryption for e-mail means that other governments frequently cannot intercept and read the e-mail between the user and the server. It is in the interest of the United States to support the continued use of efficient and innovative technologies on the Internet, including through leading web e-mail providers. The US Government can promote this interest by publicizing and supporting the existence of a well-functioning MLAT process, thereby reducing the likelihood of harmful localization measures.

E. Addressing Future Technological Challenges

This chapter has thus far addressed issues that are currently known to implicate US intelligence and communications technology policy. Communications technology will continue to change rapidly, however, so institutional mechanisms should be in place to address such changes.

Recommendation 35

We recommend that for big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are statistically reliable, cost-effective, and protective of privacy and civil liberties.

We believe that the Intelligence Community should develop Privacy and Civil Liberties Impact Assessments for new programs or substantial modifications of existing programs that contain substantial amounts of

personally identifiable information. Under the E-Government Act of 2002, federal agencies are required to prepare Privacy Impact Assessments (PIAs) in connection with the procurement of new, or substantially modified, information technology systems. These PIAs are designed to encourage building privacy considerations early into the procurement cycle for such systems.

Our focus here is on the broader programs that may constitute multiple systems. The goal in the program assessment should be broader and more policy-based than has usually been the case for PIAs. For instance, policy officials should explicitly consider the costs and benefits of a program if it unexpectedly becomes public. In some cases, that consideration may result in modifications of the program, or perhaps even in a decision not to go forward with a program.¹⁷⁵

¹⁷⁵ We should emphasize here that data-mining and big data have been the subject of previous federally-funded reports, notably including "Safeguarding Privacy in the Fight Against Terrorism," from the Technology and Privacy Advisory Committee of the Department of Defense (2004), and "Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment," by the National Research Council (2008). These studies, have examined issues of data-mining in considerable detail, and we have found them useful and illuminating. Related academic work includes Fred H. Cate, "Government Data Mining: the Need for a Legal Framework," *Harvard Civil Rights-Civil Liberties Law Review* 43, 2008; Peter Swire, "Privacy and Information Sharing in the War Against Terrorism," 51 *Villanova Law Review* 260, 2006. We encourage agencies to study this literature, and adopt risk management approaches where feasible.

Recommendation 36

We recommend that for future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues, through the Civil Liberties and Privacy Protection Board or other agencies.

Technical collection and communications technologies continue to evolve rapidly. The US Government should adopt mechanisms that can assess and respond to emerging issues. To do this effectively, expert technologists, with clearances as needed, must be deeply involved in the process.¹⁷⁶

We recommended in Chapter VI that the CLPP Board should have an Office of Technology Assessment, capable of assessing the privacy and civil liberties implications of Intelligence Community programs. Sufficient funding for this office should be part of the generally enhanced budget for policy and oversight concerning the expensive and technically sophisticated programs of the Intelligence Community.¹⁷⁷

¹⁷⁶ The Federal Trade Commission (FTC) often plays this role for evolving privacy-related issues, such as through its recent workshops on the Internet of Things or Big Data. The FTC's jurisdiction, however, is limited to the commercial sector. It has no jurisdiction over technology issues facing government agencies, including the Intelligence Community.

¹⁷⁷ If an OTA is not created within the PCLOB or a new CLPP Board, then the intelligence community should find other mechanisms to institutionalize the effects of new programs on privacy, civil liberties, and the other important values implicated by cutting-edge intelligence technologies. These new mechanisms must include effective participation by expert technologists beyond those involved in development of the program.

President Barack Obama
 The White House
 1600 Pennsylvania Avenue NW
 Washington, DC 20500

May 19, 2015

Dear President Obama,

We the undersigned represent a wide variety of civil society organizations dedicated to protecting civil liberties, human rights, and innovation online, as well as technology companies, trade associations, and security and policy experts. We are writing today to respond to recent statements by some Administration officials regarding the deployment of strong encryption technology in the devices and services offered by the U.S. technology industry. Those officials have suggested that American companies should refrain from providing any products that are secured by encryption, unless those companies also weaken their security in order to maintain the capability to decrypt their customers' data at the government's request. Some officials have gone so far as to suggest that Congress should act to ban such products or mandate such capabilities.

We urge you to reject any proposal that U.S. companies deliberately weaken the security of their products. We request that the White House instead focus on developing policies that will promote rather than undermine the wide adoption of strong encryption technology. Such policies will in turn help to promote and protect cybersecurity, economic growth, and human rights, both here and abroad.

Strong encryption is the cornerstone of the modern information economy's security. Encryption protects billions of people every day against countless threats—be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies' most valuable trade secrets, repressive governments trying to stifle dissent, or foreign intelligence agencies trying to compromise our and our allies' most sensitive national security secrets.

Encryption thereby protects us from innumerable criminal and national security threats. This protection would be undermined by the mandatory insertion of any new vulnerabilities into encrypted devices and services. Whether you call them "front doors" or "back doors", introducing intentional vulnerabilities into secure products for the government's use will make those products less secure against other attackers. Every computer security expert that has spoken publicly on this issue agrees on this point, including the government's own experts.

In addition to undermining cybersecurity, any kind of vulnerability mandate would also seriously undermine our economic security. U.S. companies are already struggling to maintain international trust in the wake of revelations about the National Security Agency's surveillance programs. Introducing mandatory vulnerabilities into American products would further push many customers—be they domestic or international,

individual or institutional—to turn away from those compromised products and services. Instead, they—and many of the bad actors whose behavior the government is hoping to impact—will simply rely on encrypted offerings from foreign providers, or avail themselves of the wide range of free and open source encryption products that are easily available online.

More than undermining every American’s cybersecurity and the nation’s economic security, introducing new vulnerabilities to weaken encrypted products in the U.S. would also undermine human rights and information security around the globe. If American companies maintain the ability to unlock their customers’ data and devices on request, governments other than the United States will demand the same access, and will also be emboldened to demand the same capability from their native companies. The U.S. government, having made the same demands, will have little room to object. The result will be an information environment riddled with vulnerabilities that could be exploited by even the most repressive or dangerous regimes. That’s not a future that the American people or the people of the world deserve.

The Administration faces a critical choice: will it adopt policies that foster a global digital ecosystem that is more secure, or less? That choice may well define the future of the Internet in the 21st century. When faced with a similar choice at the end of the last century, during the so-called “Crypto Wars”, U.S. policymakers weighed many of the same concerns and arguments that have been raised in the current debate, and correctly concluded that the serious costs of undermining encryption technology outweighed the purported benefits. So too did the President’s Review Group on Intelligence and Communications Technologies, who unanimously recommended in their December 2013 report that 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.”

We urge the Administration to follow the Review Group’s recommendation and adopt policies that promote rather than undermine the widespread adoption of strong encryption technologies, and by doing so help lead the way to a more secure, prosperous, and rights-respecting future for America and for the world.

Thank you,

Civil Society Organizations

Access

Advocacy for Principled Action in Government

American-Arab Anti-Discrimination Committee (ADC)

American Civil Liberties Union

American Library Association

Benetech

Bill of Rights Defense Committee

Center for Democracy & Technology
 Committee to Protect Journalists
 The Constitution Project
 Constitutional Alliance
 Council on American-Islamic Relations
 Demand Progress
 Defending Dissent Foundation
 DownsizeDC.org, Inc.
 Electronic Frontier Foundation
 Electronic Privacy Information Center (EPIC)
 Engine
 Fight for the Future
 Free Press
 Free Software Foundation
 Freedom of the Press Foundation
 GNOME Foundation
 Human Rights Watch
 The Media Consortium
 New America's Open Technology Institute
 Niskanen Center
 Open Source Initiative
 PEN American Center
 Project Censored/Media Freedom Foundation
 R Street
 Reporters Committee for Freedom of the Press
 TechFreedom
 The Tor Project
 U.S. Public Policy Council of Association for Computing Machinery
 World Privacy Forum
 X-Lab

Companies & Trade Associations

ACT | The App Association
 Adobe
 Apple Inc.
 The Application Developers Alliance
 Automattic
 Blockstream
 Cisco Systems
 Coinbase
 Cloud Linux Inc.
 CloudFlare
 Computer & Communications Industry Association
 Consumer Electronics Association (CEA)
 Context Relevant
 The Copia Institute

CREDO Mobile
 Data Foundry
 Dropbox
 Evernote
 Facebook
 Gandi.net
 Golden Frog
 Google
 HackerOne
 Hackers/Founders
 Hewlett-Packard Company
 Internet Archive
 Internet Association
 Internet Infrastructure Coalition (i2Coalition)
 Level 3 Communications
 LinkedIn
 Microsoft
 Misk.com
 Mozilla
 Open Spectrum Inc.
 Rackspace
 Rapid7
 Reform Government Surveillance
 Sonic
 ServInt
 Silent Circle
 Slack Technologies, Inc.
 Symantec
 Tech Assets Inc.
 TechNet
 Tumblr
 Twitter
 Wikimedia Foundation
 Yahoo

Security and Policy Experts*

Hal Abelson, Professor of Computer Science and Engineering, Massachusetts Institute of Technology
 Ben Adida, VP Engineering, Clever Inc.
 Jacob Appelbaum, The Tor Project
 Adam Back, PhD, Inventor, HashCash, Co-Founder & President, Blockstream
 Alvaro Bedoya, Executive Director, Center on Privacy & Technology at Georgetown Law
 Brian Behlendorf, Open Source software pioneer
 Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University

Matt Bishop, Professor of Computer Science, University of California at Davis
 Matthew Blaze, Director, Distributed Systems Laboratory, University of Pennsylvania
 Dan Boneh, Professor of Computer Science and Electrical Engineering at Stanford University
 Eric Burger, Research Professor of Computer Science and Director, Security and Software Engineering Research Center (Georgetown), Georgetown University
 Jon Callas, CTO, Silent Circle
 L. Jean Camp, Professor of Informatics, Indiana University
 Richard A. Clarke, Chairman, Good Harbor Security Risk Management
 Gabriella Coleman, Wolfe Chair in Scientific and Technological Literacy, McGill University
 Whitfield Diffie, Dr. sc. techn., Center for International Security and Cooperation, Stanford University
 David Evans, Professor of Computer Science, University of Virginia
 David J. Farber, Alfred Filter Moore Professor Emeritus of Telecommunications, University of Pennsylvania
 Dan Farmer, Security Consultant and Researcher, Vicious Fishes Consulting
 Rik Farrow, Internet Security
 Joan Feigenbaum, Department Chair and Grace Murray Hopper Professor of Computer Science Yale University
 Richard Forno, Jr. Affiliate Scholar, Stanford Law School Center for Internet and Society
 Alex Fowler, Co-Founder & SVP, Blockstream
 Jim Fruchterman, Founder and CEO, Benetech
 Daniel Kahn Gillmor, ACLU Staff Technologist
 Robert Graham, creator of BlackICE, sidejacking, and masscan
 Jennifer Stisa Granick, Director of Civil Liberties, Stanford Center for Internet and Society
 Matthew D. Green, Assistant Research Professor, Johns Hopkins University Information Security Institute
 Robert Hansen, Vice President of Labs at WhiteHat Security
 Lance Hoffman, Director, George Washington University, Cyber Security Policy and Research Institute
 Marcia Hofmann, Law Office of Marcia Hofmann
 Nadim Kobeissi, PhD Researcher, INRIA
 Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology
 Nadia Heninger, Assistant Professor, Department of Computer and Information Science, University of Pennsylvania
 David S. Isenberg, Producer, Freedom 2 Connect
 Douglas W. Jones, Department of Computer Science, University of Iowa
 Susan Landau, Worcester Polytechnic Institute
 Gordon Fyodor Lyon, Founder, Nmap Security Scanner Project
 Aaron Massey, Postdoctoral Fellow, School of Interactive Computing, Georgia Institute of Technology
 Jonathan Mayer, Graduate Fellow, Stanford University
 Jeff Moss, Founder, DEF CON and Black Hat security conferences

Peter G. Neumann, Senior Principal Scientist, SRI International Computer Science Lab,
 Moderator of the ACM Risks Forum
 Ken Pfeil, former CISO at Pioneer Investments
 Ronald L. Rivest, Vannevar Bush Professor, Massachusetts Institute of Technology
 Paul Rosenzweig, Professorial Lecturer in Law, George Washington University School of
 Law
 Jeffrey I. Schiller, Area Director for Security, Internet Engineering Task Force (1994-
 2003), Massachusetts Institute of Technology
 Bruce Schneier, Fellow, Berkman Center for Internet and Society, Harvard Law School
 Micah Sherr, Assistant Professor of Computer Science, Georgetown University
 Adam Shostack, author, "Threat Modeling: Designing for Security"
 Eugene H. Spafford, CERIAS Executive Director, Purdue University
 Alex Stamos, CISO, Yahoo
 Geoffrey R. Stone, Edward H. Levi Distinguished Service Professor of Law, The
 University of Chicago
 Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia
 Institute of Technology
 C. Thomas (Space Rogue), Security Strategist, Tenable Network Security
 Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker
 Institute of Public Policy
 Nicholas Weaver, Researcher, International Computer Science Institute
 Chris Wysopal, Co-Founder and CTO, Veracode, Inc.
 Philip Zimmermann, Chief Scientist and Co-Founder, Silent Circle

*Affiliations provided only for identification purposes.

Advance Edited Version

Distr.: General
22 May 2015

Original: English

Human Rights Council

Twenty-ninth session

Agenda item 3

**Promotion and protection of all human rights, civil,
political, economic, social and cultural rights,
including the right to development**

**Report of the Special Rapporteur on the promotion and
protection of the right to freedom of opinion and expression,
David Kaye***

Summary

In the present report, submitted in accordance with Human Rights Council resolution 25/2, the Special Rapporteur addresses the use of encryption and anonymity in digital communications. Drawing from research on international and national norms and jurisprudence, and the input of States and civil society, the report concludes that encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection.

* Late submission.

Contents

	<i>Paragraphs</i>	<i>Page</i>
I. Introduction.....	1–5	3
II. Secure and private communication in the digital age.....	6–13	4
A. Contemporary encryption and anonymity.....	6–10	4
B. Uses of the technologies	11–13	5
III. Encryption, anonymity and the rights to freedom of opinion and expression and privacy	14–28	6
A. Privacy as a gateway for freedom of opinion and expression.....	16–18	7
B. Right to hold opinions without interference	19–21	8
C. Right to freedom of expression.....	22–26	9
D. Roles of corporations.....	27–28	10
IV. Evaluating restrictions on encryption and anonymity	29–55	11
A. Legal framework.....	29–35	11
B. State practice: examples and concerns.....	36–55	12
V. Conclusions and recommendations	56–63	19
A. States.....	57–60	19
B. International organizations, private sector and civil society	61–63	20

I. Introduction

1. Contemporary digital technologies offer Governments, corporations, criminals and pranksters unprecedented capacity to interfere with the rights to freedom of opinion and expression. Online censorship, mass and targeted surveillance and data collection, digital attacks on civil society and repression resulting from online expression force individuals around the world to seek security to hold opinions without interference and seek, receive and impart information and ideas of all kinds. Many seek to protect their security through encryption, the scrambling of data so only intended recipients may access it, which may be applied to data in transit (e.g., e-mail, messaging, Internet telephony) and at rest (e.g., hard drives, cloud services). Others seek additional protection in anonymity, using sophisticated technologies to disguise their identity and digital footprint. Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.

2. Yet, just as the telephone may be used both to report a crime to the police and to conspire to commit one, so too may the Internet be abused to interfere with the rights of others, national security or public order. Law enforcement and intelligence services often assert that anonymous or encrypted communications make it difficult to investigate financial crimes, illicit drugs, child pornography and terrorism. Individuals express legitimate concerns about how bullies and criminals use new technologies to facilitate harassment. Some States restrict or prohibit encryption and anonymity on these and other grounds, while others are proposing or implementing means for law enforcement to circumvent these protections and access individual communications.

3. In the light of these challenges, the present report examines two linked questions. First, do the rights to privacy and freedom of opinion and expression protect secure online communication, specifically by encryption or anonymity? And, second, assuming an affirmative answer, to what extent may Governments, in accordance with human rights law, impose restrictions on encryption and anonymity? The present report seeks to answer these questions, review examples of State practice and propose recommendations. It does not purport to address every technical or legal question raised by digital technologies, but it identifies important ones for future reporting.

4. In preparing the report, the Special Rapporteur circulated a questionnaire to States, seeking relevant information on their domestic laws, regulations, policies and practices. As of 1 April 2015, 16 States had responded to this request.¹ The Special Rapporteur also issued a call for submissions from non-governmental stakeholders and convened a meeting of experts in Geneva in March 2015. The responses from Governments and the over 30 submissions by civil society organizations and individuals, which are available from the mandate holder's web page, contributed significantly to the preparation of the report.

5. A full review of the Special Rapporteur's activities since the beginning of his term in August 2014 may be found on the mandate holder's web page. This report, the current

¹ Responses were received from Austria, Bulgaria, Cuba, Germany, Greece, Guatemala, Ireland, Kazakhstan, Lebanon, Qatar, Republic of Moldova, Norway, Slovakia, Sweden, Turkey and the United States of America.

mandate holder's first, aims at furthering the work on the challenges to freedom of expression in the digital age.

II. Secure and private communication in the digital age

A. Contemporary encryption and anonymity

6. Modern approaches to private and secure communication draw on ideas that have been with humankind for millennia. The rise of electronic data storage, the Internet and mass data collection and retention made clear that sophisticated means would be needed to protect individual, corporate and government data. As e-mail, instant-messaging, Voice-over-Internet Protocols, videoconferencing and social media moved from niche services to predominant and easily monitored modes of communication, individuals developed a need for security online, so that they could seek, receive and impart information without the risk of repercussions, disclosure, surveillance or other improper use of their opinions and expression.

7. Encryption — a mathematical “process of converting messages, information, or data into a form unreadable by anyone except the intended recipient”² — protects the confidentiality and integrity of content against third-party access or manipulation. Strong encryption, once the sole province of militaries and intelligence services, is now publicly accessible and often freely available to secure e-mail, voice communication, images, hard drives and website browsers. With “public key encryption”, the dominant form of end-to-end security for data in transit, the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses her or his own private key to decrypt them. Encryption may also be used to create digital signatures to ensure that a document and its sender are authentic, to authenticate and verify the identity of a server and to protect the integrity of communications between clients against tampering or manipulation of traffic by third parties (e.g., “man-in-the-middle” attacks). Since the encryption of data in transit does not ensure against attacks on unencrypted data when it is sitting at rest at either endpoint (nor protect the security of one's private key), one may also encrypt data at rest stored on laptops, hard drives, servers, tablets, mobile phones and other devices. Online practices may also be moving away from the system described here and towards “forward secrecy” or “off-the-record” technology in which keys are held ephemerally, particularly for uses such as instant messaging.

8. Some call for efforts to weaken or compromise encryption standards such that only Governments may enjoy access to encrypted communications. However, compromised encryption cannot be kept secret from those with the skill to find and exploit the weak points, whether State or non-State, legitimate or criminal. It is a seemingly universal position among technologists that there is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind. In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online.

9. Notably, encryption protects the content of communications but not identifying factors such as the Internet Protocol (IP) address, known as metadata. Third parties may gather significant information concerning an individual's identity through metadata analysis if the user does not employ anonymity tools. Anonymity is the condition of avoiding identification. A common human desire to protect one's identity from the crowd,

² See SANS Institute, “History of encryption” (2001).

anonymity may liberate a user to explore and impart ideas and opinions more than she would using her actual identity. Individuals online may adopt pseudonyms (or, for instance, fake e-mail or social media accounts) to hide their identities, image, voice, location and so forth, but the privacy afforded through such pseudonyms is superficial and easily disturbed by Governments or others with the necessary expertise; in the absence of combinations of encryption and anonymizing tools, the digital traces that users leave behind render their identities easily discoverable. Users seeking to ensure full anonymity or mask their identity (such as hiding the original IP address) against State or criminal intrusion may use tools such as virtual private networks (VPNs), proxy services, anonymizing networks and software, and peer-to-peer networks.³ One well-known anonymity tool, the Tor network, deploys more than 6,000 decentralized computer servers around the world to receive and relay data multiple times so as to hide identifying information about the end points, creating strong anonymity for its users.

10. A key feature of the digital age is that technology changes incessantly to sate user demands. Although the present report refers to contemporary technologies that facilitate encryption and anonymity, its analysis and conclusions apply generally to the concepts behind the current technologies and should be applicable as new technologies replace the old.

B. Uses of the technologies

11. The Internet has profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within reach of everyone who has access to it. Within a brief period, it has become the central global public forum. As such, an open and secure Internet should be counted among the leading prerequisites for the enjoyment of the freedom of expression today. But it is constantly under threat, a space — not unlike the physical world — in which criminal enterprise, targeted repression and mass data collection also exist. It is thus critical that individuals find ways to secure themselves online, that Governments provide such safety in law and policy and that corporate actors design, develop and market secure-by-default products and services. None of these imperatives is new. Early in the digital age, Governments recognized the essential role played by encryption in securing the global economy, using or encouraging its use to secure Government-issued identity numbers, credit card and banking information, business proprietary documents and investigations into online crime itself.⁴

12. Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to

³ Proxy services send data through an intermediary, or "proxy server", that sends that data on behalf of the user, effectively masking the user's IP address with its own to the end recipient. Peer-to-peer networks partition and store data among interconnected servers and then encrypt that stored data so that no centralized server has access to identifying information. See, for example, Freenet.

⁴ See OECD, *Guidelines for Cryptography Policy* (1997).

safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.

13. The “dark” side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism.⁵

III. Encryption, anonymity and the rights to freedom of opinion and expression and privacy

14. The human rights legal framework for encryption and anonymity requires, first, evaluating the scope of the rights at issue and their application to encryption and anonymity; and, second, assessing whether, and if so to what extent, restrictions may lawfully be placed on the use of technologies that promote and protect the rights to privacy and freedom of opinion and expression.

15. The rights to privacy⁶ and freedom of opinion and expression⁷ have been codified in universal and regional human rights instruments, interpreted by treaty bodies and regional courts, and evaluated by special procedures of the Human Rights Council and during universal periodic review. The universal standards for privacy, opinion and expression are found in the International Covenant on Civil and Political Rights, to which 168 States are party. Even for those remaining States that are not bound by it, the Covenant presents at the very least a standard for achievement and often reflects a customary legal norm; those that have signed but not ratified the Covenant are bound to respect its object and purpose under article 18 of the Vienna Convention on the Law of Treaties. National legal systems also protect privacy, opinion and expression, sometimes with constitutional or basic law or interpretations thereof. Several global civil society projects have also provided compelling demonstrations of the law that should apply in the context of the digital age, such as the International Principles on the Application of Human Rights to Communications

⁵ See Center for Democracy and Technology, “‘Going Dark’ versus a ‘Golden Age for Surveillance’” (2011).

⁶ Article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights, article 16 of the Convention on the Rights of the Child, article 22 of the Convention on the Rights of Persons with Disabilities, article 14 of the Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, article 8 of the European Convention on Human Rights and article 11 of the American Convention on Human Rights protect the right to privacy.

⁷ Article 19 of the Universal Declaration and the International Covenant on Civil and Political Rights, article 9 of the African Charter on Human and Peoples’ Rights, article 13 of the American Convention on Human Rights and article 10 of the European Convention on Human Rights protect freedom of expression.

Surveillance and the Global Principles on National Security and the Right to Information. Although specific standards may vary from right to right, or instrument to instrument, a common thread in the law is that, because the rights to privacy and to freedom of expression are so foundational to human dignity and democratic governance, limitations must be narrowly drawn, established by law and applied strictly and only in exceptional circumstances. In a digital age, protecting such rights demands exceptional vigilance.

A. Privacy as a gateway for freedom of opinion and expression

16. Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks. The previous mandate holder noted that the rights to “privacy and freedom of expression are interlinked” and found that encryption and anonymity are protected because of the critical role they can play in securing those rights (A/HRC/23/40 and Corr.1). Echoing article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights specifically protects the individual against “arbitrary or unlawful interference with his or her privacy, family, home or correspondence” and “unlawful attacks on his or her honour and reputation”, and provides that “everyone has the right to the protection of the law against such interference or attacks”. The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression (see General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8).

17. Encryption and anonymity are especially useful for the development and sharing of opinions, which often occur through online correspondence such as e-mail, text messaging, and other online interactions. Encryption provides security so that individuals are able “to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion” (see A/HRC/23/40 and Corr.1, para. 23). Given the power of metadata analysis to specify “an individual’s behaviour, social relationships, private preferences and identity” (see A/HRC/27/37, para. 19), anonymity may play a critical role in securing correspondence. Besides correspondence, international and regional mechanisms have interpreted privacy to involve a range of other circumstances as well.⁸

18. Individuals and civil society are subjected to interference and attack by State and non-State actors, against which encryption and anonymity may provide protection. In article 17 (2) of the International Covenant on Civil and Political Rights, States are obliged to protect privacy against unlawful and arbitrary interference and attacks. Under such an affirmative obligation, States should ensure the existence of domestic legislation that prohibits unlawful and arbitrary interference and attacks on privacy, whether committed by government or non-governmental actors. Such protection must include the right to a remedy for a violation.⁹ In order for the right to a remedy to be meaningful, individuals must be given notice of any compromise of their privacy through, for instance, weakened encryption or compelled disclosure of user data.

⁸ Human Rights Committee, general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation. See also European Court of Human Rights, factsheets on data protection (www.echr.coe.int/Documents/FS_Data_ENG.pdf) and right to protection of one’s image (www.echr.coe.int/Documents/FS_Own_image_ENG.pdf).

⁹ See Human Rights Committee general comment No. 16 and general comment No. 31 on the nature of the general legal obligation imposed on States parties to the Covenant, and CCPR/C/106/D/1803/2008.

B. Right to hold opinions without interference

19. The first article of the Universal Declaration of Human Rights recognizes that everyone is “endowed with reason and conscience”, a principle developed further in human rights law to include, among other things, the protection of opinion, expression, belief, and thought. Article 19 (1) of the International Covenant on Civil and Political Rights, also echoing the Universal Declaration, provides that “everyone shall have the right to hold opinions without interference”. Opinion and expression are closely related to one another, as restrictions on the right to receive information and ideas may interfere with the ability to hold opinions, and interference with the holding of opinions necessarily restricts the expression of them. However, human rights law has drawn a conceptual distinction between the two. During the negotiations on the drafting of the Covenant, “the freedom to form an opinion and to develop this by way of reasoning was held to be absolute and, in contrast to freedom of expression, not allowed to be restricted by law or other power”.¹⁰ The ability to hold an opinion freely was seen to be a fundamental element of human dignity and democratic self-governance, a guarantee so critical that the Covenant would allow no interference, limitation or restriction. Consequently, the permissible limitations in article 19 (3) expressly apply only to the right to freedom of expression in article 19 (2). Interference with the right to hold opinions is, by contrast, per se in violation of article 19 (1).

20. Commentators and courts have devoted much less attention to the right to hold opinions than to expression. Greater attention is warranted, however, as the mechanics of holding opinions have evolved in the digital age and exposed individuals to significant vulnerabilities. Individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions. In other words, holding opinions in the digital age is not an abstract concept limited to what may be in one’s mind. And yet, today, holding opinions in digital space is under attack. Offline, interference with the right to hold an opinion may involve physical harassment, detention or subtler efforts to punish individuals for their opinion (see CCPR/C/78/D/878/1999, annex, paras. 2.5, 7.2 and 7.3). Interference may also include such efforts as targeted surveillance, distributed denial of service attacks, and online and offline intimidation, criminalization and harassment. Targeted digital interference harasses individuals and civil society organizations for the opinions they hold in many formats. Encryption and anonymity enable individuals to avoid or mitigate such harassment.

21. The right to hold opinions without interference also includes the right to form opinions. Surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes. For all these reasons, restrictions on encryption and anonymity must be assessed to determine whether they would amount to an impermissible interference with the right to hold opinions.

¹⁰ Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), p. 441.

C. Right to freedom of expression

22. The right to freedom of expression under article 19 (2) of the International Covenant on Civil and Political Rights expands upon the Universal Declaration's already broad guarantee, protecting the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". A significant accumulation of jurisprudence, special procedure reporting, and resolutions within the United Nations and regional human rights systems underscores that the freedom of expression "is essential for the enjoyment of other human rights and freedoms and constitutes a fundamental pillar for building a democratic society and strengthening democracy" (Human Rights Council resolution 25/2). The Human Rights Council, the General Assembly and individual States regularly assert that individuals enjoy the same rights online that they enjoy offline.¹¹ The present report will not repeat all the elements of this consensus. In the context of encryption and anonymity, three aspects of the text deserve particular emphasis (see paras. 23–26 below).

23. **Freedom to seek, receive, and impart information and ideas:** In environments of prevalent censorship, individuals may be forced to rely on encryption and anonymity in order to circumvent restrictions and exercise the right to seek, receive and impart information. Some States have curtailed access with a variety of tools. State censorship, for instance, poses sometimes insurmountable barriers to the right to access information. Some States impose content-based, often discriminatory restrictions or criminalize online expression, intimidating political opposition and dissenters and applying defamation and lese-majesty laws to silence journalists, defenders and activists. A VPN connection, or use of Tor or a proxy server, combined with encryption, may be the only way in which an individual is able to access or share information in such environments.

24. It bears emphasizing that human rights law also protects the right to seek, receive and impart scientific information and ideas. The Universal Declaration and the International Covenant on Economic, Social and Cultural Rights protect rights to education and "to share in scientific advancement and its benefits". Encryption and anonymity technologies enable individuals to share in such information in situations where they are otherwise denied, and they are themselves examples of scientific advancement. Their use empowers individuals to gain access to the benefits of scientific progress that might be curtailed by Government. The Special Rapporteur in the field of cultural rights noted that "the rights to science and to culture should both be understood as including a right to have access to and use information and communication and other technologies in self-determined and empowering ways" (see A/HRC/20/26, para. 19).

25. **Regardless of frontiers:** The major instruments guaranteeing freedom of expression explicitly acknowledge the transboundary scope of the right. Individuals enjoy the right to receive information from, and transmit information and ideas of all kinds to, places beyond their borders.¹² However, some States filter or block data on the basis of keywords, denying access by deploying technologies that rely on access to text. Encryption enables an individual to avoid such filtering, allowing information to flow across borders. Moreover, individuals do not control — and are usually unaware of — how or if their communications cross borders. Encryption and anonymity may protect information of all individuals as it transits through servers located in third countries that filter content.

¹¹ See, e.g., General Assembly resolution 68/167, Human Rights Council resolution 26/13 and Council of Europe recommendation CM/Rec (2014) 6 of the Committee of Ministers to member States on a guide to human rights for Internet users.

¹² The European Court of Human Rights has recognized this point. See *Ahmet Yildirim v. Turkey*, (2012); *Cox v. Turkey*, (2010); *Case of Groppera Radio AG and Others v. Switzerland* (1990).

26. **Through any media:** Articles 19 of the Universal Declaration and the International Covenant on Civil and Political Rights were drafted with the foresight to accommodate future technological advances (A/HRC/17/27). The States parties to the Covenant chose to adopt the general phrase “through any other media” as opposed to an enumeration of then-existing media. Partly on this basis, international mechanisms have repeatedly acknowledged that the protections of freedom of expression apply to activities on the Internet. Regional courts have likewise recognized that protections apply online.¹³ The European Court of Human Rights, in discussing the similar protection of expression in the European Convention for the Protection of Human Rights and Fundamental Freedoms, has indicated that the forms and means through which information is transmitted and received are themselves protected, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.¹⁴ In this sense, encryption and anonymity technologies are specific media through which individuals exercise their freedom of expression.

D. Roles of corporations

27. Corporations in a variety of sectors play roles in advancing or interfering with privacy, opinion and expression, including encryption and anonymity. Much online communication (and virtually all of it in some countries) is carried on networks owned and operated by private corporations, while other corporations own and manage websites with substantial user-generated content. Others are active players in the surveillance and spyware markets, providing hardware and software to Governments to compromise the security of individuals online. Others develop and provide services for secure and private online storage. Telecommunications entities, Internet service providers, search engines, cloud services and many other corporate actors, often described as intermediaries, promote, regulate or compromise privacy and expression online. Intermediaries may store massive volumes of user data, to which Governments often demand access. Encryption and anonymity may be promoted or compromised by each of these corporate actors.

28. A full exploration of the role of corporations to protect their users’ security online is beyond the scope of the present report, which is focused on State obligations. However, it remains important to emphasize that “the responsibility to respect human rights applies throughout a company’s global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations” (see A/HRC/27/37, para. 43). At a minimum, corporations should apply principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative’s Principles on Freedom of Expression and Privacy, the European Commission’s ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights and the Telecommunications Industry Dialogue Guiding Principles, which encourage corporations to commit to protect human rights, undertake due diligence to ensure the positive human rights impact of their work and remediate adverse impacts of their work on human rights. In the future, the Special Rapporteur will focus on the roles

¹³ European Commission of Human Rights, *Neij and Sunde Kolmisoppi v. Sweden*, (2013); European Court of Human Rights, *Perrin v. United Kingdom*, (2005); African Court on Human and Peoples’ Rights, *Zimbabwe Lawyers for Human Rights and Institute for Human Rights and Development (on behalf of Melderum) v. Zimbabwe* (2009); *Case of Herrera Ulloa v. Costa Rica*, *Herrera Ulloa v. Costa Rica*, Preliminary Objections, Merits, Reparations and Costs, Series C No. 107, IHRL 1490 (IACHR 2004).

¹⁴ See *Autronic AG v. Switzerland* (1990); *De Haes and Gijssels v. Belgium* (1997), para. 48; *News Verlags GmbH and Co. KG v. Austria* (2000).

corporations should play in preserving individual security to exercise freedom of opinion and expression.

IV. Evaluating restrictions on encryption and anonymity

A. Legal framework

29. The permissible limitations on the right to privacy should be read strictly, particularly in an age of pervasive online surveillance — whether passive or active, mass or targeted — regardless of whether the applicable standards are “unlawful and arbitrary” under article 17 of the International Covenant on Civil and Political Rights, “arbitrary” under article 12 of the Universal Declaration, “arbitrary or abusive” under article 11 of the American Convention on Human Rights, or “necessary in a democratic society” under article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (see A/HRC/13/37, paras. 14–19). Privacy interferences that limit the exercise of the freedoms of opinion and expression, such as those described in this report, must not in any event interfere with the right to hold opinions, and those that limit the freedom of expression must be provided by law and necessary and proportionate to achieve one of a handful of legitimate objectives.

30. No restrictions may be imposed on the right to hold opinions without interference; restrictions under article 19 (3) of the Covenant only apply to expression under article 19 (2). In environments where one’s opinions, however held online, result in surveillance or harassment, encryption and anonymity may provide necessary privacy. Restrictions on such security tools may interfere with the ability of individuals to hold opinions.

31. Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.

32. First, for a restriction on encryption or anonymity to be “provided for by law”, it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation (see Human Rights Committee, general comment No. 34 (2011)). Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.¹⁵

33. Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals. Even where a State prohibits by law “advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, as provided by Article 20 of the Covenant, any restrictions on expression must be consistent with Article 19(3) (A/67/357). No other grounds may justify restrictions on the freedom of expression. Moreover, because

¹⁵ See International Covenant on Civil and Political Rights, article 2 (3)(b); CCPR/C/79/Add.110, para. 22; the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.¹⁶

34. Third, the State must show that any restriction on encryption or anonymity is “necessary” to achieve the legitimate objective.¹⁷ The European Court of Human Rights has concluded appropriately that the word “necessary” in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be something more than “useful,” “reasonable” or “desirable”.¹⁸ Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals.

35. Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online.¹⁹ A proportionality assessment should ensure that the restriction is “the least intrusive instrument amongst those which might achieve the desired result”.²⁰ The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties’ rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be “proportionate to the interest to be protected”.²¹ A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State’s burden to justify the restriction will be very high.²² Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, “a detailed and evidence-based public justification” is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression (see A/69/397, para. 12).

B. State practice: examples and concerns

36. The trend lines regarding security and privacy online are deeply worrying. States often fail to provide public justification to support restrictions. Encrypted and anonymous communications may frustrate law enforcement and counter-terrorism officials, and they complicate surveillance, but State authorities have not generally identified situations — even in general terms, given the potential need for confidentiality — where a restriction has been necessary to achieve a legitimate goal. States downplay the value of traditional non-digital tools in law enforcement and counter-terrorism efforts, including transnational

¹⁶ See Human Rights Committee, general comment No. 34 on freedom of opinion and expression, para. 30, and general comment No. 31.

¹⁷ See Human Rights Committee, general comment No. 34, para. 2, and communication No. 2156/2012, Views adopted on 10 October 2014.

¹⁸ See *Case of The Sunday Times v. United Kingdom*, judgement of 26 April 1979, para. 59.

¹⁹ See African Court Human and Peoples’ Rights, *Lohe Issa Konate v. Burkina Faso*, application No. 004/2013, paras. 148 and 149 (2014); European Court of Human Rights, *Case of The Sunday Times*, para. 62.

²⁰ See Human Rights Committee, general comment No. 27 (1999) on freedom of movement, para. 14.

²¹ See *ibid.*, para. 14.

²² See Inter-American Commission on Human Rights, OEA/Serv.L/V/II.149, para. 134.

cooperation.²³ As a consequence, the public lacks an opportunity to measure whether restrictions on their online security would be justified by any real gains in national security and crime prevention. Efforts to restrict encryption and anonymity also tend to be quick reactions to terrorism, even when the attackers themselves are not alleged to have used encryption or anonymity to plan or carry out an attack. Moreover, even where the restriction is arguably in pursuit of a legitimate interest, many laws and policies regularly do not meet the standards of necessity and proportionality and have broad, deleterious effects on the ability of all individuals to exercise freely their rights to privacy and freedom of opinion and expression.

37. It also bears noting that the United Nations itself has not provided strong communication security tools to its staff or to those who would visit United Nations websites, making it difficult for those under threat to securely reach the United Nations, human rights mechanisms online.²⁴

1. Encryption

38. Some Governments seek to protect or promote encryption to ensure the privacy of communications. For instance,²⁵ the Marco Civil da Internet Law of Brazil, adopted in 2014, guarantees the inviolability and secrecy of user communications online, permitting exceptions only by court order. The E-Commerce Act and Telecommunication Act of Austria do not restrict encryption, and the Government has undertaken public awareness campaigns to educate the public about digital security. Greek law and regulations promote the effective use of both encryption and anonymity tools. Germany, Ireland and Norway permit and promote the use of encryption technologies and oppose any efforts to weaken encryption protocols. Similarly, Swedish and Slovak laws do not restrict the use of encryption online. The United States of America encourages the use of encryption, and the United States Congress should further consider a secure data act introduced in the Congress that would prohibit the Government from requiring companies to weaken product security or insert back-door access measures. Several Governments fund efforts to share or train in the use of encryption and anonymity technologies to help individuals evade censorship and protect their security online, including Canada, the Netherlands, Sweden, the United Kingdom of Great Britain and Northern Ireland and the United States. In addition, export regulations should facilitate the transfer of encryption technologies wherever possible. Although the present report does not provide an overall legal assessment of all national approaches to encryption, these noted elements — non-restriction or comprehensive protection, the requirement of court orders for any specific limitation, and public education — deserve wider application as means to protect and promote the rights to freedom of opinion and expression.

39. Nonetheless, the regulation of encryption often fails to meet freedom of expression standards in two leading respects. First, restrictions have generally not been shown to be necessary to meet a particular legitimate interest. This is especially the case given the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that may already provide substantial information for specific law enforcement or other legitimate purposes. Second, they disproportionately impact the rights

²³ But see Centre for International Governance Innovation and Chatham House, *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance* (2015).

²⁴ For instance, staff of the Office of the United Nations High Commissioner for Human Rights (OHCHR) in Geneva do not have access to end-to-end e-mail encryption, and the OHCHR website is not encrypted.

²⁵ Many examples in this paragraph are taken from the relevant government submissions.

to freedom of opinion and expression enjoyed by targeted persons or the general population.

Bans on encryption for individual use

40. Outright prohibitions on the individual use of encryption technology disproportionately restrict the freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends.

41. State regulation of encryption may be tantamount to a ban, such as rules (a) requiring licences for encryption use; (b) setting weak technical standards for encryption; and (c) controlling the import and export of encryption tools. By limiting encryption tools to government-approved standards and controlling the import or export of encryption technologies, States ensure encryption software maintains weaknesses that allow Governments to access the content of communications. For example, while the law may be in flux, India has provided that service providers may not deploy “bulk encryption” on their networks, while the law has also restricted individuals from using encryption greater than an easily breakable 40-bit key length without prior permission and required anyone using stronger encryption to provide the Government with a copy of the encryption keys.²⁶ Reports indicate that encryption products in China may be required to adhere to government-approved encryption algorithms that have not been peer-reviewed for security.²⁷ The Pakistan Telecommunication Authority requires prior approval for the use of VPNs and encryption.²⁸ Cuba requires regulatory authorization for those using encryption.²⁹ In Ethiopia, the Government has the power to set the technical standards of encryption and recently enacted regulation that criminalizes the manufacture, assembly or import of any telecommunications equipment without a permit.³⁰ Such regulations impermissibly interfere with the individual use of encryption in communications.

Intentional weakening of encryption

42. Some States have implemented or proposed implementing so-called back-door access in commercially available products, forcing developers to install weaknesses that allow government authorities access to encrypted communications. Some Governments have developed or purchased tools to allow such access for domestic surveillance purposes.³¹ Senior officials in the United Kingdom and the United States appear to advocate requiring back-door access.³² States supporting such measures often claim that a legal framework for back-door access is necessary to intercept the content of encrypted communications. Governments proposing back-door access, however, have not

²⁶ Government of India, Ministry of Communications and IT, Licence Agreement for Provision of Internet Services, (2007). Available from http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf. See especially sect. 2.2 (vii).

²⁷ See, e.g., Counter-terrorism Law, art. 15 (initial draft of 8 November 2014). Available from <http://chinalawtranslate.com/en/ctldraft/>.

²⁸ See www.ispak.pk/Downloads/PTA_VPN_Policy.pdf.

²⁹ Submission of Cuba.

³⁰ See Ethiopia Telecom Fraud Offence Proclamation 761/2012, sects. 3–10.

³¹ See Morgan Maquis-Boire and others, *For Your Eyes Only* (2013, Citizen Lab).

³² See the speech given by Prime Minister David Cameron on 12 January 2015 at the Conservative Party pledges conference for the 2015 general election and the speech given by James Comey, Director of the Federal Bureau of Investigation, on 16 October 2014, entitled “Going dark: are technology, privacy and public safety on a collision course?”, at the Brookings Institution, Washington, D.C.

demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives. Moreover, based on existing technology, intentional flaws invariably undermine the security of all users online, since a backdoor, even if intended solely for government access, can be accessed by unauthorized entities, including other States or non-State actors. Given its widespread and indiscriminate impact, back-door access would affect, disproportionately, all online users.

43. The debate on this issue highlights a critical point: requiring encryption back-door access, even if for legitimate purposes, threatens the privacy necessary to the unencumbered exercise of the right to freedom of expression. Back-door access has practical limitations; the exploitation of intentional weaknesses could render encrypted content susceptible to attack, even if access is provided with the sole intention of allowing government or judicial control. Governments certainly face a dilemma when their obligation to protect freedom of expression is in conflict with their obligations to prevent violations of the right to life or bodily integrity, which are put at risk by terrorism and other criminal behaviour. But other recourses are available to States to request the disclosure of encrypted information, such as through judicial warrants. In such situations, States must demonstrate that general limitations on the security provided by encryption would be necessary and proportionate. States must show, publicly and transparently, that other less intrusive means are unavailable or have failed and that only broadly intrusive measures, such as backdoors, would achieve the legitimate aim. Regardless, measures that impose generally applicable restrictions on massive numbers of persons, without a case-by-case assessment, would almost certainly fail to satisfy proportionality.

Key escrows

44. A key escrow system permits individual access to encryption but requires users to store their private keys with the Government or a "trusted third party". Key escrows, however, have substantial vulnerabilities. For instance, the key escrow system depends on the integrity of the person, department or system charged with safeguarding the private keys, and the key database itself could be vulnerable to attack, undermining any user's communication security and privacy. Key escrow systems, rejected (along with back-door access) after significant debate in the United States in the so-called Crypto Wars of the 1990s, are currently in place in several countries and have been proposed in others. In 2011, Turkey passed regulations requiring encryption suppliers to provide copies of encryption keys to government regulators before offering their encryption tools to users.³³ The vulnerabilities inherent in key escrows render them a serious threat to the security to exercise the freedom of expression.

Mandatory key disclosure versus targeted decryption orders

45. In a situation where law enforcement or national security arguments may justify requests for access to communications, authorities may see two options: order either decryption of particular communications or, because of a lack of confidence that a targeted party would comply with a decryption order, disclosure of the key necessary for decryption. Targeted decryption orders may be seen as more limited and less likely to raise proportionality concerns than key disclosure, focusing on specific communications rather than an individual's entire set of communications encrypted by a particular key. Key disclosure, by contrast, could expose private data well beyond what is required by the exigencies of a situation.³⁴ Moreover, key disclosure or decryption orders often force

³³ Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting.

³⁴ The European Commission Counter-Terrorism Coordinator has urged consideration of mandatory key

corporations to cooperate with Governments, creating serious challenges that implicate individual users online. Key disclosure exists by law in a number of European countries.³⁵ In both cases, however, such orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight.

Legal presumptions

46. Some States may identify the mere use of encryption technologies as illicit behaviour. For instance, charges against the Zone 9 blogger collective in Ethiopia included suggestions that the mere training in communication security was evidence of criminal behaviour.³⁶ Such presumptions fail to meet the standards for permissible restrictions. Similarly, States undermine the rights to privacy and freedom of expression when they penalize those who produce and distribute tools to facilitate online access for activists.

2. Anonymity

47. Anonymity has been recognized for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation and debate.³⁷ The Universal Declaration and the International Covenant on Civil and Political Rights do not address anonymity. During negotiation of the Covenant, it was proposed to include in article 19 (1) the phrase, "anonymity is not permitted". However, this was rejected "on the grounds, among others, that anonymity might at times be necessary to protect the author" and "that such a clause might prevent the use of pen names".³⁸ The Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights found that "the right to freedom of thought and expression and the right to private life protect anonymous speech from government restrictions".³⁹ Several States enjoy long traditions of celebrating anonymity in their political cultures, but very few provide general protection in law for anonymous expression. Some States exert significant pressure against anonymity, offline and online. Yet because anonymity facilitates opinion and expression in significant ways online, States should protect it and generally not restrict the technologies that provide it. Several States' judiciaries have protected anonymity, at least in limited instances. For instance, the Supreme Court of Canada recently struck down the warrantless acquisition of anonymous user identity online.⁴⁰ The Constitutional Court of the Republic of Korea struck down anti-anonymity laws as unconstitutional.⁴¹ The Supreme

disclosure. See Council of the European Union, General Secretariat, meeting document D1035/15 (2015).

³⁵ See, e.g., United Kingdom, Regulation of Investigatory Powers Act (mandatory key disclosure); France, Law No. 2001-1062 (disclosure of encryption keys on authorization by a judge); Spain, Law on Telecommunications 25/2007 (key disclosure).

³⁶ See <http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/>.

³⁷ See, e.g., Inter-American Commission on Human Rights, OEA/Serv.L/V/II.149, para. 134; United States, *McIntyre v. Ohio Elections Commission* (1995); Lord Neuberger, speech to RB Conference on the Internet, entitled, "What's a name? Privacy and Anonymous Speech on the Internet" (2014).

³⁸ Marc J. Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights* (1987), pp. 379-80.

³⁹ See Organization of American States, press release 17/15.

⁴⁰ *R. v. Spencer* (2014).

⁴¹ Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012.

Court of the United States has consistently protected the right to anonymous expression.⁴² The European Court of Human Rights has recognized anonymity as important to the freedom of expression but permits limitations in cases where necessary to achieve legitimate objectives.

48. Many States recognize the lawfulness of maintaining the anonymity of journalists' sources. The Mexican Supreme Court and Mexican Code of Criminal Procedures recognize the right of journalists to maintain the anonymity of their sources; yet pressures on journalists are in fact severe.⁴³ The Constitutions of Argentina, Brazil, Ecuador and Paraguay explicitly protect sources; Chile, El Salvador, Panama, Peru, Uruguay and Venezuela (Bolivarian Republic of) protect sources in law.⁴⁴ The Mozambique Constitution protects sources, while Angola purports to do so by statute.⁴⁵ Australia, Canada, Japan and New Zealand have established case-specific judicial balancing tests to analyse source protection, although pressure on journalists may undermine such protections over time.⁴⁶ States often breach source anonymity in practice, even where it is provided for in law.

Prohibition of anonymity

49. Prohibition of anonymity online interferes with the right to freedom of expression. Many States ban it regardless of any specific government interest. The Constitution of Brazil (art. 5) prohibits anonymous speech. The Constitution of the Bolivarian Republic of Venezuela (art. 57) similarly prohibits anonymity. In 2013, Viet Nam outlawed the use of pseudonyms, which forced individuals with personal blogs to publicly list their real name and address.⁴⁷ In 2012, the Islamic Republic of Iran required the registration of all IP addresses in use inside the country and cybercafé users to register their real names before using a computer.⁴⁸ Ecuadorian law requires commenters on websites and mobile phone owners to register under a real name.⁴⁹

50. Certain States have passed laws that require real-name registration for online activity, a kind of ban on anonymity. In the Russian Federation, bloggers with 3,000 or more daily readers must register with the media regulator and identify themselves publicly, and cybercafé users reportedly must provide identification to connect to public wireless facilities.⁵⁰ China reportedly announced regulations requiring Internet users to register real

⁴² *McIntyre v. Ohio Elections Commission* (1995), pp. 342 and 343.

⁴³ See new Federal Code of Criminal Procedures, art. 244.

⁴⁴ See Argentina, Constitution, art. 43; Brazil, Constitution, title II, chap. I, art. 5, XIV; Ecuador, Constitution, art. 20; Paraguay, Constitution, art. 29 (1). See also Chile, Law 19,733; El Salvador, Criminal Procedure Code; Panama, Law 67, art. 21; Peru, Criminal Procedure Code; Uruguay, Law 16,099; Bolivarian Republic of Venezuela, Law for Journalism 4.819, art. 8.

⁴⁵ See Mozambique, Constitution, art. 48(3); Angola, Press Law 7/06, art. 20(1).

⁴⁶ Australia Evidence Amendment (Journalists' Privilege) Act 2007; Canada, Court of Queen's Bench of Alberta, *Wasylshen v. Canadian Broadcasting Corporation* (2005); Japan, Case 2006 (Kyo) No. 19 (2006); New Zealand Evidence Act, sect. 68 (2006).

⁴⁷ Human Rights Watch, "Vietnam: new decree punishes press", 23 February, 2011; Freedom House, "Vietnam: freedom of the press", 2012; Article 19, Comment on Decree No. 02 of 2011 on Administrative Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam (June 2011).

⁴⁸ Islamic Republic of Iran, Bill 106, Communication Regulation Authority.

⁴⁹ See Ecuador, Organic Law on Communications (2013).

⁵⁰ Bill No. 428884-6 amending the Federal Law on Information, Information Technologies and Protection of Information and a number of legislative acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks; Reuters, "Russia Demands Internet Users Show ID to Access Public Wifi," 8 August 2014.

names for certain websites and avoid spreading content that challenges national interests.⁵¹ South Africa also requires real name registration for online and mobile telephone users.⁵²

51. Likewise, Governments often require SIM card registration; for instance, nearly 50 countries in Africa require or are in the process of requiring the registration of personally identifiable data when activating a SIM card.⁵³ Colombia has had a mandatory mobile registration policy since 2011, and Peru has associated all SIM cards with a national identification number since 2010.⁵⁴ Other countries are considering such policies. Such policies directly undermine anonymity, particularly for those who access the Internet only through mobile technology. Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest.

52. States have also attempted to combat anonymity tools, such as Tor, proxies and VPNs, by denying access to them. China has long blocked access to Tor,⁵⁵ and Russian government officials reportedly offered more than \$100,000 for techniques to identify anonymous users of Tor.⁵⁶ In addition, Ethiopia,⁵⁷ Iran (Islamic Republic of)⁵⁸ and Kazakhstan⁵⁹ have reportedly sought to block Tor traffic. Because such tools may be the only mechanisms for individuals to exercise freedom of opinion and expression securely, access to them should be protected and promoted.

Restrictions during public unrest

53. Anonymous speech has been necessary for activists and protestors, but States have regularly attempted to ban or intercept anonymous communications in times of protest. Such attempts to interfere with the freedom of expression unlawfully pursue an illegitimate objective of undermining the right to peaceful protest under the Universal Declaration and the International Covenant on Civil and Political Rights.

Intermediary liability

54. Some States and regional courts have moved towards imposing responsibilities on Internet service providers and media platforms to regulate online comments by anonymous users. Ecuador, for instance, in its Organic Communications Law, requires intermediaries to generate mechanisms to record personal data to allow the identification of those posting comments. In *Delfi v. Estonia* (application No. 64569/09), the European Court of Human Rights upheld an Estonian law that imposes liability on a media platform for anonymous defamatory statements posted on its site. Such intermediary liability is likely to result either in real-name registration policies, thereby undermining anonymity, or the elimination of posting altogether by those websites that cannot afford to implement screening procedures,

⁵¹ China Copyright and Media, Internet User Account Name Management Regulations, article 5 (2015).

⁵² South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2003; see also Electronic Communications and Transactions Act of 2002 (requiring real name registration for service providers).

⁵³ Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration", 3 February 2014.

⁵⁴ See Colombia, Decree 1630 of 2011; Perú 21, *Los celulares de prepago en la mira*, 27 May 2010.

⁵⁵ MIT Technology Review, *How China Blocks the Tor Anonymity Network*, 4 April 2012.

⁵⁶ The original offer is available from <http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008>.

⁵⁷ Runa Sandvik, Ethiopia Introduces Deep Packet Inspection, The Tor Blog (31 May 2012); see also Article 19, 12 January 2015.

⁵⁸ "Phobos", "Iran partially blocks encrypted network traffic", The Tor Blog (10 February 2012).

⁵⁹ "Phobos", "Kazakhstan upgrades censorship to deep packet inspection", The Tor Blog (16 February 2012).

thus harming smaller, independent media. The recently adopted Manila Principles on Intermediary Liability, drafted by a coalition of civil society organizations, provide a sound set of guidelines for States and international and regional mechanisms to protect expression online.

Data retention

55. Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.

V. Conclusions and recommendations

56. Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. The Special Rapporteur therefore recommends the following.

A. States

57. States should revise or establish, as appropriate, national laws and regulations to promote and protect the rights to privacy and freedom of opinion and expression. With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education.

58. Discussions of encryption and anonymity have all too often focused only on their potential use for criminal purposes in times of terrorism. But emergency situations do not relieve States of the obligation to ensure respect for international human rights law. Legislative proposals for the revision or adoption of restrictions on individual security online should be subject to public debate and adopted according to regular, public, informed and transparent legislative process. States must promote effective participation of a wide variety of civil society actors and minority groups in such debate and processes and avoid adopting such legislation under accelerated legislative procedures. General debate should highlight the protection that encryption and anonymity provide, especially to the groups most at risk of unlawful interferences. Any such debate must also take into account that restrictions are subject to strict tests: if they interfere with the right to hold opinions, restrictions must not be adopted. Restrictions on privacy that limit freedom of expression — for purposes of the present report, restrictions on encryption and anonymity — must be provided by law and be necessary and proportionate to achieve one of a small number of legitimate objectives.

59. States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.

60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users. Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms). Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.

B. International organizations, private sector and civil society

61. States, international organizations, corporations and civil society groups should promote online security. Given the relevance of new communication technologies in the promotion of human rights and development, all those involved should systematically promote access to encryption and anonymity without discrimination. The Special Rapporteur urgently calls upon entities of the United Nations system, especially those involved in human rights and humanitarian protection, to support the use of communication security tools in order to ensure that those who interact with them may do so securely. United Nations entities must revise their communication practices and tools and invest resources in enhancing security and confidentiality for the multiple stakeholders interacting with the Organization through digital communications. Particular attention must be paid by human rights protection mechanisms when requesting and managing information received from civil society and witnesses and victims of human rights violations.

62. While the present report does not draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to freedom of expression online, corporate actors should review the adequacy of their practices with regard to human right norms. At a minimum, companies should adhere to principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers.

63. The use of encryption and anonymity tools and better digital literacy should be encouraged. The Special Rapporteur, recognizing that the value of encryption and anonymity tools depends on their widespread adoption, encourages States, civil society organizations and corporations to engage in a campaign to bring encryption by design and default to users around the world and, where necessary, to ensure that users at risk be provided the tools to exercise their right to freedom of opinion and expression securely.



Information Technology
Industry Council



SIIA Accelerating Innovation in
Technology, Data & Media

June 8, 2015

President Barack Obama
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Dear President Obama,

The undersigned associations, representing a wide range of companies in the technology sector, write in connection with encryption technologies that companies incorporate into their products and services. This correspondence is intended to provide clarity on our position and to help develop a framework for further dialogue. We also take this opportunity to point out the global implications of certain policy measures relating to encryption.

We are opposed to any policy actions or measures that would undermine encryption as an available and effective tool. As you know, encryption helps to secure many aspects of our daily lives. Encryption is an essential asset of the global digital infrastructure, enabling security and confidentiality for transactions as well as assurances to individuals that their communications are private and information is protected. For example, the rapid growth in online commerce would not have happened but for consumers' trust that their payment information is secure. Consumer trust in digital products and services is an essential component enabling continued economic growth of the online marketplace.

Accordingly, we urge you not to pursue any policy or proposal that would require or encourage companies to weaken these technologies, including the weakening of encryption or creating encryption "work-arounds." We appreciate that, where appropriate, law enforcement has the legitimate need for certain information to combat crime and threats. However, mandating the weakening of encryption or encryption "work-arounds" is not the way to address this need. Doing so would compromise the security of ICT products and services, rendering them more vulnerable to attacks and would erode consumers' trust in the products and services they rely on for protecting their information.

In addition to these security and trust concerns, the U.S. policy position on encryption will send a signal to the rest of the world. Should the U.S. government require companies to weaken encryption technology, such requirements will legitimize similar efforts by foreign governments. This would threaten the global marketplace as well as deprive individuals of certain liberties.

We are committed to finding pathways forward that preserve security, privacy, and innovation. We know the issue at hand is extremely complex, with implications both domestically and internationally. We hope that by being clear in defining the nature of the problem and our position we can contribute to the current dialogue. We look forward to continuing this discussion with your administration.

Sincerely,

Information Technology Industry Council
Software & Information Industry Association

cc: The Honorable John Kerry, U.S. Secretary of State
The Honorable Loretta Lynch, U.S. Attorney General
The Honorable Penny Pritzker, U.S. Secretary of Commerce
The Honorable Jeh Johnson, U.S. Secretary of Homeland Security
The Honorable James Comey, U.S. Director of the Federal Bureau of Investigation
The Honorable Jeffrey Zients, Director of the National Economic Council



Computer Science and Artificial Intelligence Laboratory
Technical Report

MIT-CSAIL-TR-2015-026

July 6, 2015

**Keys Under Doormats: Mandating
insecurity by requiring government
access to all data and communications**

Harold Abelson, Ross Anderson, Steven M.
Bellovin, Josh Benaloh, Matthew Blaze, Whitfield
Diffie, John Gilmore, Matthew Green, Peter G.
Neumann, Susan Landau, Ronald L. Rivest, Jeffrey
I. Schiller, Bruce Schneier, Michael Specter, and
Daniel J. Weitzner



Keys Under Doormats:

MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL
DATA AND COMMUNICATIONS

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matthew Blaze,
Whitfield Diffie, John Gilmore, Matthew Green, Peter G. Neumann, Susan Landau,
Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Abstract

Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels “going dark,” these attempts to regulate the emerging Internet were abandoned. In the intervening years, innovation on the Internet flourished, and law enforcement agencies found new and more effective means of accessing vastly larger quantities of data. Today we are again hearing calls for regulation to mandate the provision of exceptional access mechanisms. In this report, a group of computer scientists and security experts, many of whom participated in a 1997 study of these same topics, has convened to explore the likely effects of imposing extraordinary access mandates.

We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today’s Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse “forward secrecy” design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today’s Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law.

Executive Summary

Political and law enforcement leaders in the United States and the United Kingdom have called for Internet systems to be redesigned to ensure government access to information — even encrypted information. They argue that the growing use of encryption will neutralize their investigative capabilities. They propose that data storage and communications systems must be designed for *exceptional access* by law enforcement agencies. These proposals are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm.

As computer scientists with extensive security and systems experience, we believe that law enforcement has failed to account for the risks inherent in exceptional access systems. Based on our considerable expertise in real-world applications, we know that such risks lurk in the technical details. In this report we examine whether it is technically and operationally feasible to meet law enforcement's call for exceptional access without causing large-scale security vulnerabilities. We take no issue here with law enforcement's desire to execute lawful surveillance orders when they meet the requirements of human rights and the rule of law. Our strong recommendation is that anyone proposing regulations should first present concrete technical requirements, which industry, academics, and the public can analyze for technical weaknesses and for hidden costs.

Many of us worked together in 1997 in response to a similar but narrower and better-defined proposal called the Clipper Chip [1]. The Clipper proposal sought to have all strong encryption systems retain a copy of keys necessary to decrypt information with a trusted third party who would turn over keys to law enforcement upon proper legal authorization. We found at that time that it was beyond the technical state of the art to build key escrow systems at scale. Governments kept pressing for key escrow, but Internet firms successfully resisted on the grounds of the enormous expense, the governance issues, and the risk. The Clipper Chip was eventually abandoned. A much more narrow set of law enforcement access requirements have been imposed, but only on regulated telecommunications systems. Still, in a small but troubling number of cases, weakness related to these requirements have emerged and been exploited by state actors and others. Those problems would have been worse had key escrow been widely deployed. And if all information applications had had to be designed and certified for exceptional access, it is doubtful that companies like Facebook and Twitter would even exist. Another important lesson from the 1990's is that the decline in surveillance capacity predicted by law enforcement 20 years ago did not happen. Indeed, in 1992, the FBI's Advanced Telephony Unit warned that within three years Title III wiretaps would be useless: no

more than 40% would be intelligible and that in the worst case all might be rendered useless [2]. The world did not “go dark.” On the contrary, law enforcement has much better and more effective surveillance capabilities now than it did then.

The goal of this report is to similarly analyze the newly proposed requirement of exceptional access to communications in today’s more complex, global information infrastructure. We find that it would pose far more grave security risks, imperil innovation, and raise thorny issues for human rights and international relations.

There are three general problems. First, providing exceptional access to communications would force a U-turn from the best practices now being deployed to make the Internet more secure. These practices include *forward secrecy* — where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications. A related technique, *authenticated encryption*, uses the same temporary key to guarantee confidentiality and to verify that the message has not been forged or tampered with.

Second, building in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security — every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services, which tend to use similar technologies and are more likely to have the resources to manage vulnerabilities that may arise from new features. Features to permit law enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious — making security testing difficult and less effective.

Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement’s keys guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement’s stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple keyholders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the United States Government Office of Personnel Management (OPM) show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data because OPM had insecure infrastructure. If service providers implement exceptional

access requirements incorrectly, the security of all of their users will be at risk.

Our analysis applies not just to systems providing access to encrypted data but also to systems providing access directly to plaintext. For example, law enforcement has called for social networks to allow automated, rapid access to their data. A law enforcement backdoor into a social network is also a vulnerability open to attack and abuse. Indeed, Google's database of surveillance targets was surveilled by Chinese agents who hacked into its systems, presumably for counterintelligence purposes [3].

The greatest impediment to exceptional access may be jurisdiction. Building in exceptional access would be risky enough even if only one law enforcement agency in the world had it. But this is not only a US issue. The UK government promises legislation this fall to compel communications service providers, including US-based corporations, to grant access to UK law enforcement agencies, and other countries would certainly follow suit. China has already intimated that it may require exceptional access. If a British-based developer deploys a messaging application used by citizens of China, must it provide exceptional access to Chinese law enforcement? Which countries have sufficient respect for the rule of law to participate in an international exceptional access framework? How would such determinations be made? How would timely approvals be given for the millions of new products with communications capabilities? And how would this new surveillance ecosystem be funded and supervised? The US and UK governments have fought long and hard to keep the governance of the Internet open, in the face of demands from authoritarian countries that it be brought under state control. Does not the push for exceptional access represent a breathtaking policy reversal?

The need to grapple with these legal and policy concerns could move the Internet overnight from its current open and entrepreneurial model to becoming a highly regulated industry. Tackling these questions requires more than our technical expertise as computer scientists, but they must be answered before anyone can embark on the technical design of an exceptional access system.

In the body of this report, we seek to set the basis for the needed debate by presenting the historical background to exceptional access, summarizing law enforcement demands as we understand them, and then discussing them in the context of the two most popular and rapidly growing types of platform: a messaging service and a personal electronic device such as a smartphone or tablet. Finally, we set out in detail the questions for which policymakers should require answers if the demand for exceptional access is to be taken seriously. Absent a concrete technical proposal, and without adequate answers to the questions raised in this report, legislators should reject out of hand any proposal to return to the failed cryptography control policy of the 1990s.

Contents

1	Background of today's debate on exceptional access	5
1.1	Summary of the current debate	5
1.2	Findings from the 1997 analysis of key escrow systems	6
1.3	What has changed and what remains the same since 1990s?	7
2	Scenarios	11
2.1	Scenario 1: Providing exceptional access to globally distributed, encrypted messaging applications	11
2.2	Scenario 2: Exceptional access to plaintext on encrypted devices such as smartphones	14
2.3	Summary of risks from the two scenarios	15
3	Security impact of common law enforcement requirements with exceptional access	18
3.1	Access to communications content	18
3.2	Access to communications data	19
3.3	Access to data at rest	20
4	Principles at stake and unanswered questions	20
4.1	Scope, limitations, and freedoms	21
4.2	Planning and design	22
4.3	Deployment and operation	23
4.4	Evaluation, assessment, and evolution	24
5	Conclusion	24
6	Author Biographies	30
7	Acknowledgments	31

1 Background of today’s debate on exceptional access

The encryption debate has been reopened in the last year with both FBI Director James Comey and UK Prime Minister David Cameron warning, as in the early 1990s, that encryption threatens law enforcement capabilities, and advocating that the providers of services that use encryption be compelled by law to provide access to keys or to plaintext in response to duly authorized warrants. We have therefore reconvened our expert group to re-examine the impact of mandatory exceptional access in today’s Internet environment.¹

In the 1990s, the governments of United States and a number of other industrialized countries advocated weakening encryption. Claiming that widespread encryption would be disastrous for law enforcement, the US government proposed the use of the *Clipper Chip*, an encryption device that contained a government master key to give the government access to encrypted communications. Other governments followed suit with proposals for encryption licensing that would require copies of keys to be held in escrow by *trusted third parties* — companies that would be trusted to hand over keys in response to warrants. The debate engaged industry, NGOs, academia, and others. Most of the authors of the present paper wrote a report on the issues raised by key escrow or trusted-third-party encryption that analyzed the technical difficulties, the added risks, and the likely costs of such an escrow system[1]. That push for key escrow was abandoned in 2000 because of pressure from industry during the dotcom boom and because of political resistance from the European Union, among others.

1.1 Summary of the current debate

The current public policy debate is hampered by the fact that law enforcement has not provided a sufficiently complete statement of their requirements for technical experts or lawmakers to analyze. The following exhortation from United States FBI Director James Comey is as close as we come:

“We aren’t seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process — front doors that provide the evidence and information we need to investigate crime and

¹We follow the 1996 National Academies CRISIS report in using the phrase “exceptional access” to “stress that the situation is not one that was included within the intended bounds of the original transaction.” [4, p. 80]

prevent terrorist attacks.”

“Cyber adversaries will exploit any vulnerability they find. But it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end — all in the name of privacy and network security.” [5]

Prime Minister David Cameron simply wants the police to have access to everything. Speaking in the wake of the Charlie Hebdo murders in Paris, he said:

“In our country, do we want to allow a means of communication between people which, even in extremis, with a signed warrant from the home secretary personally, that we cannot read? ... The question remains: are we going to allow a means of communications where it simply is not possible to do that? My answer to that question is: no, we must not.” [6]

So, we must ask, is it possible to build in such exceptional access without creating unacceptable risk? In order to understand the technical and operational issues, we first review the results of our 1997 report and consider what has changed since then. We next try to clarify ideal law enforcement requirements and understand the kinds of risks that are likely to arise if these generic requirements are imposed broadly in the global Internet environment. Then, we present two technology scenarios typical of the landscape facing modern electronic surveillance. Combining what is publicly known about surveillance practices today, along with common legal requirements, we are able to present scenarios that illustrate many of the key risks that exceptional access will entail.

We do not suggest that our own interpretation of Comey’s stated requirements serve as a basis for regulation but merely as a starting point for discussion. If officials in the UK or US disagree with our interpretation, we urge them to state their requirements clearly. Only then can a rigorous technical analysis be conducted in an open, transparent manner. Such analysis is crucial in a world that is so completely reliant on secure communications for every aspect of daily lives, from nations’ critical infrastructure, to government, to personal privacy in daily life, to all matters of business from the trivial to the global.

1.2 Findings from the 1997 analysis of key escrow systems

We begin by reviewing the findings on the risks of key recovery/key escrow systems from a paper that many of us wrote almost 20 years ago[1]. Many of us came together then to

examine the security risks of ensuring law enforcement access to encrypted information. We found that any key escrow system had basic requirements that placed substantial costs on end users, and that these costs would have been too difficult and expensive to implement. For law enforcement to have quick and reliable access to plaintext, every key escrow system required the existence of highly sensitive yet perennially available secret keys. This requirement alone inevitably leads to an increased risk of exposure, inflated software complexity, and high economic costs.

The first downside is increased risk of a security incident. An organization that holds an escrow key could have a malicious insider that abuses its power or leaks that organization's key. Even assuming an honest agency, there is an issue of competence: cyberattacks on keyholders could easily result in catastrophic loss.

The additional complexity of a key escrow system compounds these risks. At the time, all openly proposed key escrow solutions had major flaws that could be exploited; even normal encryption was difficult to implement well, and key escrow made things much harder. Another source of complexity was the scale of a universal key recovery system — the number of agents, products, and users involved would be immense, requiring an escrow system well beyond the technology of the time. Further, key escrow threatened to increase operational complexity: a very large number of institutions would have to securely and safely negotiate targeting, authentication, validity, and information transfer for lawful information access.

All of the above factors raise costs. Risks of exposure, for instance, change the threat landscape for organizations, which must then worry about mistaken or fraudulent disclosures. The government would have increased bureaucracy to test and approve key recovery systems. Software vendors would have to bear the burden of increased engineering costs. In 1997, we found that systems enabling exceptional access to keys would be inherently less secure, more expensive, and much more complex than those without. This result helped policymakers decide against mandated exceptional access.

1.3 What has changed and what remains the same since 1990s?

It is impossible to operate the commercial Internet or other widely deployed global communications network with even modest security without the use of encryption. An extensive debate in the 1980s and 1990s about the role of encryption came to this conclusion once before. Today, the fundamental technical importance of strong cryptography and the difficulties inherent in limiting its use to meet law enforcement purposes remain the same. What has changed is that the scale and scope of systems dependent on strong encryption are far greater, and our society is far more reliant on far-flung digital networks that are

under daily attack.

In the early 1990s, the commercialization of the Internet was being thwarted by US government controls on encryption — controls that were in many ways counterproductive to long-term commercial and national security interests. A 1996 United States National Academy of Science study concluded that, “On balance, the advantages of more widespread use of cryptography outweigh the disadvantages” [4, p. 6]. Four years later, partly in response to pressures from industry, partly in response to the loosening of cryptographic export controls by the European Union, partly because crypto export controls were declared unconstitutional by US Circuit Courts, and partly because of increasing reliance on electronic communications and commerce, the US relaxed export controls on encryption [7].

The Crypto Wars actually began in the 1970s, with conflicts over whether computer companies such as IBM and Digital Equipment Corporation could export hardware and software with strong encryption, and over whether academics could publish cryptographic research freely. They continued through the 1980s over whether the NSA or the National Institute of Standards and Technology (NIST) would control the development of cryptographic standards for the non-national security side of the government (NIST was given the authority under the 1987 Computer Security Act). They came to full force during the 1990s, when the US government, largely through the use of export controls, sought to prevent companies such as Microsoft and Netscape from using strong cryptography in web browsers and other software that was at the heart of the growing Internet. The end of the wars — or the apparent end — came because of the Internet boom.

In many ways, the arguments are the same as two decades ago. US government cryptographic standards — the Data Encryption Standard then, the Advanced Encryption Standard now — are widely used both domestically and abroad. We know more now about how to build strong cryptosystems, though periodically we are surprised by a break. However, the real security challenge is not the mathematics of cryptosystems; it is engineering, specifically the design and implementation of complex software systems. Two large government efforts, `healthcare.gov` and the FBI Trilogy program, demonstrate the difficulties that scale and system integration pose in building large software systems. `Healthcare.gov`, the website implementing the president’s signature healthcare program, failed badly in its initial days, unable to serve more than a tiny percentage of users [8]. A decade earlier, five years of effort spent building an electronic case file system for the FBI — an effort that cost \$170 million — was abandoned as unworkable [9].

At one level, the worst has not come to pass — the power grid, the financial system, critical infrastructure in general, and many other systems all function reliably using com-

plex software. On another level, the worst is occurring daily. Recent breaches for financial gain include: T.J. Maxx, theft of 45 million credit card records [10]; Heartland Payment Systems, compromise of 100 million credit cards [11]; Target, compromise of 40 million credit cards; Anthem, collection of names, addresses, birthdates, employment and income information, and Social Security numbers of 80 million people that could result in identity theft [12].

Attacks on government agencies are also increasing. A set of 2003 intrusions targeting US military sites collected such sensitive data as specifications for Army helicopter mission planning systems, Army and Air Force flight-planning software, and schematics for the Mars Orbiter Lander [13]. Such theft has not only been from the defense industrial base, but has included the pharmaceuticals, Internet, biotechnology and energy industries. In 2010, then Deputy Secretary of Defense William Lynn concluded, “Although the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term” [14].

The December 2014 North Korean cyberattacks against Sony, the first such by a nation-state, resulted in large headlines. But the 2011 theft from RSA/EMC of the seed keys — initial keys used to generate other keys — in hardware tokens used to provide two-factor authentication [15], and the recent theft of personnel records from the US Office of Personnel Management are far more serious issues. The former undermined the technical infrastructure for secure systems, while the latter, by providing outsiders with personal information of government users, creates leverage for many years to come for potential insider attacks, undermining the social infrastructure needed to support secure governmental systems — including any future system for exceptional access. And while attacks against critical infrastructure have not been significant, the potential to do so has been demonstrated in test cases [16] and in an actual attack on German steel mill that caused significant damage to a blast furnace [17].

As exceptional access puts the security of Internet infrastructure at risk, the effects will be felt every bit as much by government agencies as by the private sector. Because of cost and Silicon Valley’s speed of innovation, beginning in the mid-1990s, the US government moved to a commercial off the shelf (COTS) strategy for information technology equipment, including communications devices. In 2002, Information Assurance Technical Director Richard George told a Black Hat audience that “NSA has a COTS strategy, which is: when COTS products exist with the needed capabilities, we will encourage their use whenever and wherever appropriate . . .”[18]. Such a COTS solution makes sense, of course, only if the private sector technologies the government uses are secure.

Communications technologies designed to comply with government requirements for backdoors for legal access have turned out to be insecure. For ten months in 2004 and 2005, 100 senior members of the Greek government (including the Prime Minister, the head of the Ministry of National Defense and the head of the Ministry of Justice) were wiretapped by unknown parties through lawful access built into a telephone switch owned by Vodafone Greece [19]. In 2010 an IBM researcher observed that a Cisco architecture for enabling lawful interception in IP networks was insecure.² This architecture had been public for several years, and insecure versions had been implemented by several carriers in Europe [20]. And when the NSA examined telephone switches built to comply with government-mandated access for wiretapping, it discovered security problems with *all* the switches submitted for testing[21]. Embedding exceptional access requirements into communications technology will ensure even more such problems, putting not only private-sector systems, but government ones, at risk.

Speaking on the topic of law enforcement access and systems security, Vice Chairman of the Joint Chiefs of Staff Admiral James A. Winnefeld recently remarked, “But I think we would all win if our networks are more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike [NSA Director Mike Rogers] on the intelligence side than very vulnerable networks and an easy problem for Mike and part of that, it’s not only is the right thing to do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber. I’m also very confident that Mike has some very clever people working for him, who might actually still be able to get some good work done.”

While the debate over mandated law enforcement access is not new, it does take on added urgency in today’s world. Given our growing dependence on the Internet, and the urgent need to make this and other digital infrastructures more secure, any move in the direction of decreased security should be looked upon with extreme skepticism. Once before, when considering this issue, governments around the world came to the conclusion that designing in exceptional access provisions to vital systems would increase security risk and thwart innovation. As the remainder of this paper will show, such measures are even riskier today.

²It is worth noting that the router’s design was based on standards put forth by the European Telecommunications Standards Institute.

2 Scenarios

Law enforcement authorities have stated a very broad requirement for exceptional access. Yet there are many details lacking including the range of systems to which such requirements would apply, the extraterritorial application, whether anonymous communications would be allowed, and many other variables. To analyze the range of security risks that may arise in commonly used applications and services, we examine two popular scenarios: encrypted real-time messaging services and devices such as smartphones that use strong encryption to lock access to the device.

2.1 Scenario 1: Providing exceptional access to globally distributed, encrypted messaging applications

Imagine a massively distributed global messaging application on the Internet currently using end-to-end encryption. Many examples of such systems actually exist, including Signal, which is available on iPhone and Android, Off-the-Record (OTR), a cryptography-enabling plug-in for many popular computer chat programs, and the often cited TextSecure and WhatsApp. Could one provide a secure application while meeting law enforcement exceptional access requirements?

To provide law enforcement access to encrypted data, one natural approach is to provide law enforcement direct access to keys that can be used to decrypt the data, and there is a frequently suggested and seemingly quite attractive mechanism for escrowing decryption keys. Data is typically encrypted — either for storage or transmission — with a symmetric key,³ and many data transmission protocols (e.g., the Transport Layer Security (TLS) protocol) can operate in a mode where the data to be sent is encrypted with a symmetric key that is in turn encrypted with a public key⁴ associated with the intended recipient. This encrypted symmetric key then travels with the encrypted data, and the recipient accesses the data by first using its private key to decrypt the symmetric key and then using the symmetric key to decrypt the data.

A common suggestion is to augment this approach by encrypting the symmetric key a second time — this time with a special escrowing public key. If the data is then transmitted, two encryptions of the symmetric key accompany the data — one with the public key of the intended recipient and one with a public key associated with an escrow agent. If the data has been encrypted with a symmetric key for storage rather than

³A symmetric key is one that is used for both encryption and decryption.

⁴A public key is used to encrypt data that can then be decrypted only by an entity in possession of an associated private key.

transmission, the symmetric key might be encrypted with the public key of an escrow agent and this escrowed key could remain with the encrypted data. If a law enforcement entity obtains this encrypted data — either during transmission or from storage — the escrow agent could be enlisted to decrypt the symmetric key, which could then be used to decrypt the data.

There are, however, three principal impediments to using this approach for third-party escrow. Two are technical and the third is procedural.

The first technical obstacle is that although the mode of encrypting a symmetric key with a public key is in common use, companies are aggressively moving away from it because of a significant practical vulnerability: *if an entity's private key is ever breached, all data ever secured with this public key is immediately compromised*. Because it is unwise to assume a network will never be breached, a single failure should never compromise all data that was ever encrypted.

Thus, companies are moving towards *forward secrecy*, an approach that greatly reduces the exposure of an entity that has been compromised. With forward secrecy, a new key is negotiated with each transaction, and long-term keys are used only for authentication. These transaction (or *session*) keys are discarded after each transaction — leaving much less for an attacker to work with. When a system with forward secrecy is used, an attacker who breaches a network and gains access to keys can only decrypt data from the time of the breach until the breach is discovered and rectified; historic data remains safe. In addition, since session keys are destroyed immediately after the completion of each transaction, an attacker must interject itself into the process of each transaction in real time to obtain the keys and compromise the data.⁵

The security benefits make clear why companies are rapidly switching to systems that provide forward secrecy.⁶ However, the requirement of key escrow creates a long-term vulnerability: if *any* of the private escrowing keys are *ever* compromised, then *all* data that *ever* made use of the compromised key is permanently compromised. That is, in order to accommodate the need for surreptitious, third-party access by law enforcement agencies, messages will have to be left open to attack by anyone who can obtain a copy of one of the many copies of the law enforcement keys. *Thus all known methods of achieving third-party escrow are incompatible with forward secrecy.*

Innovations providing better forward secrecy also support a broad social trend: users are moving en masse to more ephemeral communications. Reasons for moving to ephemeral communications range from practical decisions by corporations to protect proprietary in-

⁵Lack of forward secrecy was identified in the 1997 paper [1] as a weakness of key escrow systems then. Since that time, the need for forward secrecy has grown substantially.

⁶See [22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32].

formation from industrial espionage to individuals seeking to protect their ability to communicate anonymously and avoid attack by repressive governments. Many corporations delete email after 90 days, while individuals are moving from email to chat and using services like Snapchat where messages vanish after reading. Leading companies such as Twitter, Microsoft, and Facebook are supporting the move to transient messaging, and using modern security mechanisms to support it. This social and technical development is not compatible with retaining the means to provide exceptional access.

The second technical obstacle is that current best practice is often to use *authenticated encryption*, which provides *authentication* (ensuring that the entity at the other end of the communication is who you expect, and that the message has not been modified since being sent) as well as *confidentiality* (protecting the privacy of communications, including financial, medical, and other personal data). However, disclosure of the key for authenticated encryption to a third party means the message recipient is no longer provided with technical assurance of the communication's integrity; disclosure of the key allows the third party not only to *read* the encrypted traffic but also to *forg*e traffic to the recipient and make it look as if it is coming from the original sender. Thus disclosing the key to a third party creates a new security vulnerability. Going back to the encryption methods of the 1990s, with separate keys for encryption and authentication, would not only double the computational effort required, but introduce many opportunities for design and implementation errors that would cause vulnerabilities.

The third principal obstacle to third-party key escrow is procedural and comes down to a simple question: who would control the escrowed keys? Within the US, one could postulate that the FBI or some other designated federal entity would hold the private key necessary to obtain access to data and that judicial mechanisms would be constructed to enable its use by the plethora of federal, state, and local law enforcement entities. However, this leaves unanswered the question of what happens outside a nation's borders. Would German and French public- and private-sector organizations be willing to use systems that gave the US government access to their data — especially when they could instead use locally built systems that do not? What about Russia? Would encrypted data transmitted between the US and China need to have keys escrowed by both governments? Could a single escrow agent be found that would be acceptable to both governments? If so, would access be granted to just one of the two governments or would both need to agree to a request?

These difficult questions must be answered before any system of exceptional access can be implemented. Such an architecture would require global agreements on how escrow would be structured, often against the best interests of certain countries' domestic goals,

together with mandates in virtually all nations to only sell and use compliant systems.

2.2 Scenario 2: Exceptional access to plaintext on encrypted devices such as smartphones

Imagine a smartphone platform vendor that seeks to accommodate law enforcement exceptional demands. When law enforcement comes into possession of a device, perhaps at a crime scene, and then obtains the necessary legal authorization (in the US this would be a warrant as a result of *Riley v. California*), the agent collects a unique identifying number from the device through some service mechanism, and then sends a request to the platform vendor to unlock the device remotely or provide the keys necessary for law enforcement to unlock the device locally.

At first glance, providing access to plaintext on devices — laptop hard drives, smartphones, tablets — is straightforward. Indeed, many corporations already escrow device encryption keys. However, and as is frequently the case, scaling up a corporate mechanism to a global one is hard.

When encrypting device storage, the user-entered passphrase is generally not used directly as an encryption key. There are many reasons for this; from a usability perspective, the most important one is to make it easier for the user to change the passphrase. If the key were used directly, it would be a time-consuming process to decrypt and re-encrypt the entire device when the passphrase is changed. Instead, a random key is used for bulk encryption; the user-supplied key (called the Key-Encrypting Key, or KEK) is used to encrypt the random key.

To protect against brute-force attacks against the user's passphrase, the device vendor may go a step further and combine it with a device-specific unique identifier to produce the KEK. In the iPhone, the KEK is stored in a special tamper-resistant processor that limits the guess rate to once every 80 milliseconds. This protects device owners against, for example, sophisticated thieves who might try to gain access to things like banking passwords. But regardless of how the KEK is generated, obtaining access to the plaintext requires that the device-encrypting key be encrypted under some additional key or keys. These could be manufacturer-owned keys or keys belonging to one or more law enforcement agencies. Either choice is problematic[33].

If a vendor-supplied key is used, some sort of network protocol to decrypt the device key is necessary. This request must be authenticated, but how? How can the vendor have secure credentials for all of the thousands of law enforcement agencies around the world? How can the result be strongly bound to the device, to prevent unscrupulous agencies from requesting keys to devices not in their lawful possession? These are not

easy requirements to meet, especially for devices that will not even boot without a valid key. They are likely to require changes to security hardware or to the software that drives it; both are difficult to do properly. Fixing glitches — especially security glitches — in deployed hardware is expensive and often infeasible.

Providing devices with law enforcement keys is equally difficult. Again, how can the vendor know who supplied the keys? How are these keys to be changed? ⁷ How many keys can be installed without causing unacceptable slowdowns? Another alternative is to require that law enforcement ship devices back to the vendor for exceptional access decryption. However, it will still be necessary to store over long periods of time keys that can decrypt all of the sensitive data on devices. This only shifts the risks of protecting these keys to the device manufacturers.

Some would argue that per-country keys could be a sales requirement. That is, all devices sold within the US would be required to have, say, a preinstalled FBI-supplied key. That, however, does not suffice for devices brought in by travelers — and those are the devices likely to be of interest in terrorism investigations. A requirement that keys be installed at the border is also problematic. There are no standard input ports or key-loading mechanisms; furthermore, it would expose American travelers to malware installed by border guards in other countries [34, 35].

2.3 Summary of risks from the two scenarios

Designing exceptional access into today’s information services and applications will give rise to a range of critical security risks. First, major efforts that the industry is making to improve security will be undermined and reversed. Providing access over any period of time to thousands of law enforcement agencies will necessarily increase the risk that intruders will hijack the exceptional access mechanisms. If law enforcement needs to look backwards at encrypted data for one year, then one year’s worth of data will be put at risk. If law enforcement wants to assure itself real time access to communications streams, then intruders will have an easier time getting access in real time, too. This is a trade-off space in which law enforcement cannot be guaranteed access without creating serious risk that criminal intruders will gain the same access.

Second, the challenge of guaranteeing access to multiple law enforcement agencies in multiple countries is enormously complex. It is likely to be prohibitively expensive and also an intractable foreign affairs problem.

Simple requirements can yield simple solutions (e.g. a door lock). But the requirements

⁷We note that some pieces of malware, such as Stuxnet and Duqu 2, have relied on code-signing keys issued to legitimate companies. When a key is compromised, it must be replaced.

of law enforcement access to encrypted data are inherently complex and, as we have already shown, nearly contradictory. Complex or nearly contradictory requirements yield brittle, often-insecure solutions. As NSA's former head of research testified in 2013:

“When it comes to security, complexity is not your friend. Indeed it has been said that complexity is the enemy of security. This is a point that has been made often about cybersecurity in a variety of contexts including, technology, coding and policy. The basic idea is simple: as software systems grow more complex, they will contain more flaws and these flaws will be exploited by cyber adversaries.” [36]

We have a very real illustration of the problem of complexity in a recent analysis of one of the most important security systems on the Internet: SSL/TLS. Transport Layer Security (TLS) and its predecessor Secure Socket Layer (SSL) are the mechanisms by which the majority of the web encrypts its traffic — every time a user logs into a bank account, makes an electronic purchase, or communicates over a social network, that user is trusting SSL/TLS to function properly. All a user needs to know of all of this complexity is that the lock or key icon shows up in the browser window. This indicates that the communication between the user and the remote website is secure from interception.

Unfortunately, writing code that correctly implements such cryptographic protocols has proven difficult; weakened protections makes it harder still. For instance, OpenSSL, the software used by about two-thirds of websites to do TLS encryption, has been plagued with systems-level bugs resulting in catastrophic vulnerabilities. The now-infamous Heart-bleed bug was caused by a missing bounds check, an elementary programming error that lurked in the code for two years, leaving 17% of *all* websites vulnerable to data theft. More recent vulnerabilities, however, were caused by legacy restrictions on the exportation of cryptographic algorithms, dating back to the Crypto Wars. The fact that there are so many different implementations of TLS, all of which have to interoperate to make the Web secure, has proven to be a real source of security risk [37]. Website operators are reluctant to switch to more secure protocols if this will lose them even a few percent of prospective customers who are still using old software, so vulnerabilities introduced deliberately during the Crypto Wars have persisted to this day. Introducing complex new exceptional access requirements will similarly add more security bugs that will lurk in our software infrastructure for decades to come.

Third, there are broader risks for poorly deployed surveillance technology. Exceptional access mechanisms designed for law enforcement use have been exploited by hostile actors in the past. Between 1996 and 2006, it appears that insiders at Telecom Italia enabled the

wiretapping of 6,000 people, including business, financial, and political leaders, judges, and journalists [38]. In a country of 60 million, this means that no major business or political deal was truly private. The motivation here appeared to be money, including the possibility of blackmail. As we mentioned earlier, from 2004 to 2005, the cell phones of 100 senior members of the Greek government, including the Prime Minister, the head of the Ministry of National Defense, the head of the Ministry of Justice, and others. Vodafone Greece had purchased a telephone switch from Ericsson. The Greek phone company had not purchased wiretapping capabilities, but these were added during a switch upgrade in 2003. Because Vodafone Greece had not arranged for interception capabilities, the company did not have the ability to access related features, such as auditing. Nevertheless, someone acting without legal authorization was able to activate the intercept features and keep them running for ten months without being detected. The surveillance was uncovered only when some text messages went awry. Although the techniques of how it was done are understood, who was behind the surveillance remains unknown[19].

Next, there are the broader costs to the economy. Economic growth comes largely from innovation in science, technology, and business processes. At present, technological progress is largely about embedding intelligence — software and communications — everywhere. Products and services that used to be standalone now come with a mobile phone app, an online web service, and business models that involve either ads or a subscription. Increasingly these are also “social”, so you can chat to your friends and draw them into the vendor’s marketing web. Countries that require these new apps and web services to have their user-to-user communications functions authorized by the government will be at a significant disadvantage. At present, the world largely uses US apps and services, rather than the government-approved ones from Russia and China. This provides enormous leverage to US businesses.

Finally, this market advantage gives real benefits not just economically but in terms of soft power and moral leadership. The open Internet has long been a foreign policy goal of the US and its allies for a lot of good reasons. The West’s credibility on this issue was damaged by the Snowden revelations, but can and must recover. Lawmakers should not risk the real economic, geopolitical, and strategic benefits of an open and secure Internet for law enforcement gains that are at best minor and tactical.

3 Security impact of common law enforcement requirements with exceptional access

Since there is no specific statement of law enforcement requirements for exceptional access, we consider what we understand to be a very general set of electronic surveillance needs applicable in multiple jurisdictions around the world. Our goal here is to understand the general nature of security risks associated with the application of exceptional access requirements in the context of traditional categories of electronic surveillance. Law enforcement agencies in different countries have presented different requirements at different times, which we will treat under four headings: access to communications content, access to communications data, access to content at rest, and covert endpoint access. All types of access must be controlled and capable of being audited according to local legal requirements; for example, under the requirements of US law, one must respect the security and privacy of non-targeted communications.⁸

3.1 Access to communications content

Most police forces are permitted to access suspect data. In countries with respect for the rule of law, such access is carefully regulated by statute and supervised by an independent judiciary, though most of the world's population do not enjoy such legal protections. Law enforcement access might be to a central database of unencrypted messages where this exists at a central provider. Where there is no central database, such as for a telephone or video call, the police must tap the communication as it happens. How might an exceptional access requirement be implemented to enable for access to communications content? If the data is encrypted, the most obvious mechanism to allow for police access would require that traffic between Alice in country X and Bob in country Y would have its session key also encrypted under the public keys of the police forces in both X and Y, or of third parties trusted by them. This, however, raises serious issues.

First, any escrow requirement will restrict other important security functionality such as forward secrecy, the use of transient identities, and strong location privacy. As illustrated in the scenario analysis above, an exceptional access requirement overlaid on the traditional content surveillance will put the security of the content at risk. To the extent that capabilities exist to provide law enforcement exceptional access, they can be abused by others.

Second, the global nature of Internet services makes compliance with exceptional access

⁸In the USA, 47 USC 1002(a)(4)

rules both hard to define and hard to enforce. If software sold in country X will copy all keys to that country's government, criminals might simply buy their software from countries that don't cooperate; thus, US crooks might buy their software from Russia. And if software automatically chooses which governments to copy using a technique such as IP geolocation, how does one prevent attacks based on location spoofing? While it is possible to design mobile phone systems so that the host jurisdictions have access to the traffic (so long as the users do not resort to VoIP), this is a much harder task for general-purpose messaging applications.

Third, one might have to detect or deter firms that do not provide exceptional access, leading to issues around certification and enforcement. For example, if the US or the UK were to forbid the use of messaging apps that are not certified under a new escrow law, will such apps be blocked at the national firewall? Will Tor then be blocked, as in China? Or will it simply become a crime to use such software? And what is the effect on innovation if every new communications product must go through government-supervised evaluation against some new key escrow protection profile?

3.2 Access to communications data

Communications data traditionally meant call detail records and (since mobile phones became common) caller location history; it was obtained by subpoena from phone companies, and is used in the investigation of most serious violent crimes such as murder, rape, and robbery. Communications data remains widely available as service providers keep it for some time for internal purposes. However, police forces outside the US complain that the move to globalized messaging services makes a lot of data harder to obtain. For example, emails are now typically encrypted using TLS; that is, the message is encrypted between the user's computer and the service provider (e.g., Google for Gmail, Microsoft for Hotmail, etc.). Thus, to acquire the communications in plaintext, law enforcement must serve the email provider with a court order. A new UK surveillance law may require message service firms like Apple, Google, and Microsoft to honor such requests expeditiously and directly as a condition of doing business in the UK. So will there be uniform provisions for access to communications data subject to provisions for warrants or subpoenas, transparency, and jurisdiction?

As already noted, determining location is not trivial, and cheating (using foreign software, VPNs, and other proxies) could be easy. Criminals would turn to noncompliant messaging apps, raising issues of enforcement; aggressive enforcement might impose real costs on innovation and on industry generally.

3.3 Access to data at rest

Communications data are one instance of the general problem of access to data at rest. Almost all countries allow their police forces access to data. Where basic rule of law is in place, access is under the authority of a legal instrument such as a warrant or subpoena, subject to certain limits. Many corporations already insist on escrowing keys used to protect corporate data at rest (such as BitLocker on corporate laptops). So this is one field with an already deployed escrow “solution”: a fraud investigator wanting access to a London rogue trader’s laptop can simply get a law enforcement officer to serve a decryption notice on the bank’s CEO. But still, many of the same problems arise. Suspects may use encryption software that does not have escrow capability, or may fail to escrow the key properly, or may claim they have forgotten the password, or may actually have forgotten it. The escrow authority may be in another jurisdiction, or may be a counterparty in litigation. In other words, what works tolerably well for corporate purposes or in a reasonably well-regulated industry in a single jurisdiction simply does not scale to a global ecosystem of highly diverse technologies, services, and legal systems.

Another thorny case of access to data at rest arises when the data is only present on, or accessible via, a suspect’s personal laptop, tablet, or mobile phone. At present, police officers who want to catch a suspect using Tor services may have to arrest him while his laptop is open and a session is live. Law enforcement agencies in some countries can get a warrant to install malware on a suspect’s computer. Such agencies would prefer antivirus companies not to detect their malware; some might even want the vendors to help them, perhaps via a warrant to install an upgrade with a remote monitoring tool on a device with a specific serial number. The same issues arise with this kind of exceptional access, along with the issues familiar from covert police access to a suspect’s home to conduct a surreptitious search or plant a listening device. Such exceptional access would gravely undermine trust and would be resisted vigorously by vendors.

4 Principles at stake and unanswered questions

With people’s lives and liberties increasingly online, the question of whether to support law enforcement demands for guaranteed access to private information has a special urgency, and must be evaluated with clarity. From a public policy perspective, there is an argument for giving law enforcement the best possible tools to investigate crime, subject to due process and the rule of law. But a careful scientific analysis of the likely impact of such demands must distinguish what might be desirable from what is technically possible. In this regard, a proposal to regulate encryption and guarantee law enforcement access

centrally feels rather like a proposal to require that all airplanes can be controlled from the ground. While this might be desirable in the case of a hijacking or a suicidal pilot, a clear-eyed assessment of how one could design such a capability reveals enormous technical and operational complexity, international scope, large costs, and massive risks — so much so that such proposals, though occasionally made, are not really taken seriously.

We have shown that current law enforcement demands for exceptional access would likely entail very substantial security risks, engineering costs, and collateral damage. If policy-makers believe it is still necessary to consider exceptional access mandates, there are technical, operational, and legal questions that must be answered in detail before legislation is drafted. From our analysis of the two scenarios and general law enforcement access requirements presented earlier in the paper, we offer this set of questions.

4.1 Scope, limitations, and freedoms

The first set of questions that an exceptional access proposal must address concerns the scope of applicability of the exceptional access requirement, any limitations on the mandate, and what user freedoms would remain protected under such proposals. Questions such as these arise in this category:

1. Are all systems that use encryption covered, or just some? Which ones?
2. Do all online communications and information platforms have to provide access to plain text, or merely provide keys to agencies that had already collected ciphertext using technical means?
3. Would individuals, corporations, nonprofit institutions, or governments be allowed to deploy additional encryption services on top of those systems with exceptional access? Would those user-installed systems also have to meet exceptional access requirements?
4. Would machine-to-machine systems be covered? What about Internet of Things and industrial control (SCADA) systems? Much information exchange is from one machine to another, such as communicating personal health data from a sensor to a smartphone, field-based agricultural sensing devices to tractors, or load balancing controls in electric power, gas, oil and water distribution systems.
5. How would cross-border regulatory differences be resolved? Would technology developers have to meet different exceptional access requirements in each jurisdiction where their systems are used? Or would there be a globally harmonized set of regulatory requirements?

6. How can the technical design of an exceptional access system prevent mass surveillance that would covertly violate the rights of entire populations, while still allowing covert targeted surveillance of small numbers of suspects as an actual "exception" to a general rule of citizen privacy?
7. Would there be an exception for research and teaching?
8. Could companies refuse to comply with exceptional access rules based on a fear of violating human rights?
9. Would anonymous communications, widely recognized as vital to democratic societies, be allowed?

4.2 Planning and design

Designing the technology and planning the administrative procedures that would be needed to implement a comprehensive exceptional access system raises many questions:

1. What are the target cost and benefit estimates for such a program? No system is cost-free and this one could be very expensive, especially if it has to accommodate a large number of providers, such as today's millions of app developers.
2. What security and reliability measures would be established for the design? How would system prototypes be tested? How long would companies have to comply with exceptional access rules?
3. How would existing services and products be treated if they do not comply with exceptional access rules? Would providers have to redesign their systems? What if those systems cannot accommodate exceptional access requirements?
4. Who would be involved in the design of the systems and procedures — just the US government, or would other governments be invited to participate? Could foreign technology providers such as Huawei participate in the design discussions?
5. Would the technical details of the program be made public and open for technical review? What level of assurance would be provided for the design?
6. We note that it generally takes many years after a cryptographic protocol is published before it is deemed secure enough for actual use. For example, the Needham-Schroeder public-key protocol, first published in 1978 [39], was discovered to have security flaw only in 1995 by Gavin Lowe (17 later!) [40].

4.3 Deployment and operation

Once regulations are established and technical design parameters set, there would remain questions about how systems would be deployed, who would supervise and regulate compliance, and how the design of the system would evolve to address inevitable technical and operational bugs that emerge. We know of no system that is designed perfectly the first time, and it is well understood that maintenance, support, and evolution of existing systems constitutes a major expense.

1. Who would supervise compliance? Would an existing regulatory agency such as the FCC be given jurisdiction over the entire process? How would other countries regulate US domestic and foreign services? Would there be a global harmonization of rules regulation and enforcement? Would the International Telecommunications Union have a role in setting and enforcing requirements?
2. Would global technical standards be required? How would these be developed and enforced? How would be such standards be changed/improved/patched? Would traditional standards bodies such as the UN International Telecommunications Union T-sector or ISO set standards, or would the world look to Internet standards bodies such as the IETF and the World Wide Web Consortium? How would the world converge on one set of standards?
3. Would the US government provide reference software libraries implementing the desired functionality?
4. Would programs and apps need to be certified before they were allowed to be sold? Who would test or certify that programs produced operate as intended?
5. Who would be liable if the plaintext-disclosure mechanisms were buggy (either in design or in implementation), causing the disclosure of all citizens' information? More generally, what would happen when (not if) critical secret information was revealed, such as the private keys that allow encrypted data to be read by anyone, that destroyed the privileged position of law enforcement?
6. How many companies would withdraw all but local sales staff from markets where exceptional access was mandated in ways that clashed with their business strategies or the rights of users in other countries, as Google already has done from China and Russia?

4.4 Evaluation, assessment, and evolution

Large systems exist because successful systems evolve and grow. Typically, this evolution happens through interaction guided by the institution (software company, government agency, or open-source community) responsible for the system. A system that evolves subject to a set of constraints, such as medical systems that need to maintain a safety case or flight control systems that need to maintain not just a safety case but also need to meet real-time performance requirements, evolve less quickly and at more cost. If all systems that communicate must in future evolve subject to an exceptional access constraint, there will be real costs, which are hard to quantify, since the question of who exactly would be responsible for establishing and policing the exceptional access constraint is not clear. However that question is answered, the following further issues will arise.

1. What oversight program would be required to monitor the effectiveness, cost, benefits, and abuse of exceptional access?
2. What sunset provisions would be build into legislation for such a program? What conditions would be in place for its termination (e.g., for lack of sufficient benefit, for excessive cost, or for excessive abuse)?
3. One unintended consequence of such a program may be a much-reduced use of crypto altogether. This would further weaken our already fragile and insecure information infrastructure, so how do we incentivize companies to continue encrypting sensitive user communications?
4. A further unintended consequence of such a program might be to make the US and other participating countries less welcoming to technological innovation; diminishing or displacing innovation may have consequences for economic growth and national security. How will these economic impacts be assessed before an exceptional access program is mandated? Further, what economic effect would be considered too impactful for exceptional access to be considered worthwhile?

5 Conclusion

Even as citizens need law enforcement to protect themselves in the digital world, all policy-makers, companies, researchers, individuals, and law enforcement have an obligation to work to make our global information infrastructure more secure, trustworthy, and resilient. This report's analysis of law enforcement demands for exceptional access to private communications and data shows that such access will open doors through which

criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend. The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict. The costs to developed countries' soft power and to our moral authority would also be considerable. Policy-makers need to be clear-eyed in evaluating the likely costs and benefits. It is no surprise that this report has ended with more questions than answers, as the requirements for exceptional access are still vague. If law enforcement wishes to prioritize exceptional access, we suggest that they need to provide evidence to document their requirements and then develop genuine, detailed specifications for what they expect exceptional access mechanisms to do. As computer scientists and security experts, we are committed to remaining engaged in the dialogue with all parts of our governments, to help discern the best path through these complex questions.

References

- [1] H. Abelson, R. N. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller, and others, "The risks of key recovery, key escrow, and trusted third-party encryption," 1997. [Online]. Available: <http://academiccommons.columbia.edu/catalog/ac:127127>
- [2] Advanced Telephony Unit, Federal Bureau of Investigation, "Telecommunications Overview, slide on Encryption Equipment," 1992. [Online]. Available: https://www.cs.columbia.edu/~smb/Telecommunications_Overview_1992.pdf
- [3] E. Nakashima, "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say," *The Washington Post*, May 2013. [Online]. Available: https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html
- [4] K. W. Dam, H. S. Lin, and others, *Cryptography's role in securing the information society*. National Academies Press, 1996.
- [5] James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" Oct. 2014, speech at the Brookings Institution. [Online]. Available: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>

- [6] David Cameron, “PM: spy agencies need more powers to protect Britain,” Jan. 2015. [Online]. Available: <https://embed.theguardian.com/embed/video/uk-news/video/2015/jan/12/david-cameron-spy-agencies-britain-video>
- [7] W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, Mass: The MIT Press, Jan. 1998.
- [8] Paul Ford, “The Obamacare Website Didn’t Have to Fail. How to Do Better Next Time,” Oct. 2013. [Online]. Available: <http://www.bloomberg.com/bw/articles/2013-10-16/open-source-everything-the-moral-of-the-healthcare-dot-gov-debacle>
- [9] D. Eggen and G. Witte, “The FBI’s Upgrade That Wasn’t,” *The Washington Post*, Aug. 2006. [Online]. Available: <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/17/AR2006081701485.html>
- [10] Jaikumar Vijayan, “TJX data breach: At 45.6m card numbers, it’s the biggest ever,” Mar. 2007. [Online]. Available: <http://www.computerworld.com/article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html>
- [11] Brian Krebs, “Security fix - payment processor breach may be largest ever,” Jan. 2009. [Online]. Available: http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html
- [12] R. Abelson and M. Goldstein, “Anthem Hacking Points to Security Vulnerability of Health Care Industry,” *The New York Times*, Feb. 2015. [Online]. Available: <http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html>
- [13] N. Thornburgh, “The Invasion of the Chinese Cyberspies,” *Time*, Aug. 2005. [Online]. Available: <http://content.time.com/time/magazine/article/0,9171,1098961,00.html>
- [14] William J. Lynn III, “Defending a New Domain,” *Foreign Affairs*, Oct. 2010. [Online]. Available: <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>
- [15] Arthur Coviello, “Open Letter from Arthur Coviello, Executive Chairman, RSA, Security Division of EMC, to RSA customers,” Mar. 2011.
- [16] Jeanne Meserve, “Sources: Staged cyber attack reveals vulnerability in power grid - CNN.com,” *CNN*, Sep. 2007. [Online]. Available: <http://www.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=topnews>

- [17] K. Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," Jan. 2015. [Online]. Available: <http://www.wired.com/2015/01/german-steel-mill-hack-destruction/>
- [18] R. George, "Views on the future direction of information assurance," Jul. 2002, remarks by Richard George at Blackhat Las Vegas. [Online]. Available: <https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-george-keynote.doc>
- [19] V. Prevelakis and D. Spinellis, "The athens affair," *Spectrum, IEEE*, vol. 44, no. 7, pp. 26–33, 2007. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4263124
- [20] Tom Cross, "Exploring Lawful Intercept to Wiretap the Internet," Washington, DC, USA, 2010. [Online]. Available: https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-Lawfull-Intercept-slides.pdf
- [21] Richard George, "Private communication between Richard George, Former Technical Director, Information Assurance Directorate, NSA and Susan Landau," Dec. 2011.
- [22] Nicole Perlroth and Vindu Goel, "Twitter Toughening Its Security to Thwart Government Snoops," Nov. 2013. [Online]. Available: <http://bits.blogs.nytimes.com/2013/11/22/twitter-toughening-its-security-to-thwart-government-snoops/>
- [23] Larry Seltzer, "Google moves forward towards a more perfect SSL," Nov. 2013. [Online]. Available: <http://www.zdnet.com/article/google-moves-forward-towards-a-more-perfect-ssl/>
- [24] D. Gupta, "Google Enables 'Forward Secrecy (PFS)' by 'Default' for HTTPS Services," Nov. 2011. [Online]. Available: <http://www.ditii.com/2011/11/23/google-enables-forward-secrecy-pfs-by-default-for-https-services/>
- [25] Selena Larson, "After Heartbleed, 'Forward Secrecy' Is More Important Than Ever," Apr. 2014. [Online]. Available: <http://readwrite.com/2014/04/15/heartbleed-perfect-forward-secrecy-security-encryption>
- [26] Adam Langley, "Protecting data for the long term with forward secrecy," Nov. 2011. [Online]. Available: <http://googleonlinesecurity.blogspot.com/2011/11/protecting-data-for-long-term-with.html>
- [27] J. Kiss, "Twitter adds more security to thwart predators and government agencies," Nov. 2013. [Online]. Available: <http://www.theguardian.com/technology/2013/nov/23/twitter-security-google-facebook-data-nsa>

- [28] Parker Higgins, “Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection,” Aug. 2013. [Online]. Available: <https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection>
- [29] Michael Mimoso, “Microsoft Expands TLS, Forward Secrecy Support | Threatpost | The first stop for security news,” Jul. 2014. [Online]. Available: <https://threatpost.com/microsoft-expands-tls-forward-secrecy-support/106965>
- [30] —, “Microsoft Brings Perfect Forward Secrecy to Windows | Threatpost | The first stop for security news,” May 2015. [Online]. Available: <https://threatpost.com/new-crypto-suites-bring-perfect-forward-secrecy-to-windows/112783>
- [31] P. Bright, “Microsoft expands the use of encryption on Outlook, OneDrive,” Jul. 2014. [Online]. Available: <http://arstechnica.com/security/2014/07/microsoft-expands-the-use-of-encryption-on-outlook-onedrive/>
- [32] Liam Tung, “Yahoo finally enables HTTPS encryption for email by default,” Jan. 2014. [Online]. Available: <http://www.zdnet.com/article/yahoo-finally-enables-https-encryption-for-email-by-default/>
- [33] Apple, “iOS Security on iOS 8.3 or Later,” Tech. Rep., Apr. 2015. [Online]. Available: https://www.apple.com/business/docs/iOS_Security_Guide.pdf
- [34] N. Perlroth, “Electronic Security a Worry in an Age of Digital Espionage,” *The New York Times*, Feb. 2012. [Online]. Available: <http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html>
- [35] Ben Thompson, “UAE Blackberry update was spyware,” *BBC*, Jul. 2009. [Online]. Available: <http://news.bbc.co.uk/2/hi/8161190.stm>
- [36] Frederick R. Chang, “Is Your Data on the Healthcare.gov Website Secure?” Written Testimony, U.S. House of Representatives, Nov. 2013. [Online]. Available: <http://docs.house.gov/meetings/SY/SY00/20131119/101533/HHRG-113-SY00-Wstate-ChangF-20131119.pdf>
- [37] B. Beurdouche, K. Bhargavan, A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, and J. K. Zinzindohoue, “A messy state of the union: Taming the composite state machines of TLS,” in *IEEE Symposium on Security and Privacy*, 2015. [Online]. Available: <https://www.smacktls.com/smack.pdf>

- [38] Piero Colaprico, ““Da Telecom dossier sui Ds” Mancini parla dei politici - cronaca - Repubblica.it,” Jan. 2007. [Online]. Available: <http://www.repubblica.it/2006/12/sezioni/cronaca/sismi-mancini-8/dossier-ds/dossier-ds.html>
- [39] R. M. Needham and M. D. Schroeder, “Using encryption for authentication in large networks of computers,” *Communications of the ACM*, vol. 21, no. 12, pp. 993–999, 1978. [Online]. Available: <http://dl.acm.org/citation.cfm?id=359659>
- [40] G. Lowe, “An Attack on the Needham-Schroeder Public-key Authentication Protocol,” *Information Processing Letters*, vol. 56, no. 3, pp. 131–133, Nov. 1995. [Online]. Available: [http://dx.doi.org/10.1016/0020-0190\(95\)00144-2](http://dx.doi.org/10.1016/0020-0190(95)00144-2)

6 Author Biographies

Harold “Hal” Abelson is a Professor of Electrical Engineering and Computer Science at MIT, a fellow of the IEEE, and a founding director of both Creative Commons and the Free Software Foundation.

Ross Anderson is Professor of Security Engineering at the University of Cambridge.

Steven M. Bellovin is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University.

Josh Benaloh is Senior Cryptographer at Microsoft Research where his research focuses on verifiable election protocols and related technologies.

Matt Blaze is Associate Professor of Computer and Information Science at the University of Pennsylvania where he directs the Distributed Systems Lab.

Whitfield “Whit” Diffie is an American cryptographer whose 1975 discovery of the concept of public-key cryptography opened up the possibility of secure, Internet-scale communications.

John Gilmore is an entrepreneur and civil libertarian. He was an early employee of Sun Microsystems, and co-founded Cygnus Solutions, the Electronic Frontier Foundation, the Cypherpunks, and the Internet’s *alt* newsgroups.

Matthew Green is a Research Professor at the Johns Hopkins University Information Security Institute. His research focus is on cryptographic techniques for maintaining users’ privacy, and on new techniques for deploying secure messaging protocols.

Peter G. Neumann, Senior Principal Scientist at the SRI International Computer Science Lab, and moderator of the ACM Risks Forum for thirty years.

Susan Landau is a professor of cybersecurity policy at Worcester Polytechnic Institute. She is the author of *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (MIT Press, 2011) and co-author, with Whitfield Diffie, of *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 1998).

Ronald L. Rivest is an MIT Institute Professor, and well known for his co-invention of the RSA public-key cryptosystem, as well for founding RSA Security and Verisign.

Jeffrey I. Schiller was the Internet Engineering Steering Group Area Director for Security (1994–2003).

Bruce Schneier is a security technologist, author, Fellow at the Berkman Center for Internet and Society at Harvard Law School, and the CTO of Resilient Systems, Inc. He has written a number of books, including *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (Norton, 2015).

Michael A. Specter is a security researcher and PhD candidate in Computer Science at MIT's Computer Science and Artificial Intelligence Laboratory.

Daniel J. Weitzner is Principal Research Scientist at the MIT Computer Science and Artificial Intelligence Lab and Founding Director, MIT Cybersecurity and Internet Policy Research Initiative. From 2011–2012, he was United States Deputy Chief Technology Officer in the White House.

7 Acknowledgments

The authors thank several individuals who were extremely helpful in the production of this report. Alan Davidson was instrumental in the early discussions that led to this report while he was Vice President and Director of the Open Technology Institute at the New America Foundation. Beth Friedman, Technical Communicator at Resilient Systems, provided invaluable editing support. The MIT Cybersecurity and Internet Policy Research Initiative helped with convening the authors and producing the final version of the report.



Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

United States Senate
Committee on the Judiciary
July 8, 2015

Statement of the Application Developers Alliance

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.

This statement shares with the Committee 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. Some witnesses and written statements will almost certainly discuss the technological impossibility of this task. Alliance members are concerned about the technical challenges and costs, but also about the resulting legal and investment uncertainty, consumer mistrust, and business turbulence that will result from these internally conflicting goals. The Alliance urges the Judiciary Committee and the 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. The Alliance urges the Committee 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 our phones have a traditional mobile telephone service as well as Viber, WhatsApp, Google Hangouts and Skype. Each of these apps, the phone's operating system, the software in each network access point and the networks themselves may incorporate encryption so that personal 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 the global focus on trust and security, many businesses are bundling encryption with products and services and are investing to improve those offerings. 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 Committee 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 and enterprise 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 companies may 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 by requirements to build multiple back doors, and will also have greater trust problems than established competitors. Of course, apps that do not comply with a

government's 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, the App Developers Alliance urges the Committee and 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.

Thank you for the opportunity to share our thoughts about this important matter. The App Developers Alliance looks forward to working with the Committee on this very important issue.



July 8, 2015

The Honorable Charles E. Grassley
Chairman
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Patrick J. Leahy
Ranking Member
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Richard Burr
Chairman
U.S. Senate Select Committee on Intelligence
221 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Dianne Feinstein
Vice Chairman
U.S. Senate Select Committee on Intelligence
221 Hart Senate Office Building
Washington, D.C. 20510

Dear Chairman Grassley, Chairman Burr, Ranking Member Leahy, and Vice Chairman Feinstein:

On behalf of BSA | The Software Alliance¹ (BSA), I write to express our appreciation for both the U.S. Senate Committee on the Judiciary and the U.S. Senate Select Committee on Intelligence holding hearings today on the issues of encryption, technology, and the legitimate roles of law enforcement and security agencies. We believe these hearings will foster a constructive public dialogue about these important topics, which are a crucial concern to the technology companies BSA represents, their customers at home and abroad, and government agencies charged with protecting our security.

This letter provides the perspective of BSA members—companies that develop and offer essential software, security tools, communications devices, servers, and computers that drive the American and global information economy, and that improve our daily lives.

Today's consumers use technology and store massive amounts of personal information and highly sensitive business information in dramatic new ways. A safe and secure data storage system is critical to all of our daily lives. The data stored with technology companies often is highly personal—and users rightly view it as their own. The data a single user stores with a technology provider can display the sum of her private life. Anyone with access to that data would be able to recreate her movements, her communications, her purchases, and even her thoughts, as revealed, for example, in her web queries. While many of our laws are designed to protect the sanctity of the information an individual secrets inside her home, individuals may consider the data they store with technology companies as being even more sensitive.

BSA members earn users' trust by providing essential security technologies that protect users against cyber threats. That is why BSA members create, develop, and deploy products and services that incorporate robust security measures in response to our users' demands. These security measures include the encryption of data both at rest and in transit, including user-controlled encryption features.

¹ BSA's members include: Adobe, Altium, Apple, ANSYS, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Datastax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

Chairman Grassley, Chairman Burr, Ranking Member Leahy, and Vice Chairman Feinstein
 July 8, 2015
 Page 2

Those features put control in the hands of the user, and in so doing help increase both security and user trust.

Our member companies are fully committed to the important mission of law enforcement in keeping Americans safe and investigating criminal activity and stand ready to do their part. At the same time, companies need both clarity about their obligations and the freedom to innovate to meet users' demands.

Our goal is to ensure our users' information remains truly private and out of the hands of bad actors. To achieve this goal, we need safeguards that responsibilities imposed on technology companies do not endanger the security of our users' information, or network security more broadly.

Some have proposed solutions that would limit the use of security technologies, build in flaws, or dictate design and capabilities by requiring master encryption keys. Unfortunately, these are not real solutions. Rather, they are recipes for further problems. Such proposals would actually undermine the effectiveness of the security tools we use to keep our users' information safe and secure. These proposals would weaken our ability to protect users' information from cybercriminals, undermine the viability of information tools, and harm the consumer trust equation. Importantly, requiring technology that provides law enforcement access to information also risks undermining the security of all electronic communications and digitally stored information. Put simply, proposals to require a "back door" into encrypted information would leave users more vulnerable to cybercrimes.

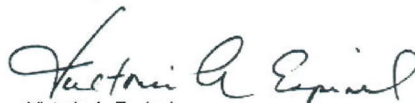
Calls for the weakening of encryption controls may also have international repercussions, which would further degrade many security measures protecting U.S. consumers. It is a reality that national borders do not limit threats to our citizens. Criminals, terrorists and other determined actors from around the world pose real and immediate threats to our safety and security. Other countries pay close attention to obligations that the U.S. government places on U.S. technology companies operating in the global marketplace. Internationally, calls for weakened encryption embolden some regimes to leverage similar policies, which put at risk fundamental human rights and can create artificial commercial disadvantages for U.S. companies and barriers to market access. We need to ensure that we can support any new standards adopted in the U.S. if other countries adopted the same standards. While we may have faith that U.S. law enforcement will responsibly exercise its discretion under any new authorities, we must be conscious that other countries may adopt the same standard and yet exercise their discretion quite differently.

Consumers use devices and cloud services to create and store personal data in a way that was hardly contemplated just a few years ago. Electronically stored information often is even more intimate and sensitive than physical records individuals would have stored in their homes or businesses at the turn of the century. Their expectation of privacy and security in digital information has, rightly, grown along with its prevalence.

Responsible technology providers want to assist law enforcement in legitimate investigations, in ways that are consistent with protecting consumer privacy and the security of the network and provide ample breathing room for innovation and meeting legitimate customers' needs.

We very much look forward to working with you, the law enforcement community and relevant stakeholders.

Sincerely,



Victoria A. Espinel
 President and CEO

The Hill

July 08, 2015, 06:30 am

Why encryption back doors threaten human rights

By Cynthia M. Wong

In recent years, pro-democracy and pro-human rights protesters from Egypt and Tunisia to Thailand and Hong Kong have used social media and mobile phones to organize and broadcast their message to fellow citizens and the world. But governments are ratcheting up their surveillance capabilities in response. Fear of heavy monitoring and the reprisals that can follow has led human rights activists to adopt services that support encryption. To them, encryption is a critical security tool to avoid being identified, arrested, harassed, or worse—merely for criticizing government policy.

The U.S. government supports Internet freedom abroad as a pillar of its human rights foreign policy. In recognition of the link between encryption and human rights, Congress has appropriated over \$125 million to the State Department and US AID since 2008 to promote Internet freedom, including through programs that develop encryption tools and train activists on how to use them.

But the FBI has embarked on an aggressive campaign to convince the public that encryption built into our digital tools should be weakened in the name of countering terrorism. Yet it has failed to recognize the broad, though unintended, harm such an approach would bring to human rights activists worldwide.

On June 3, Michael Steinbach, assistant director of the FBI's counterterrorism division, testified before the House Committee on Homeland Security that technology companies like Apple and Google should "prevent encryption above all else" because terrorists are increasingly using the companies' secured tools to shield communications and access to their activity is "going dark."

"Privacy, above all other things, including safety and freedom from terrorism, is not where we want to go," Steinbach said. FBI Director James Comey is likely to make the same argument before two hearings at the Senate Judiciary and Intelligence Committees on Wednesday.

Governments have a human rights obligation to investigate and prosecute crime and thwart terrorist attacks. But while strong encryption may limit some existing surveillance capabilities, these limitations are greatly offset by the explosion of new kinds of investigatory material enabled by the digital world, including location information and vast stores of metadata. It is also unlikely that limiting strong encryption in U.S. products would prevent bad actors from using it. Terrorists could merely shift to foreign alternatives.

Most jarring for human rights groups, however, is that the FBI's "going dark" narrative simply ignores the cost of undermining encryption to human rights activists around the world. For activists, this debate is just as much about their safety and freedom as about privacy.

All Internet users, including those most vulnerable, rely on the security practices of U.S. tech companies to protect them from abusive surveillance and cybercriminals. In December 2010, in the midst of the Tunisian uprisings, Facebook, a crucial platform for the activists, began receiving reports that Tunisian Facebook accounts had been compromised or deleted. Facebook soon discovered that the government had launched a large-scale attack to steal social media passwords of activists and journalists and access their private communications and contacts. So Facebook turned to encryption, enabling HTTPS, a secure communication protocol, automatically to thwart the attack in Tunisia.

Facebook now deploys HTTPS automatically for its 1.4 billion users. In 2014, Apple and Google announced they would go further and begin encrypting data stored on mobile devices used by activists worldwide, with even the companies unable to decrypt locally stored data. WhatsApp, a group chat application, is also rolling out end-to-end encryption for its 800 million users. These measures can help protect the safety of protest organizers in places like Hong Kong, Thailand, and the Middle East, along with millions of other, even if they may not realize it.

The FBI insists that they don't want a "back door" into secured services, but rather a requirement that companies design their services so they can still decrypt data with a lawful court order. But whatever label you use, the nearly universal view within the digital security community is that there is no technical solution that would allow the FBI to decrypt all communications, but wouldn't leave internet users exposed to actors (government and non-government) that would try to uncover that vulnerability for malicious purposes. Repressive regimes will exploit back doors to identify "troublemakers" and throw them in jail.

And if the FBI forces tech companies to weaken their security, then why wouldn't every other government demand the same, including those that equate dissent with terrorism. How comfortable would we be if Russia, China, and Saudi Arabia had back door access to Apple and Google devices?

Indeed, China has already started down this road in a counter-terrorism bill introduced earlier this year that would require firms to install back doors and disclose encryption keys. The US government would lack credibility to criticize these demands on behalf of US industry or on human rights grounds.

Strong encryption is a cornerstone of security in the digital age. It helps protect vulnerable human rights activists everywhere. Internet back doors make us all less safe. The FBI and Congress should not ignore these inconvenient facts, even in the name of fighting terror.

Wong is a senior Internet researcher at Human Rights Watch



Joel E. Abelow
District Attorney

OFFICE OF THE
DISTRICT ATTORNEY
COUNTY OF RENSSELAER
RENSSELAER COUNTY COURTHOUSE
TROY, NEW YORK 12180
(518) 270-4040



July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to lawful governmental searches.

Respectfully,


JOEL E. ABELOVE
District Attorney

JEA:cm

WASHINGTON
LEGISLATIVE OFFICE



July 7, 2015

RE: Senate Judiciary Committee Hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy"

Dear Chairman Grassley, Ranking Member Leahy, and Members of the Committee,

On behalf of the American Civil Liberties Union ("ACLU"), we submit this letter in connection with the July 8, 2015 hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy."

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

Over the last decade, the technology industry has made significant progress in protecting the security of Americans' private data, including electronic communications, through the expanded use of encryption technologies. This increased security has not only paved the way for enhanced technological and economic development, it has been critical to ensuring free expression and an open Internet.

Unfortunately, there have been calls by some to weaken – rather than strengthen – these encryption technologies. Specifically, the Director of the FBI, James Comey, has proposed modifications to the Communication Assistance to Law Enforcement Act (CALEA) that would gut strong protections for encryption technology passed by Congress in the 1990s.

While no formal proposal has yet been made public, the ACLU will oppose any proposal to (1) remove the protections for strong, backdoor-free encryption in CALEA; (2) require, request, or incentivize technology companies or communication providers to weaken encryption to enable greater government surveillance; or (3) incentivize, request, or mandate that technology companies retain information or metadata to circumvent encryption efforts.

Such proposals threaten privacy and place an improper burden on private entities to build the government's surveillance infrastructure, decrease cyber and national security, and are unnecessary given current law enforcement access to electronic information. Rather than weakening encryption, the

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6th FL.
WASHINGTON, DC 20005
T/202.544.1691
F/202.544.0738
WWW.ACLU.ORG

MICHAEL W. MACLEOD-BALL
ACTING DIRECTOR

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

OFFICERS AND DIRECTORS
SUSAN H. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

ACLU urges Congress and the Executive branch to take steps to expand the use of strong encryption, thereby protecting America's technology infrastructure from increasingly sophisticated cyber threats.

I. Recent encryption advances

In recent years, there have been several encryption advancements, enhancing security and privacy for millions of Americans. Such enhancements have provided increased protection for data that is stored on devices (such as smartphones), as well as data that is transmitted over the Internet.

For example, last year, Apple and Google announced advancements to provide greater protection for information stored on mobile devices. Both companies announced that their smartphone operating systems would, by default, protect data stored on devices with encryption.¹ Apple had for several years included such strong encryption technology in its mobile operating system; however, prior to last year, this method of encryption only protected a few categories of data stored on devices, such as email messages and data created by third party apps. Last year, Apple expanded the categories of data protected by industry-standard encryption to include photos, text messages, the address book, and several other forms of previously less-protected private data.² Similarly, last September Google announced that it would turn on disk encryption by default in the next version of its Android operating system. Subsequently, however, the company reversed course and announced that encryption would remain an opt-in feature due to reduction in speed suffered by many Android devices when encryption is used.³

Enhanced encryption has also been used to protect data as it is transmitted over the Internet. Over the past five years, this method of encryption has increasingly become an industry best practice. Major companies like Google, Facebook, and Twitter all use HTTPS and other transport encryption technologies to ensure that communication between their customers and their own servers are secure. The Washington Post also now encrypts parts of its website to provide greater protection to readers who visit the newspaper's website.⁴ Additionally, in just the past several months, the federal government has followed the technology industry's lead, and announced that all US government websites will use HTTPS encryption within two years.⁵ Similarly, 76 members of Congress use HTTPS encryption by default on their official websites.⁶

The adoption of these encryption technologies has yielded significant benefits to consumers,

¹ Craig Timberg, *Apple will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), 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*, WASH. POST (Sept. 18, 2014), <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/>.

² Cyrus Farivar, *Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot*, ARS TECHNICA (Sept. 18, 2014), <http://arstechnica.com/apple/2014/09/17/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/>.

³ Andrew Cunningham, *Google Quietly Backs Away from Encrypting New Lollipop Devices by Default*, ARS TECHNICA (Mar. 2, 2015), <http://arstechnica.com/gadgets/2015/03/02/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/>.

⁴ Andrea Peterson, *Washington Post starts to automatically encrypt part of Web site for visitors*, WASH. POST (June 20, 2015), <https://www.washingtonpost.com/blogs/the-switch/wp/2015/06/30/washington-post-starts-to-automatically-encrypt-part-of-web-site-for-visitors/>.

⁵ See *The HTTPS-Only Standard*, CHIEF INFORMATION OFFICER, <https://https.cio.gov/> (last visited Apr. 29, 2015) ("The American people expect government websites to be secure and their interactions with those websites to be private. Hypertext Transfer Protocol Secure (HTTPS) offers the strongest privacy protection available for public web connections with today's internet technology. The use of HTTPS reduces the risk of interception or modification of user interactions with government online services.")

⁶ *Tweet from Eric Mill*, TWITTER (Apr. 18, 2015), <https://twitter.com/konklone/status/589538454352097282>.

businesses, and government agencies, providing enhanced protection from the ever-increasing threat posed by cyber criminals and foreign governments.

II. Requiring, requesting, or incentivizing companies to build backdoors into their products threatens privacy and places an improper burden on private entities

When Congress passed CALEA in 1994, it disturbingly mandated that telephone companies rework their networks to be wiretap ready – expanding the government’s surveillance capabilities in unnecessary and unprecedented ways. Notwithstanding this, however, Congress explicitly limited the scope of CALEA to include specific language that explicitly protects companies that wish to deliver strong encryption without a backdoor for law enforcement to their customers.⁷ The legislative history of the act makes clear that it was the intent of Congress to protect the right to use encryption to safeguard information. Notwithstanding this, however, some government officials have sought changes that would remove the strong existing legal protections for encryption and grant the government the ability to compel that companies provide a surveillance backdoor into every electronic communication service, product, or app.

Imagine if the government required every home to be built with government-issued, Internet-connected cameras and microphones pre-installed. It would provide little reassurance to know that the government would have to get a search warrant to turn those cameras on. We understand intuitively that government surveillance of private activities would be much too easy, and a mandate of this type would be contrary to the protections in our constitution. Requiring a backdoor into any encrypted device is essentially the same; it guarantees that law enforcement has a view of the information of all Americans stored on mobile devices, regardless of whether there is cause to believe they have committed a crime.

At the same time, proposals like Director Comey’s are a dramatic expansion of a dangerous idea – that the private sector should be responsible for building the government’s surveillance infrastructure. Such proposals switch the burden for surveillance from the government to companies (and through them to their customers, the American people). Every customer would be paying to have surveillance capability pre-installed and ready to go at a moment’s notice—a government surveillance tax. Consumers would be forced to purchase fundamentally insecure products, with no option to allow them to protect their communications and stored data from cybersecurity threats. Not only does this represent an improper government intrusion, but, as a practical matter, the cost to law enforcement of surveillance has provided real privacy protection by forcing law enforcement to determine if investigations are practical and appropriate uses of resources. An expansion of the surveillance obligations mandated by CALEA would weaken this critical protection, and open the Internet to easy and pervasive government scrutiny.

Such pervasive government scrutiny also represents a threat to free expression and an open internet by eliminating the ability of individuals to communicate anonymously without fear of interception by the government. Opening all electronic communication to the possible government scrutiny would create a chilling effect on free speech, dissuading the public, journalists, or activists from engaging in protected, anonymous speech. Indeed, prominent journalists have reported that fear of government scrutiny and surveillance has made it more difficult to communicate with sources, leading to self-censoring and hindering reporting on critical issues, especially those related to national security where government secrecy and the

⁷ 47 USC § 1002(b)(3) states, “A telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.”

potential for the abuse of civil liberties are at their highest.⁸

Many of America's founders recognized this connection between the notion of free expression, anonymity, and cryptography. James Madison, for example, relied on ciphers both in a political capacity as Secretary of State and in his personal correspondence with Thomas Jefferson.⁹ Archives of Madison's encrypted letters show him discussing topics ranging from his unsuccessful courtships, to his personal political rivals, to his views on the need to raise taxes.¹⁰ James Lovell, a member of the Continental Congress, designed codes and ciphers that were used widely by members of the congress and their families. John and Abigail Adams famously used Lovell's ciphers to encrypt their personal correspondence.¹¹ Other early encryptors included George Washington, James Monroe, Alexander Hamilton, Aaron Burr, and John Jay, the first Chief Justice of the U.S. Supreme Court.¹²

U.S. foreign policy has also long supported the notion of anonymity and encryption, as a way of promoting free expression and an open internet around the world. As part of this policy, the U.S. government has supported encryption projects that provide secure communications to journalists and human rights activists who are often targeted by repressive regimes.¹³ For example, the U.S. government has helped to create tools that provide end-to-end encryption, which provide greater security to users.¹⁴ Director Comey's proposal is contrary this policy, and opens the door to repressive regimes demanding the same access to the technology products of their citizens, in order to target dissenters and suppress free expression.

III. Weakening encryption harms cyber and national security

Absent encryption, all networked communications are fundamentally insecure. Anyone with access to the servers that store our data or the networks that transmit it would be able to intercept

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

⁹ The James Madison Papers, *James Madison's Ciphers*, LIBRARY OF CONGRESS, http://memory.loc.gov/annmem/collections/madison_papers/mjmciphers.html (last visited Feb. 9, 2015).

¹⁰ Ralph E. Weber, *Masked Dispatches: Cryptograms and Cryptology in American History, 1775-1900* 83 (2011).

¹¹ David Kahn, *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* 181 (1996); The James Madison Papers, *supra* note 9; Weber, *supra* note 11, at 83.

¹² John A. Fraser, III, *The Use of Encrypted, Coded and Secret Communications Is an 'Ancient Liberty' Protected by the United States Constitution*, 2 Va. J.L. & Tech. 2 (1997), available at http://www.vjolt.net/vol2/issue/vol2_art2.html. In the century following the invention of the telegraph in 1844, forty-four new commercial ciphers were patented by Americans for both commercial and private uses. See Simon Singh, *The Code Book* 61, 79 (1999); Kahn, *supra* note 12, at 191.

¹³ See, e.g., About the Program, OPEN TECH. FUND, <https://www.opentechfund.org/about> (noting creation of the Open Technology Fund ("OTF") with U.S. government funding, and OTF's goal of securing access to the Internet with "encryption tools").

¹⁴ WhatsApp is adopting encryption mechanisms developed by Open Whisper Systems, which is funded by the Open Technology Fund. See *Projects*, OPEN TECH. FUND, <https://www.opentechfund.org/projects>; *Open Whisper Systems Partners with WhatsApp to Provide End-to-End Encryption*, OPEN WHISPER SYSTEMS BLOG (Nov. 18, 2014), <https://whispersystems.org/blog/whatsapp/>; see also White House, *National Security Strategy* 21 (Feb. 2015), http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf ("The United States is countering this trend by providing direct support for civil society and by advocating rollback of laws and regulations that undermine citizens' rights. We are also supporting technologies that expand access to information, enable freedom of expression, and connect civil society groups in this fight around the world.")

any communication, tamper with it, or delete it altogether. This not only jeopardizes freedom of expression and an open Internet, it also poses a threat to national and cybersecurity. Modern encryption is an answer to this threat. Properly implemented, it helps to protect against the increasingly frequent and costly cyberattacks waged by malicious hackers and oppressive regimes.

Technical experts, independent oversight boards, and governments have long acknowledged the value of encryption. For example, nearly two decades ago, the Internet Architecture Board ("IAB") and the Internet Engineering Steering Group ("IESG") wrote:

The IAB and IESG would like to encourage policies that allow ready access to uniform strong cryptographic technology for all Internet users in all countries. The Internet is becoming the predominant vehicle for electronic commerce and information exchange. It is essential that the support structure for these activities can be trusted.¹⁵

More recently, a review group hand-selected by President Obama echoed that view, recommending that the U.S. government take additional steps to promote security, by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.¹⁶

A proposal that would require companies to weaken existing technologies to facilitate law enforcement access is contrary to this sage advice. As prior efforts have shown, it is virtually impossible to build law enforcement access into products that cannot also be exploited by criminals, hackers, and malicious foreign government. As Stephanie Pell, a professor at the Army Cyber Institute at West Point, has observed:

Back doors create additional "attack surfaces," that is, code must be written to create the back door and the code must have unfettered access to communications content. **This means that when compromised, an encrypted communications system with a lawful interception back door is far more likely to result in the catastrophic loss of communications confidentiality than a system that never has access to the unencrypted communications of its users.**¹⁷ (emphasis added)

There are ample real-world examples that demonstrate the weaknesses inherent in "lawful interception" systems. For example, in 2004 and 2005, the mobile phones of dozens of members of the Greek government were spied upon by an unknown adversary who exploited a backdoor intended for law enforcement.¹⁸ And, in 2009, Google and Microsoft's law enforcement surveillance teams were compromised by Chinese hackers who gained access to a sensitive database with years'

¹⁵ IAB and IESG Statement on Cryptographic Tech. & the Internet (Aug. 1996), available at <https://tools.ietf.org/html/rfc1984>.

¹⁶ PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMM'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 22 (2013), available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

¹⁷ Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix—Doctrine to Follow*, 14 N.C. J. L. & TECH. 489 (2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262397.

¹⁸ Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE SPECTRUM (June 29, 2007), <http://spectrum.ieee.org/telecom/security/the-athens-affair>.

worth of information about the U.S. government's surveillance targets.¹⁹ In 2014, Microsoft's surveillance team was compromised again, this time by the Syrian Electronic Army.²⁰

If major technology companies like Microsoft and Google have not been able to secure their systems, smaller, less well-resourced companies likely remain even more vulnerable. These examples highlight that proposed expansions to CALEA would come at an unacceptable cost to our national and cyber security.

IV. An expansion to CALEA is unnecessary given the unprecedented access law enforcement has to information stored on electronic devices

In many respects, law enforcement authorities are now operating in a "golden age of surveillance."²¹ While technology promises to secure the content of our communications, it, disturbingly, has at the same time made our lives more transparent to law enforcement than ever before. With little effort, law enforcement agencies can now determine a suspect's exact location over a period of months, access records of all of his calls and electronic communications, and obtain every other digital fingerprint he leaves when interacting with technology.²² The increased use of encryption, whether to protect data transmitted over the Internet or in storage on mobile devices, leaves intact many of these existing investigative avenues, which in many cases themselves raise significant privacy concerns.

Additionally, as a practical matter, some of the information protected by disk encryption may still be accessible to law enforcement via alternative means. Much of the information stored on cell phones and other electronic devices are often backed up on the cloud. For example, Apple provides users with free cloud storage as a backup for photos, music, emails, text messages, and other information stored on cell phones, and such backups are enabled by default. Similarly, companies are increasingly relying on cloud computing services to store and backup information, as a way of enhancing security and efficiency. Thus, existing encryption technologies delivered to consumers by companies like Apple would not interfere with the law enforcement access to information stored in the cloud through appropriate administrative or judicial process.

Moreover, for those who do pose serious threats, governments often have other tools at their disposal. For example, where the NSA cannot crack the encryption used by its targets, it circumvents it in other ways.²³ The FBI has for more than a decade had the capability to hack into the computers

¹⁹ Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, WASH. POST (May 20, 2013), http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89e9-3be80951e767_story.html.

²⁰ Tom Warner, *Microsoft Confirms Syrian Electronic Army Hacked into Employee Email Accounts*, THE VERGE (Jan. 15, 2014, 4:35 PM) <http://www.theverge.com/2014/1/15/5312798/microsoft-email-accounts-hacked-syrian-electronic-army>.

²¹ Peter Swire, *'Going Dark' Versus a 'Golden Age for Surveillance'*, CTR. FOR DEM. & TECH. (Nov. 28, 2011), <https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance-%E2%80%99/>.

²² See *United States v. Pineda-Moreno*, No. 08-30385, at 11 (9th Cir. 2010) (denial for rehearing en banc), available at <http://cdn.ca9.uscourts.gov/datastore/opinions/2010/08/12/08-30385.pdf> ("When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use.")

²³ Tom Simonite, *NSA Leak Leaves Crypto-Math Intact but Highlights Known Workarounds*, MIT TECH. REV. (Sept. 9, 2013), <http://www.technologyreview.com/news/519171/nsa-leak-leaves-crypto-math-intact-but-highlights-known-workarounds/>.

and mobile devices of targets, allowing agents to capture data that might otherwise be protected by encryption and potentially raising additional privacy concerns.²⁴

Furthermore, there is little evidence that encryption has been a significant impediment in existing law enforcement investigations. For example, in 2014, the federal government only encountered three federal wiretaps as being encrypted. In only two of these cases were federal agencies unable to access the information sought.²⁵ Given existing investigative methods, as well as the plethora of electronic information readily available to law enforcement, expanding CALEA to further facilitate government surveillance is unnecessary and unwise.

V. Congress and the Executive branch should seek to expand the use of encryption technologies and secure our communications systems

Instead of weakening encryption efforts, Congress and the Executive branch should work to patch and remove the many existing vulnerabilities in our communications networks that can be exploited by nation states and cyber criminals. For example, our cellular communications networks use weak, decades-old encryption algorithms, and as a result, Americans calls and text messages can be intercepted by criminals and foreign governments. Indeed, according to ex-U.S. government officials, these vulnerabilities are being exploited by foreign intelligence services here in the Washington, D.C.²⁶ Similarly, numerous government systems, including the recently hacked Office of Personnel Management (OPM) systems, which exposed the sensitive information of millions of federal employees, reportedly do not use encryption to protect sensitive data.^{27 28}

At a time when cybersecurity threats are at the top of our national security agenda, the government should be promoting the use of strong encryption, not calling on companies to weaken their systems and leave them vulnerable to hackers. The expanded use of strong encryption would be much more effective at addressing threats to cyber security than an expansion to CALEA or the creation of new surveillance authorizes under the guise of enhancing cyber information sharing.

If you have any questions, please feel free to contact Legislative Counsel Neema Singh Guliani at 202-675-2322 or nguliani@aclu.org.

Sincerely,

²⁴ *FBI Sheds Light on 'Magic Lantern' PC Virus*, USA TODAY (Dec. 13, 2001),

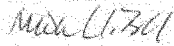
<http://usatoday30.usatoday.com/tech/news/2001/12/13/magic-lantern.htm>.

²⁵ UNITED STATES COURTS, WIRETAP REPORT 2014 (2014), available at <http://www.uscourts.gov/statistics-reports/wiretap-report-2014>.

²⁶ Jeff Stein, *New Eavesdropping Equipment Sucks All Data Off Your Phone*, NEWSWEEK (June 22, 2014, 8:27 AM), www.newsweek.com/2014/07/04/your-phone-just-got-sucked-255790.html; Ashkan Soltani & Craig Timberg, *Tech Firm Tries to Pull Back Curtain on Surveillance Efforts in Washington*, WASH. POST (Sept. 17, 2014), http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/18c1f590-3e81-11e4-b03f-de718edeb92f_story.html.

²⁷ Tal Kopan and David Perera, *Oversight Chairman: Fire Leaders of Hacked Agency*, POLITICO (June 16, 2015), <http://www.politico.com/story/2015/06/katherine-archuleta-opm-computer-hack-house-119067.html>.

²⁸ Prior to the hack, the OPM Office of Inspector General had noted that several OPM systems lacked appropriate encryption. See Office of the Inspector General United States Office of Personnel Management Statement (June 24, 2015), available at <https://oversight.house.gov/wp-content/uploads/2015/06/McFarland-OPM-OIG-Statement-6-24-Data-Breach-II.pdf>.



Michael W. Macleod-Ball
Acting Director
American Civil Liberties Union
915 15th St., NW, Washington, DC 20005



Neema Singh Gulliani
Legislative Counsel
American Civil Liberties Union
915 15th St., NW, Washington, DC 20005
202.675.2322
ngulliani@aclu.org



COUNTY OF COOK
OFFICE OF THE STATE'S ATTORNEY

ANITA ALVAREZ
STATE'S ATTORNEY

69 WEST WASHINGTON, SUITE 3200
CHICAGO, ILLINOIS 60602
(312) 603-1880

July 6, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to lawful governmental searches.

Sincerely,


Anita Alvarez
State's Attorney of Cook County

BELINDA HILL
FIRST ASSISTANT



CRIMINAL JUSTICE CENTER
1201 FRANKLIN, SUITE 600
HOUSTON, TEXAS 77002-1901

**DEVON ANDERSON
DISTRICT ATTORNEY
HARRIS COUNTY, TEXAS**

Honorable Chuck Grassley
Chairman, Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Comments for July 8, 2015 Hearing – “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy”

Dear Mr. Chairman:

My name is Tammy Thomas. I am an assistant district attorney employed by Devon Anderson, the District Attorney of Harris County, Texas. This has been my vocation for the last 25 years. I am currently the chief of the District Attorney’s Major Offender Division, handling some of the most complex and difficult cases in the criminal justice system.

In writing to you and your Committee today, I am joining New York County District Attorney Cyrus R. Vance, Jr. and other prosecutors across the country in expressing our concerns about the efforts of Apple and Google to make their smartphones and other “smart” devices (such as the MacBook Pro) impervious to search warrants and similar judicial orders.

As a mother, neighbor and citizen with many family members in private life, I fully understand, respect, and value individual privacy rights. To that end, I want to emphasize that we are not proposing that law enforcement investigators be given access to information protected by encryption without a warrant based on probable cause. We recognize that the Fourth Amendment’s requirements apply to searches of smartphones.

That said, there *are* times in a law-abiding society when probable cause justifies the search of a smartphone. The impervious encryption proposed by Apple and Google defeats such reasonable searches and seizures.

As a career prosecutor who has investigated and prosecuted truly dangerous people committing terrible crimes, I know too well the costs that encryption has already imposed, not only to the ability of law enforcement to properly investigate cases but also on public safety. By way of illustration, please consider the following true-life cases:

- *State of Texas v. Ali Awad Mahmoud Irsan, et al.* – The main target, Ali Awad Mahmoud Irsan, has been described as a Jordanian-Muslim extremist “honor killer” who is currently under indictment for murdering two individuals in 2012 and who, by his own admission, is responsible for killing a third individual for similar motives in another county in Texas in 1999.

Hon. Chuck Grassley
 July 8, 2015
 Page 2.

Three other family members are charged with felonies in connection with aspects of these murders, including Ali Irsan's daughter, Nadia. In connection with this investigation, federal authorities obtained a search warrant for Nadia's MacBook laptop, which was intercepted on a trip back into the United States from Jordan. She refused, however, to provide the password and federal authorities have not yet broken the encryption to access the information.

Based on the known facts related to Nadia's contribution to Irsan's crimes, plus her own commentary about her MacBook computer, we believe that the information necessary to hold her responsible as a party to Irsan's murders is on that computer hard-drive and is being protected by the encryption.

- *State of Texas v. Justin Braswell* – This is another case that I personally investigated. Braswell was charged with indecency with a child for fondling his own biological daughter who, at the time, was under the age of twelve.

Braswell was a free-lance photographer who specialized in photographing little girls at cheerleading competitions. He also had a MacBook Pro with an enormous amount of stored information on it (3 terabytes). We know he had child pornography on the computer because, when the police executed the search warrant at his house in a rural area in another county, he had gone to bed and left the MacBook Pro open to some images of child pornography that we were able to recover.

He was charged federally for the images he happened to have left open on his computer. In federal custody, he later confided to another inmate that he hoped we would not access the computer because he had images of himself committing a crime against a child who had come over to spend the night with his girlfriend's daughter.

Based on this information, we obtained a search warrant to review the contents of the MacBook Pro. It is my understanding that, after six years, the federal authorities are still trying to break the encryption on it. To this day, we still do not know who the child he was referring to is and the extent of this pedophile's criminal activity. Frustratingly, despite my best efforts to keep him in prison, he is probably close to release on parole at this point.

These cases illustrate the dangerous vulnerability created by impervious encryption and by granting what Google and Apple really want: blanket immunity from their responsibility to comply with search warrants.

Hon. Chuck Grassley
 July 8, 2015
 Page 2.

It is the warrant based on probable cause that is central to our system of checks and balances on unfair government intrusion upon individual privacy rights in virtually every other context. I sincerely hope that we have not reached a day and age in which a corporation such as Apple or Google (who ironically have no apparent interest in discussing safeguards for private citizens against their own searching and compiling of data stored on their own servers for their own profit) would be given what would amount to legal immunity from a legally valid search warrant based on probable cause and signed by a neutral and detached magistrate.

Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. If this is an arms race between criminals and law enforcement, the criminals will have won because this proposal by Apple and Google only protects criminals' privacy and creates the worst possible scenario for law enforcement and, more importantly, the victims we are trying to protect.

Sincerely,



TAMMY J. THOMAS
 Assistant District Attorney
 Chief, Major Offenders and Organized Crime Division
 (713) 755-5800



JEAN PETERS BAKER
Jackson County Prosecuting Attorney

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

**Re: Going Dark: Encryption, Technology, and the Balance Between
Public Safety and Privacy**

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

As a private citizen, but also as a prosecutor, I appreciate the tremendous value of privacy, yet the high cost that Apple's and Google's actions will have on state and local law enforcement and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Jean Peters Baker
Jean Peters Baker
Prosecutor for Jackson County
Kansas City, Missouri





OFFICE OF THE
DISTRICT ATTORNEY
BROOKS T. BAKER

3 EAST PULTENEY SQUARE
BATH, NEW YORK 14810

TELEPHONE: (607) 664-2270
FACSIMILE: (607) 664-2159
WWW.STEUBENCONY.ORG

July 14, 2015

ASSISTANT
DISTRICT
ATTORNEYS

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

PARALEGALS

- ANNE M. ROVITO
- VERONICA L. STEEL
- SHANA M. ROBERTSON

INVESTIGATORS

- NOEL P. TERWILLIGER
- DANIEL T. STUTZMAN

Respectfully,

Brooks T. Baker
District Attorney



Office of the
District Attorney
County of Rockland

THOMAS P. ZUGIBE
DISTRICT ATTORNEY

July 15, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

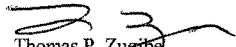
This Committee has heard from many law enforcement experts who have passionately conveyed the message from various law enforcement agencies nationwide: Going Dark is a real danger to ordinary Americans due to the limits it places on our ability to fight crime. I wish to lend my voice to those who have tried to make this Committee understand the dangers that will result from your allowing encryption technology to become the standard on electronic devices.

Never before in our history has there been such a threat to law enforcement's ability to collect and analyze evidence. I speak not of evidence beyond our legal ability to obtain. The police and prosecutors are well aware that the trade-off of a vibrant democracy and our Constitutional protections remains that some offenders, even the worst ones, go free because of the limits on our power to collect and utilize evidence.

Our concern is far greater with regard to going dark because the current private sector encryption will prevent us from discharging our duties by limiting our ability to collect vital evidence **even when the law allows us to access the information**. Allowing criminals to literally hide behind their digitally encrypted walls will stymie legitimate and fully legal efforts to obtain information to which we are otherwise entitled. It is small wonder that law enforcement walks in lockstep to support legislation that will allow a "back door" to ensure that criminals are brought to justice.

For some reason, there are those who roll their eyes when we speak of the effect this encryption will have on our cases. But this Committee should be well aware: It is a certainty that allowing private encryption will prevent prosecutions of untold numbers of murderers, rapists and child molesters, as well as numerous white collar criminals. It is a trade off this nation should not and need not make. Only you can stop it.

Very truly yours,


Thomas P. Zugibe
District Attorney



**Office of the
Special Narcotics Prosecutor
for the City of New York**

Bridget G. Brennan, Special Narcotics Prosecutor

80 CENTRE STREET, SIXTH FLOOR
NEW YORK, NY 10013
212-815-0102, OFFICE
212-815-0144, FAX

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

**Re: Going Dark: Encryption, Technology, and the Balance
Between Public Safety and Privacy**

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Bridget G. Brennan
Special Narcotics Prosecutor
for the City of New York



Richard A. Brown
District Attorney

DISTRICT ATTORNEY
QUEENS COUNTY
125-01 QUEENS BOULEVARD
KEW GARDENS, NEW YORK 11415-1568

(718) 286-6000
www.queensda.org

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

**Re: Going Dark: Encryption, Technology and the
Balance Between Public Safety and Privacy**

Dear Senators:

I write to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I understand and appreciate the importance and tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement and on crime victims across the country must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement then crimes will go unsolved, criminals will go free, and the safety of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment to the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Richard A. Brown
District Attorney



JON E. BUDELMANN
DISTRICT ATTORNEY

OFFICE OF THE
DISTRICT ATTORNEY
CAYUGA COUNTY

95 GENESEE STREET, FIRST FLOOR
AUBURN, NEW YORK 13021
(315) 253-1391 • Fax (315) 253-1521
E-MAIL: cayugada@cayugacounty.us
July 14, 2015



CHRISTOPHER T. VALDINA
CHIEF ASSISTANT
DIANE M. ADSIT
HEATHER M. DE STEFANO
NATHAN J. GARLAND
CARL J. ROSENKRANZ
JEFFREY A. DOMACHOWSKI
BRIAN T. LEEDS
ASSISTANT DISTRICT ATTORNEYS

UNITED STATES SENATE
Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption Technology/Privacy
versus Public Safety/Court Ordered Discovery

Dear Senators:

I am writing to express my concern that Apple and Google are working to make their smartphones impervious to search warrants and similar judicially ordered discovery based upon probable cause to believe evidence of a crime exists on such devices.

I fully believe in our Citizens' right to privacy, to be free from identity theft, particularly at this time when we use smartphones to complete all sorts of financial transactions. However, the terrible cost that the planned/impending actions on the part of Apple, Google (and others) will have on Federal, State and Local Law Enforcement (not to mention the impacted crime victims who will not receive justice) across the entire country must also be considered.

Putting it simply, if those committing crimes can hide the evidence on their smartphones, and now that evidence is forever beyond the reach of any law enforcement, then not only will it get easier for criminals to conduct their illicit conduct, but crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the technologically race between criminals and law enforcement, the criminals will have won a huge and enduring victory.

The Fourth Amendment of the United States Constitution, and similar provisions in the various State Constitutions already protect citizens' privacy from unwarranted invasions. As you know the rights provided already require that a showing of probable cause be made before an impartial magistrate before any warrants may be issued by judges-- not prosecutors. All this before smartphones may be searched at all. Such warrants, which have been instrumental in solving a d prosecuting many serious crimes, will become a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful*, sanctioned governmental searches.

Respectfully,

JON E. BUDELMANN
Cayuga County District Attorney

We Do Not Accept Service By Facsimile



Office of the Orleans Parish District Attorney

Leon A. Cannizzaro, Jr.
DISTRICT ATTORNEY

July 15, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between
Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

With kindest regards, I remain

Cordially,



Leon A. Cannizzaro, Jr.



The Commonwealth of Massachusetts

DISTRICT ATTORNEY OF SUFFOLK COUNTY
DANIEL F. CONLEY

One Bulfinch Place, Suite 300
Boston, MA 02114-2921

Telephone: (617) 619-4000
Fax: (617) 619-4210

July 6, 2015

The Honorable Charles Grassley
Chair, Senate Judiciary Committee
135 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Patrick Leahy, Judiciary Committee
Ranking Member, Senate Judiciary Committee
437 Russell Senate Office Building
Washington, D.C. 20510

Dear Chairman Grassley and Ranking Member Leahy:

I am writing in advance of the Judiciary Committee hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy" to share my thoughts and concerns on this critical and difficult issue. Striking a proper balance between the greater public safety and individual privacy rights is no easy task. I don't pretend to have all of the answers but of one thing I am certain: determining how these important interests are properly balanced should not be left to unelected and unaccountable corporations but reserved to the collective wisdom of Congress and the Courts, as has been the case for hundreds of years.

I had the privilege to testify in April on this same issue before the Committee on Oversight and Government Reform Subcommittee on Information Technology and pointed out that Apple's new iOS 8 operating system and Google's new operating systems have been intentionally designed to prevent any law enforcement access, even if that access is authorized in a warrant by an independent judge. The impact of their decision has fallen disproportionately hard on state and local law enforcement who rely on evidence stored on handheld electronic devices in a large and still growing number of cases.

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.

Apple and Google, it would seem, have created this response at least in part to ease foreign and domestic customer concerns over protecting the private information stored on cell phones. The irony is that Apple and Google's actions have had a disproportionately negative impact on state



and local law enforcement agencies such as mine, who must have lawful access to certain data in order to solve crimes, serve victims and hold offenders accountable. Offices like mine obtain this evidence through means that are fair, ethical, and legal.

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. Denying law enforcement legal access to any evidence stored on a smartphone simply because it is a smart phone makes no more sense today than if law enforcement were denied warrant-approved access to safes or car trunks years ago.

Just to be crystal clear, state and local enforcement agencies like mine 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 private companies, including Google, and had long been a practice for Apple as well. 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.

When I made this same point in April, one of the committee members took great offense, telling me that Apple and Google did not possess the "coercive power" of agencies like mine. But agencies like mine are led by democratically elected officials who are operating within the confines of the law. Further, Apple and Google operating systems account for over 96 percent of all operating systems worldwide. While their "power" is certainly different from government agencies, they have incredible reach and control over the marketplace that cannot be overlooked, downplayed or diminished.

Apple and Google's new operating systems have made legitimate and necessary 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.

The practical implications of what Apple and Google are doing cannot be diminished or dismissed, either. Consider, for example, the reprehensible practice called "upskirting", where men who use their phones to surreptitiously take pictures and videos up the skirts of females. Under Massachusetts law, even having a witness testify that someone held a phone beneath the

skirt of another is insufficient evidence of the crime; a picture had to have been taken. If law enforcement can't access the phone, then the offense is not chargeable. Or consider the Boston area teacher who is now serving a 45-year federal prison sentence. He was found to be not only trading child pornography but videotaping himself raping children. If law enforcement had not been able to obtain the evidence contained on his phone however, that evidence would have been beyond our reach and he would have been above the law. Think about the impact of Apple and Google's actions on human trafficking and the commercial sexual exploitation of children. Human trafficking has moved off of 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. Now, I don't believe that Apple or Google set out to design systems that would protect "upskirters," help rapists escape justice, or 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.

Those who defend these systems downplay these stories as merely anecdotal and have even said that law enforcement can't point to a single case where an investigation has been held up due to encryption technology. This is untrue. As of May, my office was in possession of 139 phones, lawfully seized as evidence, pursuant to a judicial order. Of these, 39 were operating on the Apple and Google systems and in 10 of these cases, all active, defendants have refused to share their passwords. These cases, 2 of which are homicides and 1 a sexual assault, are held up.

These numbers are expected to increase rapidly. Already, 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 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.

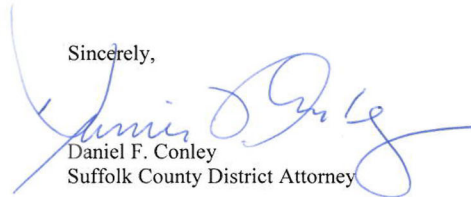
In addition, I can think of no other example of a tool or technology that is specifically designed and allowed to exist completely beyond the legitimate reach of law enforcement, our courts, our Congress, and thus, the people. Not safe deposit boxes, not telephones, not automobiles, not homes. Even if 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. Apple and Google and their defenders argue that by creating any means of access for anyone that the entire system becomes less secure. But what lock was ever created that didn't have a key?

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.

Just recently, the trial of one of the Boston Marathon bombers concluded. The bombers actions 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 ask that Congress and the courts - and not unelected, unaccountable corporations – reserve to themselves the right to strike the proper balance between public safety and privacy and that the voices of state and local law enforcement officials be given their proper due because it is here where the impact of these operating systems will have their greatest and gravest impacts.

Sincerely,

A handwritten signature in blue ink, appearing to read "Daniel F. Conley", is written over a horizontal line. The signature is fluid and cursive, with a large loop at the end.

Daniel F. Conley
Suffolk County District Attorney

July 7, 2015

Hon. Charles Grassley, Chair
Judiciary Committee
United States Senate
135 Hart Senate Office Building
Washington, D.C. 20510

Hon. Patrick Leahy, Ranking Member
Judiciary Committee
United States Senate
437 Russell Senate Office Building
Washington, D.C. 20510

RE: Smartphone encryption and the impact on crime victims

Dear Chairman Grassley and Ranking Member Leahy:

We represent a diverse group of organizations that advocate for crime victims. We are survivors of sexual assault, domestic violence and child abuse, victims of identity theft, and families of innocent men, women and children victimized by crime. We work to advance public policies which aid law enforcement in the resolution of unresolved crimes, and the prevention of future ones.

We believe strongly that smartphone encryption policies recently introduced by America's leading technology companies unnecessarily hinder the critical investigative operations of state and local law enforcement, while unintentionally protecting criminals. Today we ask you, our federal lawmakers, to determine the proper balance between the purported benefits of these new encryption standards, and the need for state and local law enforcement to prosecute and prevent crime.

We stand ready to assist the Committee in any way we can.

Christopher Bromson
Assistant Director, Crime Victims Treatment Center
Co-Chair, Downstate Coalition for Crime Victims Legislative Committee

Christine Fowley
Chair, NYC Sexual Violence Direct Service Collaborative
Supervisor, Crime Victims Treatment Center

Hon. Judy Harris Kluger, Executive Director
Sanctuary for Families

Stephanie Nilva, Executive Director
Day One New York

Richard Ortiz, Forensic Nurse Coordinator
Richmond University Medical Center

Rosemonde Pierre-Louis, Commissioner
NYC Mayor's Office to Combat Domestic Violence

Danny Salim, Anti-Violence Program Manager
Arab American Family Support Center

Verena Salvi, Social Worker
New York Presbyterian Hospital Domestic and Other Violence Emergencies (DOVE) Program

Susan Xenarios
Director, Crime Victims Treatment Center
Co-Chair, Downstate Coalition for Crime Victims



ANDREW M. CUOMO
Governor

JOSEPH A. D'AMICO
Superintendent

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

As Superintendent of the New York State Police, I am writing to express my concern about the practice of manufacturing cell phones that cannot be unlocked by the manufacturer or service provider, even when appropriately provided with a search warrant issued by a court of competent jurisdiction.

While both state and federal courts recognize that a person has a right to privacy in the contents of his or her cell phone, they have also held that a search of that device is reasonable under the Fourth Amendment when the search is authorized by a warrant. The practice of manufacturing devices that cannot be opened by the manufacturer or service provider creates an opportunity for criminals to use these devices to conduct unlawful business and store digital evidence of criminal behavior. As a result, a criminal can be confident that evidence of his or her criminal behavior will never be discovered by police, even when a neutral magistrate has made a probable cause determination and has issued a search warrant directing the police to search the device.

Allowing this manufacturing process to continue will thwart legitimate investigative techniques and will impact those investigations that often utilize the use of cell phones, including terrorism, drug trafficking and the sexual abuse of children. Therefore, I fully support the efforts by the District Attorneys of New York State to ensure that cell phones sold or leased in New York State be capable of being decrypted and unlocked in the event that a judge has ordered the police to search the phone pursuant to a search warrant.

Accordingly, I join with the District Attorneys in New York State in their efforts to ensure that manufacturers take the necessary steps to enable law enforcement to conduct searches of these devices whenever directed by a judicial warrant.

Very truly yours,

Joseph A. D'Amico
Superintendent

OFFICE OF THE
SULLIVAN COUNTY DISTRICT ATTORNEY

District Attorney
James R. Farrell



Office (845) 794-3344
Fax (845) 807-0649

Lawrence H. Cooke Courthouse
414 Broadway
Monticello, New York 12701

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology & the Balance Between Public Safety & Privacy

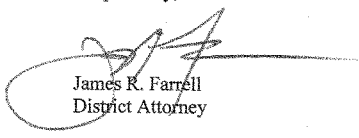
Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,


James R. Farrell
District Attorney



COUNTY OF MONTGOMERY
COURTHOUSE
P.O. BOX 311
NORRISTOWN, PENNSYLVANIA
19404-0311

OFFICE OF THE DISTRICT ATTORNEY

RISA VETRI FERMAN
DISTRICT ATTORNEY

KEVIN R. STEELE
FIRST ASSISTANT DISTRICT ATTORNEY

SAMUEL J. GALLEN
CHIEF COUNTY DETECTIVE

JESSE S. KING
CHIEF OF STAFF

DISTRICT ATTORNEY'S OFFICE
DISTRICT ATTORNEY'S FAX
COUNTY DETECTIVE BUREAU

(610) 278-3090
(610) 278-3095
(610) 278-3368

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

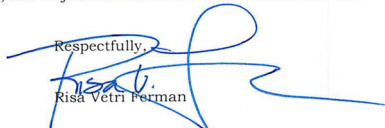
I write to weigh in on the ongoing dialogue about the balance between privacy and powerful technology. Recent efforts by Google and Apple have made their devices, including smartphones and tablets, impervious to lawful search warrants and similar judicial orders.

There is no doubt that privacy rights are critically important. The Constitution protects citizens from unreasonable searches and seizures at the hands of the Government, but has long expressly allowed for government access to a person's personal "papers and effects" in appropriate and reasonable circumstances, where probable cause has been presented to a neutral magistrate or judge. This is the same standard that allows law enforcement to search one's house, car, and other areas of privacy. However, the technology industry intends to remove the reasonable standard all together as it implements technology that will make its devices entirely impenetrable to not only law enforcement, but to the companies themselves. This would be the case no matter how reasonable, or even emergent, access to data on these devices may be.

The unfortunate fact is that criminals and terrorists are well aware that they can find refuge in the encryption systems of these companies. Despite claims that the intention is to satisfy consumer demands to protect private data, this safe-haven is being marketed to those people most likely to benefit from it – those looking to conceal their unlawful actions. To be sure, we need look no further than Apple's own website, which boasts, "we wouldn't be able to comply with a wiretap order even if we wanted to." What purpose does such a statement serve, but for the promotion of asylum for the criminal or terrorist element? Furthermore, what is to stop other technology companies from following suit, encrypting all desktop and laptop computers and limiting lawful investigative efforts in those areas?

In essence, Apple and Google are promoting impunity for criminals communicating on their smartphones, diminished public safety, and unjust results for the victims of crime. This is simply too high a price to pay.

Respectfully,


Risa Vetri Ferman



**DISTRICT ATTORNEY
WILLIAM J. FITZPATRICK**

County of Onondaga
Criminal Courthouse, 4th Floor
505 South State Street
Syracuse, New York 13202
315-435-2470
Fax: 315-435-3969

July 2, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: **Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy**

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Sincerely,

WILLIAM J. FITZPATRICK
DISTRICT ATTORNEY

PRESIDENT-ELECT NATIONAL DISTRICT ATTORNEYS ASSOCIATION



OFFICE OF THE HENNEPIN COUNTY ATTORNEY
MICHAEL O. FREEMAN COUNTY ATTORNEY

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: **Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy**

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

MICHAEL O. FREEMAN
HENNEPIN COUNTY ATTORNEY



Megan P. Dadd, ADA
David G. Mashewski, ADA
Jannine Phillips, Victim Services

YATES COUNTY DISTRICT ATTORNEY
VALERIE G. GARDNER

415 Liberty Street, Suite 272
Penn Yan, New York 14527
Tel: (315) 536-5550
Fax: (315) 536-5556



Secretary to DA
Molly K. Linehan
Service by Fax Not Accepted

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

RE: **Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy**

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished.

By way of example, my office is currently prosecuting a mother and her boyfriend for taking and distributing indecent photos of a fifteen year old female. These photos were taken, without the child's knowledge, while she was bathing and during medicated sleep. The evidence retrieved by lawful warrant from the cell phones of the mother and her boyfriend was essential in enabling our courts to protect this child from further victimization, and has brought these individuals to court to answer for their actions. Without this evidence, none of this would have been possible.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Please help us protect our children and ensure the safety of our communities.

Respectfully,

Valerie G. Gardner
Yates County District Attorney

THE DISTRICT ATTORNEY OF DUTCHESS COUNTY

236 MAIN STREET
POUGHKEEPSIE, N.Y. 12601
(845) 486-2300
FAX (845) 486-2324

WILLIAM V. GRADY
DISTRICT ATTORNEY

BRIDGET R. STELLER
Chief Assistant District Attorney

BUREAU CHIEFS
Edward F. Whitesell
Marjorie J. Smith
Frank F. Chase
Matthew A. Weishaupt
Edward T. McLoughlin

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

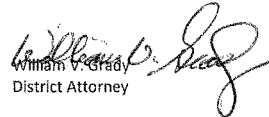
Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Very truly yours,


William V. Grady
District Attorney

WVG/gmb



**Justice Center for the
Protection of People
with Special Needs**

ANDREW M. CUOMO
Governor

JEFF WISE
Executive Director

July 16, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between
Public Safety and Privacy

Dear Senators:

I stand with my colleagues in the New York State District Attorney's Association in expressing my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to lawful governmental searches.

Respectfully,

Patricia Gunning
Special Prosecutor
NYS Justice Center for the Protection of
People with Special Needs
(518) 549-0367
(518) 795-7730



SUSAN HAWK
CRIMINAL DISTRICT ATTORNEY
DALLAS COUNTY, TEXAS

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

A handwritten signature in blue ink, appearing to read "Susan Hawk", is written over a horizontal line.

Susan Hawk
Dallas County District Attorney



KAREN A. HEGGEN
DISTRICT ATTORNEY

OFFICE OF THE
DISTRICT ATTORNEY
OF SARATOGA COUNTY

MUNICIPAL CENTER • 25 WEST HIGH STREET
BALLSTON SPA, NEW YORK 12020
(518) 885-2263
FAX (518) 884-8627



July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

As the District Attorney of a County of approximately 215,000 people, it is imperative to our successful prosecution of cases to have access to the 21st century technology that the criminals use daily in their illegal enterprises. While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Karen A. Heggen
District Attorney

KAH:pah

cc: Ben Rosenberg, Asst. Dist. Atty., Manhattan DA's Office
Senator Charles Schumer
Senator Kristin Gillibrand



ASSOCIATION of PROSECUTING ATTORNEYS

BOARD OF DIRECTORS

CHAIRMAN

Paul L. Howard
District Attorney
Fulton County, GA

VICE-CHAIRMAN

R. Seth Williams
District Attorney
Philadelphia, PA

SECRETARY

Thomas Carr
City Attorney
Boulder County, CO

Mike Feurer

City Attorney
Los Angeles, CA

Risa Vetri Ferman

District Attorney
Montgomery County, PA

John T. Chisholm

District Attorney
Milwaukee County, WI

Dan Satterberg

Prosecuting Attorney
King County, WA

Rod Underhill

District Attorney
Multnomah County, OR

Cyrus R. Vance, Jr.

District Attorney
New York County, NY

APA OFFICERS

PRESIDENT

David LaBahn
Chief Executive Officer

VICE-PRESIDENT

Steven Jansen
Chief Operating Officer

TREASURER

Steven Naugle
Chief Financial Officer

July 7, 2015

Senator Chuck Grassley
135 Hart Senate Office Building
Washington, DC 20510

Senator Patrick Leahy
435 Russell Senate Building
Washington, DC 20510

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Chairman Grassley, Ranking Member Leahy and Members of the
Committee:

The Association of Prosecuting Attorneys (APA) is a private non-profit
whose mission is to support and enhance the effectiveness of prosecutors
in their efforts to create safer communities. We are the only national
organization to include and support all prosecutors, including both
appointed and elected prosecutors, as well as their deputies and assistants,
whether they work as city attorneys, city prosecutors, district attorneys,
state's attorneys, attorneys general or US attorneys.

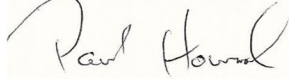
On behalf of APA and in my individual capacity as the District Attorney
from Atlanta, I am writing to express my concern about the efforts that
Apple and Google have made to make their smartphones impervious to
search warrants and similar lawfully sought and approved judicial orders.

As a career prosecutor, I fully understand, support and appreciate the
tremendous value of privacy, the terrible cost that Apple's and Google's
actions will have on state and local law enforcement, and on crime victims
across the country, must also be considered. Simply put, if criminal
wrongdoers can hide the evidence of their crimes on their smartphones,
and if that evidence is forever beyond the reach of law enforcement and
the courts, then crimes will go unsolved, criminals will go free, and the
safety of all of our citizens will be diminished. In the "arms race"
between criminals and law enforcement, the criminals will have won.

Last year, the U.S. Supreme Court ruled in *Riley* that a search warrant is required to search an individual's cell phone. As a legal association, we have advised the investigating agencies to seek search warrants consistent with the Court's decision and have no issue that this is the law of the land. However, when industry chooses to put products into the stream of commerce which will make these warrants meaningless, we believe the Congress has jurisdiction and should act to protect our great nation's safety.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "Paul Howard", with a stylized flourish at the end.

Paul L. Howard
Chairman of the Board and Fulton County District Attorney



JEFFERSON COUNTY DISTRICT ATTORNEY'S OFFICE

Jefferson County Office Building, Seventh Floor
175 Arsenal Street
Watertown, New York 13601
Telephone: (315) 785-3053
Facsimile: (315) 785-3371

Chief Assistant
Kristyna S. Mills

Senior Assistants
Patricia Dziuba
Nicole Kyle

District Attorney
Cindy F. Intschert

**Assistant
District Attorneys**
Rodney Kyle
Walter Jeram
Harmony Healy
Sean Sterling
George Shaffer, III
Christina Curri

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

A balance can be struck between an individual's right to privacy and public safety. The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. Those provisions require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. A search warrant is a lawful order of a court. We have sought and obtained warrants permitting the examination of cell phones in past criminal investigations involving murder, sexual assault, child pornography and other heinous crimes. Unfortunately, those warrants will be a nullity in the future if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Cindy F. Intschert
Jefferson County District Attorney



2929 NORTH FRONT STREET
HARRISBURG, PA 17110
(717) 238-5416
FAX (717) 231-3912

FOUNDED 1912

PENNSYLVANIA DISTRICT ATTORNEYS ASSOCIATION

PRESIDENT

D. PETER JOHNSON
Union County

July 7, 2015

VICE PRESIDENT

RISA VETRI FERMAN
Montgomery County

Committee on the Judiciary
United States Senate
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

SECRETARY-TREASURER

DAVID J. ARNOLD, JR.
Lebanon County

Via Electronic Mail

IMMEDIATE-PAST PRESIDENT

DAVID J. FREED
Cumberland County

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

EXECUTIVE COMMITTEE

JOHN T. ADAMS
Berks County

I write to express the concern held by Pennsylvania's prosecutors about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

RICHARD A. GOLDINGER
Butler County

While we fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

DAVID W. HECKLER
Bucks County

ANDREW J. JARBOLA
Lackawanna County

RAYMOND J. TONKIN
Pike County

MICHAEL PIECUCH
Snyder County

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

LEGISLATIVE CHAIR

R. SETH WILLIAMS
Philadelphia County

CHAIRMAN OF APPEALS

STEPHEN A. ZAPPALA, JR.
Allegheny County

If the Pennsylvania District Attorneys Association can be of further assistance in this matter please let us know. Thank you for your continuing efforts to promote public safety.

COMMUNICATIONS CHAIR

EDWARD M. MARSICO, JR.
Dauphin County

Respectfully,

EXECUTIVE DIRECTOR

RICHARD W. LONG

D. Peter Johnson
President

OFFICE OF THE DISTRICT ATTORNEY
WASHINGTON COUNTY – STATE OF NEW YORK



383 Broadway – Building C
Fort Edward, New York 12828
Telephone: (518) 746-2525
Fax: (518) 746-2568

J. Anthony Jordan
District Attorney

Christian P. Morris
First Assistant

Devin J. Anderson
Sara E. Fischer
Brandon P. Rathbun
Assistant District Attorneys

Paul R. Frettoloso
Investigator

Rebecca A. Evansky
Laura C. Taylor
Crime Victim Specialists

July 15, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

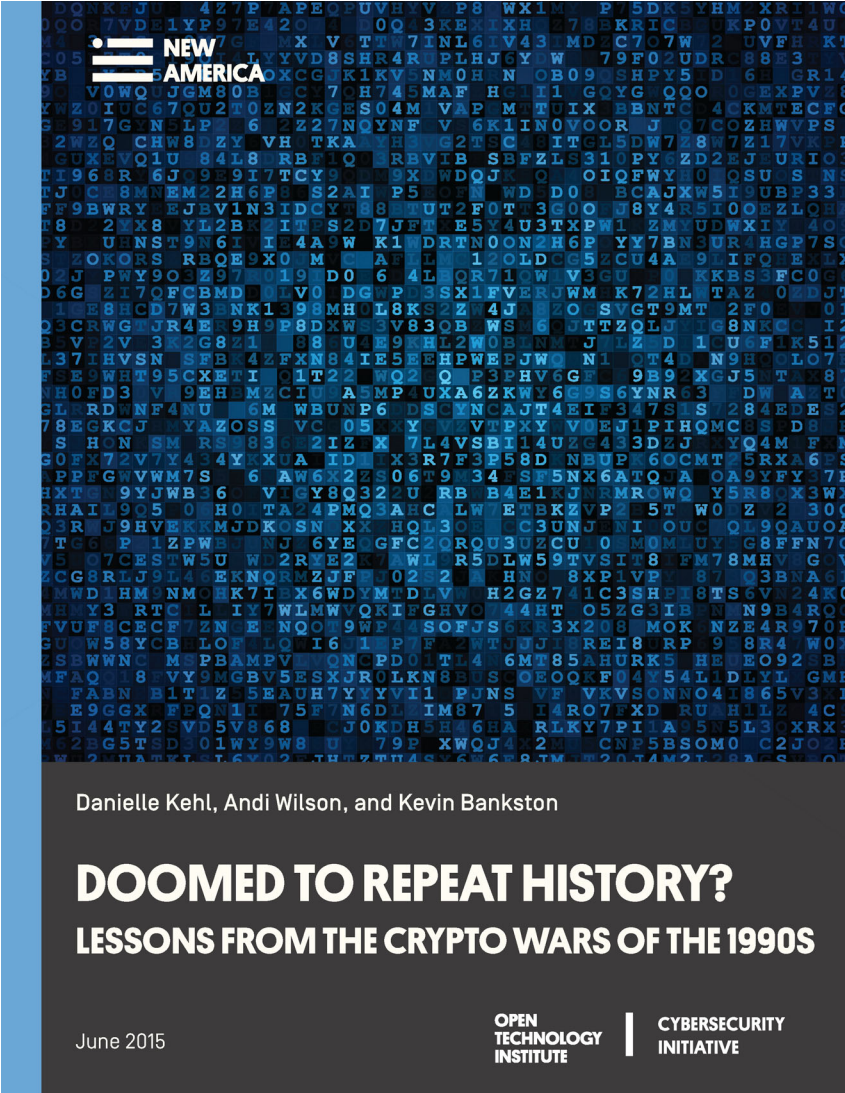
This issue is very real. In Washington County we are prosecuting an infant fatality where evidence shows that a 14 month old had been fed heroin for over 9 months; ultimately resulting in the overdose death of the baby from heroin and cocaine ingestion. A critical piece of the

evidence was secured from one of the Defendant's phone. The defendants are the deceased child's mother and her boyfriend. They are also both charged with selling heroin and cocaine. I have attached to this correspondence just two of the photos we were able to secure from the phone as a result of a valid search warrant. Without these key pieces of evidence, these defendants and others in the future may never be held accountable.

Respectfully,

A handwritten signature in black ink, appearing to read 'J. Anthony Jordan', written over the printed name.

J. Anthony Jordan



NEW AMERICA

Danielle Kehl, Andi Wilson, and Kevin Bankston

DOOMED TO REPEAT HISTORY?

LESSONS FROM THE CRYPTO WARS OF THE 1990S

June 2015

OPEN TECHNOLOGY INSTITUTE | CYBERSECURITY INITIATIVE



© 2015 NEW AMERICA

This report carries a Creative Commons license, which permits non-commercial re-use of New America content when proper attribution is provided. This means you are free to copy, display and distribute New America's work, or include our content in derivative works, under the following conditions:

ATTRIBUTION.

You must clearly attribute the work to New America, and provide a link back to www.newamerica.org.

NONCOMMERCIAL.

You may not use this work for commercial purposes without explicit prior permission from New America.

SHARE ALIKE.

If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.

For the full legal code of this Creative Commons license, please visit creativecommons.org. If you have any questions about citing or reusing New America content, please contact us.

AUTHORS

Danielle Kehl, Senior Policy Analyst, Open Technology Institute

Andi Wilson, Program Associate, Open Technology Institute

Kevin Bankston, Director, Open Technology Institute

ABOUT THE OPEN TECHNOLOGY INSTITUTE

The Open Technology Institute at New America is committed to freedom and social justice in the digital age. To achieve these goals, it intervenes in traditional policy debates, builds technology, and deploys tools with communities. OTI brings together a unique mix of technologists, policy experts, lawyers, community organizers, and urban planners to examine the impacts of technology and policy on people, commerce, and communities. Our current focus areas include surveillance, privacy and security, network neutrality, broadband access, and Internet governance.

ABOUT THE CYBERSECURITY INITIATIVE

The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security Program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work — for the countries, for companies and for individuals.

ACKNOWLEDGEMENTS

The authors would like to thank Hal Abelson, Steven Bellocin, Jerry Berman, Matt Blaze, Alan Davidson, Joseph Hall, Lance Hoffman, Seth Schoen, and Danny Weitzner for their input and comments on an earlier draft of this paper. This paper does not necessarily reflect their views. We would also like to thank the staff and fellows at New America for their help: Jordan McCarthy, David Post, and Robert Morgus.

PHOTO CREDIT COVER PHOTO - Shutterstock

EXECUTIVE SUMMARY

In the past year, a conflict has erupted between technology companies, privacy advocates, and members of the U.S. law enforcement and intelligence communities over the right to use and distribute products that contain strong encryption technology. This debate between government actors seeking ways to preserve access to encrypted communications and a coalition of pro-encryption groups is reminiscent of an old battle that played out in the 1990s: a period that has come to be known as the “Crypto Wars.” This paper tells the story of the that debate and the lessons that are relevant to today. It is a story not only about policy responses to new technology, but also a sustained, coordinated effort among industry groups, privacy advocates, and technology experts from across the political spectrum to push back against government policies that threatened online innovation and fundamental human rights.

Encryption is a method by which two parties can communicate securely. Although it has been used for centuries by the military and intelligence communities to send sensitive messages, the debate over the public’s right to use encryption began after the discovery of “public key cryptography” in 1976. In a seminal paper on the subject, two researchers named Whitfield Diffie and Martin Hellman demonstrated how ordinary individuals and businesses could securely communicate data over modern communications networks, challenging the government’s longstanding domestic monopoly on the use of electronic ciphers and its ability to prevent encryption from spreading around the world. By the late 1970s, individuals within the U.S. government were already discussing how to solve the “problem” of the growing individual and commercial use of strong encryption. War was coming.

The act that truly launched the Crypto Wars was the White House’s introduction of the “Clipper Chip” in 1993. The Clipper Chip was a state-of-the-art microchip developed by government engineers which could be inserted into consumer hardware telephones, providing the public with strong cryptographic tools without sacrificing the ability of law enforcement and intelligence agencies to access unencrypted versions of those communications. The technology relied on a system of “key escrow,” in which a copy of each chip’s unique encryption key would be stored by the government. Although White House officials mobilized both political and technical allies in support of the proposal, it faced immediate backlash from technical experts, privacy advocates, and industry leaders, who were concerned about the security and economic impact of the technology in addition to obvious civil liberties concerns. As the battle wore on throughout 1993 and into 1994, leaders from across the political spectrum joined the fray, supported by a broad coalition that opposed the Clipper Chip. When computer scientist Matt Blaze discovered a flaw in the system in May 1994, it proved to be the final death blow: the Clipper Chip was dead.

Nonetheless, the idea that the government could find a palatable way to access the keys to encrypted communications lived on throughout the 1990s. Many policymakers held onto hopes that it was possible to securely implement what they called “software key escrow” to preserve access to phone calls, emails, and other communications and storage applications. Under key escrow schemes, a government-certified third party would keep a “key” to every device. But the government’s shift in tactics ultimately proved unsuccessful; the privacy, security, and economic concerns continued to outweigh any potential benefits. By 1997, there was an overwhelming amount of evidence against moving ahead with any key escrow schemes.

While the domestic fight over key escrow wore on throughout the mid-1990s, another related battle was brewing on the international front over U.S. export controls and encryption technology. The question at the center of that debate was whether American technologies containing strong encryption should be made available overseas — which would in turn have a significant effect on the domestic availability and use of encryption tools. Until 1996, cryptographic tools were classified as munitions in the United States, with strict limits on the type of encryption that could be exported and the maximum cryptographic key length. Despite growing opposition to these restrictions, the U.S. government

had a strong incentive to maintain encryption export controls as a means to delay the spread and adoption of strong encryption technology abroad. The practical result of the policy was that many companies exported weaker versions of their encrypted products, or were kept out of foreign markets altogether. By the mid-1990s, experts projected billions of dollars in potential losses as a result of these policies. Coupled with growing evidence that foreign-made encryption was readily available around the world, the rationale behind maintaining these controls became increasingly tenuous. Many of the same organizations and individuals that rallied against the Clipper Chip came together to mobilize against encryption export controls, arguing that they undermined U.S. economic competitiveness and individual privacy, with little evidence that they were actually achieving their stated goals.

From 1996 to 1999, the Clinton Administration gradually liberalized encryption export controls, beginning with the 1996 Executive Order that moved most commercial encryption tools from the U.S. Munitions List to the Commerce Control List. The next step involved relaxing limits on the strength of encryption keys. Although these concessions were originally used as a bargaining chip in the commercial key escrow debate — companies would be allowed to export higher strength encryption if they agreed to retain the keys — those requirements were eventually abandoned after pressure from industry and public interest groups. In September 1999, the White House announced a sweeping policy change that removed virtually all restrictions on the export of retail encryption products, regardless of key length. As journalist Steven Levy put it succinctly: “It was official: public crypto was our friend.”

In the decades since the resolution of the Crypto Wars, many of the predictions about how strong encryption would benefit the economy, strengthen Internet security, and protect civil liberties have been borne out. In particular, the widespread availability of robust encryption laid the groundwork for the emergence of a vibrant marketplace of new Internet services based on secure digital communications and the widespread migration of sensitive communications online. The emergence of foundational technologies like the Secure Sockets Layer (SSL) and the Secure Shell Protocol (SSH) allowed the encrypted web to expand rapidly to include electronic banking, electronic medical records systems, online bill payment tools, home automation systems, e-filing systems for taxes, and VPNs. The evolution of the ecosystem for encrypted communications has also enhanced the protection of individual communications and improved cybersecurity, and today, strong encryption is an essential ingredient to the overall security of the modern network. And finally, the end of the Crypto Wars ushered in an age where the security and privacy protections afforded by the use of strong encryption also help promote free expression.

Unfortunately, the consensus that strong encryption is good for security, liberty, and economic growth has come under threat in recent years. The June 2013 revelations about the U.S. National Security Agency’s pervasive surveillance programs — not to mention the NSA’s direct attempts to thwart Internet security to facilitate its own spying — dramatically shifted the national conversation, highlighting the vulnerabilities in many of the tools and networks on which we now rely for both everyday and sensitive communications. While ordinary individuals, civil liberties advocates, and major technology companies have since embraced greater use of encryption as a necessary step to address a wide range of modern threats from both government and nongovernment actors, intelligence agencies and law enforcement officials have also become increasingly outspoken against measures to strengthen these systems through encryption. To make their case, they have revived many of the arguments they made about encryption in the 1990s, seeming to have forgotten the lessons of the past.

It seems like we may once again be on the verge of another war: a Crypto War 2.0. But it would be far wiser to maintain the peace than to begin a new and unnecessary conflict. There is no reason to repeat our previous mistakes.

TABLE OF CONTENTS

Introduction.....	1
I. Before the Crypto Wars.....	2
The Birth of Public Key Cryptography.....	3
The U.S. Government Prepares for Battle.....	3
II. The Battle of the Clipper Chip and the War Over Key Escrow.....	5
How the Clipper Chip Worked.....	5
Public Mobilization Against the Clipper Chip.....	6
Marching Toward Clipper's Demise.....	8
The Clipper Chip is Dead! Long Live Key Escrow!.....	9
Commercial Key Escrow: "A Swing and a Miss".....	9
III. The Battle Over Encryption Export Controls.....	12
Testing the Waters: The Cases of Karn, Bernstein, and Zimmermann.....	12
Encryption Source Code as a Weapon.....	12
The Campaign for Crypto Without Borders.....	13
From Weakening Crypto to Weakened Restrictions: The Liberalization Process.....	15
IV. Post-War: How the Crypto Warriors Were Proven Right.....	18
The Internet and the Information Economy Have Grown Exponentially	
Since the Crypto Wars.....	18
Strong Encryption Has Become a Bedrock Technology that	
Protects the Security of the Internet.....	19
Strong Encryption Has Become An Integral Tool in the Protection of Privacy	
and the Promotion of Free Expression Online.....	19
The Organizing Efforts Carried Out in Support of Internet Openness	
During the Crypto Wars Have Helped Shape Modern Internet Advocacy Campaigns.....	20
Conclusion: Encryption Under Threat... Again.....	21
Endnotes.....	22

INTRODUCTION

History sometimes repeats itself.

In the past year, a conflict has erupted between technology companies, privacy advocates, and members of the U.S. law enforcement and intelligence communities over the right to use and distribute products and services that use strong encryption. In September 2014, Apple announced that it would be moving to smartphone encryption by default on all devices running its new iOS, followed a few days later by a similar announcement from Google about the latest version of the Android operating system.¹ Since the 2013 Snowden disclosures — which caused consumer trust in American technology companies to plummet² — a number of U.S. companies have taken greater steps to use the more secure HTTPS protocol, to encrypt end-user devices by default, and to make end-to-end encryption³ available for their email and messaging services.⁴ Although many users in the United States and around the world welcomed the changes, the Apple and Google announcements in particular prompted significant backlash from some American law enforcement and intelligence officials.⁵ FBI Director James Comey has argued that Apple and Google's new privacy-enhancing features will “allow people to place themselves beyond the law” and that default encryption could seriously hinder criminal investigations, calling on Congress to take action to force companies to maintain some kind of backdoor to allow government access to communications if a warrant has been obtained.⁶ Former Attorney General Eric Holder has also urged tech companies to leave backdoors open for police,⁷ and their arguments have received support from the National Security Agency and the Office of the Director for National Intelligence.⁸ The requests have ignited a public discussion about whether it is technically feasible to implement surveillance backdoors without undermining the overall security of cryptographic systems, and what the economic and civil liberties implications are.⁹

This is not a new debate. A similar policy battle over encryption happened twenty years ago: a conflict that has come to be known as the “Crypto Wars.”¹⁰ Throughout the 1990s, policymakers and advocates fiercely debated the tradeoffs related to the proliferation of encryption technology both in the United States and overseas. Although the dispute had been brewing beneath the surface for years, the beginning of the Crypto Wars can be traced back to the Clinton Administration's 1993 “Clipper Chip” proposal, which eventually evolved into a broader debate about “key escrow” technologies and whether the government or a trusted third party should hold master keys that could be used to decode any encrypted communications. By 1996, the battle was being fought on two fronts, as the conflict over the U.S. government's attempt to restrict the proliferation of strong encryption technology overseas through export controls erupted. After a groundswell of opposition from privacy advocates, industry representatives, and prominent politicians — including significant online organizing and lobbying efforts to educate the public and the highlight the technical and legal flaws in the U.S. government's policies — the Administration capitulated, abandoning the Clipper Chip and related key escrow proposals and relaxing U.S. export controls on strong encryption products.¹¹ By the time Vice President Al Gore finally announced sweeping changes to U.S. export restrictions in the fall of 1999, it was clear that the Crypto Wars were over, and the arguments in favor of strong encryption had won.

This paper tells the story of the original Crypto Wars and the lessons that they offer. It is a story about policy responses to new technology, but it is also a story about a sustained, coordinated effort among industry groups, privacy advocates, and technology experts from across the political spectrum to push back against government policies that threatened online innovation and fundamental human rights. Its goal is to remind us of what happened twenty years ago and why the debate reached the conclusion that it did, so that we might avoid the Crypto Wars 2.0. Unless we learn the lessons of the first Crypto Wars, we may be doomed to repeat the mistakes of the past.

I. BEFORE THE CRYPTO WARS

Contrary to what many people now believe, encryption technology is not a product of the digital age, nor something that the Founding Fathers could not have fathomed when they wrote the United States Constitution.¹² In fact, in the early 1790s, while serving as George Washington's Secretary of State, Thomas Jefferson himself relied upon encryption to securely encode and decode messages in the letters that he sent overseas, using a wooden device that he invented known as a wheel cipher.¹³ Encryption methods have actually been used for centuries by diplomats, intelligence officers, and soldiers — from the ancient Romans to the likes of Benjamin Franklin, Alexander Hamilton, and John Adams — to send sensitive messages without fear that the contents could be read if they were intercepted.¹⁴

Modern encryption relies on mathematical algorithms to protect the security and integrity of messages and streams of data as they are transmitted electronically or when stored on devices.¹⁵ For much of the twentieth century, these sophisticated encryption techniques were available almost exclusively to members of the government, military, and intelligence communities. Even as encryption methods became more effective and easier to use over time, they still required special technology or training that was closely guarded, and much of the cutting-edge development in the field was not visible to the public.¹⁶ As a result, although significant advances had been made in the field by the early 1970s, sending encrypted electronic messages remained beyond the reach of ordinary individuals until 1976.

DEFINING CRYPTOGRAPHY

The term “cryptography” refers to the practice and study of theory and techniques for secure storage and communications. Encryption is the actual process of combining the contents of a message (“plaintext”) with a secret value or password (the encryption “key”) in such a way that scrambles the content into a totally new form (“ciphertext”) that is unintelligible to unauthorized users. The goal is that only someone with the correct key can decrypt the information and convert it back into plaintext.

THE BIRTH OF PUBLIC KEY CRYPTOGRAPHY

“The crypto war is the inevitable consequence of a remarkable discovery made almost 20 years ago, a breakthrough that combined with the microelectronics revolution to thrust the once-obscure field of cryptography into the mainstream of communications policy.”

- Stephen Levy, “Battle of the Clipper Chip” (1994)

“The set of algorithms, equations and arcane mathematics that make up public key cryptography are a crucial technology for preserving computer privacy in and making commerce possible on the Internet. Some hail its discovery as one of the most important accomplishments of 20th-century mathematics... Without it, there would be no privacy in cyberspace.”

- Peter Wayner, “A Patent Falls, and the Internet Dances” (1997)

Everything changed with the invention of public key cryptography in 1976. Two researchers named Whitfield Diffie and Martin Hellman published a revolutionary paper on a new technology they called “public key cryptography,”¹⁷ which demonstrated how ordinary individuals and businesses could securely communicate data over modern communications networks.¹⁸ Diffie and Hellman described a process in which each participant in a conversation created related public and private keys, which could then be used to encrypt and decrypt plaintext conversations.¹⁹

Their crucial insight was that the key used to encrypt a message could be linked to, but distinct from, the key used to decrypt the message — so that anyone could create and distribute a unique “public” key, useful only for creating messages that no one but the owner of the corresponding “private” key would be able to unscramble.²⁰ Unlike previous methods of encryption, this approach allowed two or more parties to communicate privately and securely even if they had never previously met.²¹

The discovery of public key cryptography laid the foundation for a number of innovations in secure communications over the next 40 years. Not long after Diffie and Hellman’s “New Directions in Cryptography” was published, three mathematicians at the Massachusetts Institute of Technology — Ronald Rivest, Adi Shamir, and Leonard Adleman — developed a system that put the split-key encryption theory into practice.²² The technique that they created in 1977, known as “RSA” (a combination of their initials), ensured that electronic mail messages could be kept private. It also offered a means to digitally “sign” messages to show authenticity.²³ This discovery, coupled with Diffie and Hellman’s paper and other research, sparked the beginning of significant academic interest in cryptography.²⁴

In those early days, however, the commercial viability of technology that used public key encryption remained unclear.²⁵ The market for strong cryptosystems that eventually developed had two fundamental drivers: the increasing use of personal computers by large companies, and the demand for secure email technology for individual use.²⁶ So as both became more common in the 1980s, commercial demand for encryption products exploded.²⁷ The increased use of networked PCs by corporations required that they use strong encryption to protect those networks, especially as more and more confidential data was computerized.²⁸ New markets emerged for authentication and digital signature software, antivirus software, data storage protection, firewalls, utility software, network security products, and virtual private network (VPN) software.²⁹

While corporations drove much of the commercial development of cryptographic technology, a burgeoning community of privacy activists also began to create encryption tools for individual users. Computer scientist Philip Zimmermann designed one of the first major practical tools for end-to-end public key encryption of

files and e-mail — a project called Pretty Good Privacy (PGP) — and released it publicly in 1991. As Zimmermann explained, “until recently, if the government wanted to violate the privacy of ordinary citizens, they had to expend a certain amount of expense and labor to intercept and steam open and read paper mail.”³⁰ But with email, this was no longer the case — messages transmitted in plaintext were essentially postcards that could be read by anyone who intercepted them. A tool to encrypt text, emails, files, and contents of hard drives helped empower individuals to “take their privacy into their own hands.”³¹

THE U.S. GOVERNMENT PREPARES FOR BATTLE

“If people had access to the means to encrypt their private communications, there could be a place to hide—and a universal means to privacy was what an agency charged with eavesdropping is hell-bent to prevent.”

— Steven Levy, *Crypto* (2001)

While businesses and individuals may have been happy about the increasing use of encryption, the U.S. government was not. From the 1970s onward, intelligence and military officials in particular had identified advances in cryptographic technology as a threat to U.S. security and taken actions to discourage or halt research on encryption.³² They understood that the widespread adoption of encryption — by both corporations and individuals — challenged their longstanding domestic monopoly on the use of electronic ciphers, as well as their ability to prevent encryption from spreading around the world.³³ As Jay Stowsky, a professor at UC Berkeley, explained, “[Early civilian cryptographers’] extraordinary achievements from the 1970s on were not viewed as benign by the world-class eavesdroppers at the NSA... As commercial applications developed by U.S. companies nevertheless became ever more sophisticated and widely accessible, the full weight of the federal government was brought to bear to control the pattern and pace of their diffusion.”³⁴ But maintaining this control became increasingly difficult as a growing number of individuals and corporate actors built upon the work of early pioneers like Diffie, Hellman, and the RSA trio in the 1980s.³⁵

By the early 1990s, the proliferation of personal computers, cell phones, and the Internet forced these concerns about the impact of encryption on

surveillance capabilities to the surface.³⁶ In January 1991, Senator Joe Biden inserted new language into the draft of an anti-terrorism bill, expressing a Sense of Congress that electronic communications service providers and equipment manufacturers “shall ensure that communications systems permit the government to obtain the plaintext contents of voice, data, and other communications when appropriately authorized by law.”³⁷ Although the proposal did not advance, the message to companies was clear: the government was not likely to tolerate communications services offering strong encryption unless they also included “backdoors” allowing the government to lawfully obtain the decrypted contents of encrypted messages. Meanwhile, within the NSA, discussions began in earnest in 1992 about how the government might permanently address the “problem” of the widespread use of encryption.³⁸

The murmurings about a possible “solution” signaled that a major conflict over encryption was inevitable. War was coming.

II. THE BATTLE OF THE CLIPPER CHIP AND THE WAR OVER KEY ESCROW

"We need the 'Clipper Chip' and other approaches that can both provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities."

- White House Press Statement (April 1993)

On April 16, 1993, the White House unveiled a new initiative to address the competing challenges presented by the growing use of encryption.³⁹ The concept was simple: Government engineers had developed a state-of-the-art microchip, known as the "Clipper Chip," which could be inserted into consumer hardware telephones, providing the public with strong cryptographic tools without sacrificing the ability of law enforcement and intelligence agencies to access unencrypted versions of those communications.⁴⁰ The White House's official announcement called it "an important step in addressing the problem of encryption's dual-edge sword."⁴¹

The government offered assurances that the cryptographic algorithm used in the chips was more powerful than most available commercial encryption standards, protecting sensitive information while preserving "the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals."⁴² Although adoption of the standard was technically voluntary, the government committed to purchasing a massive number of devices containing the Clipper Chip, which officials hoped would strongly influence the marketplace and result in its widespread adoption throughout the 1990s.⁴³

HOW THE CLIPPER CHIP WORKED

The Clipper Chip technology relied on a system of "key escrow," in which a copy of each chip's unique encryption key would be stored by the government. In order to increase security, every key would be split in two so that no single organization had all the information necessary to conduct an unauthorized wiretap. These parts were entrusted to the Commerce Department's National Institute of Standards and Technology (NIST) and the Treasury Department. When they had "lawful authorization," the two federal agencies would jointly release them to law enforcement, providing the means to access unencrypted copies of the encrypted conversations.⁴⁴

The NSA selected an encryption algorithm known as "Skipjack" to use in the Clipper Chip. Skipjack represented the culmination of the agency's efforts to establish a crypto standard that was ostensibly both strong and easy to compromise for legitimate law enforcement purposes. It was considerably more sophisticated and robust than any other established encryption algorithm then available.⁴⁵ But the NSA was only willing to let Skipjack be used under two conditions. First, because the algorithm itself was classified, it could only be embedded into devices (such as secure phones) that were manufactured in collaboration with the government; no one outside of the NSA was allowed to actually see how Skipjack worked, or use it for non-authorized purposes.⁴⁶ Second, the government mandated that Skipjack only be used in tandem with another system that introduced a "backdoor" into the cryptographic process — officially known as a "Law Enforcement Access Field," or LEAF — which government officials could use to gain access to the keys that protected any Skipjack-encrypted communication.⁴⁷

The supposed strength of the Skipjack algorithm was central to the government's justification of the Clipper Chip proposal. By offering consumers encryption that was significantly more advanced than anything that had previously been

available, they hoped to build public trust and acceptance of the technology — enough to overcome concerns that it also facilitated government access through key escrow.⁴⁸ So the government convened a panel of academic and industry experts to conduct a review of Skipjack.⁴⁹ The leader of the group, a computer science professor from Georgetown named Dorothy Denning, was not only a crypto expert but had spent significant time researching and defending the positive role that the “hacker culture” could play in a modern information society.⁵⁰ In the early 1990s, she came out in favor of escrowed encryption as a means to balance individual privacy interests with overall social good.⁵¹ In later years, Denning explained that as a participant in the panel she aimed to address concerns that the Clipper Chip was insecure and allegations that the NSA’s decision to keep Skipjack classified was an attempt to hide vulnerabilities in the algorithm.⁵²

The report’s overall assessment of Skipjack was overwhelmingly positive. It concluded that it would be “36 years before the cost of breaking Skipjack by exhaustive search will be equal to the cost of breaking DES today,” and that “there is no significant risk that Skipjack can be broken through a shortcut method of attack.”⁵³

In July 1993, around the same time that the expert panel’s interim report on Skipjack was published, NIST initiated a public comment process on the Clipper Chip and the concept of key escrow more broadly. In a stark contrast to the affirmation expressed by Denning’s group, only two of the 320 comments NIST received in response to its call were positive.⁵⁴ Experts participating in the NIST process voiced three primary sets of concerns with the proposal. First, many were wary of trusting the U.S. government as a keyholder, which would give federal agencies and law enforcement officials unprecedented access to — and power over — the private information of their citizens. Diffie, the father of public-key cryptography, argued that key escrow eliminated one of the system’s key strengths: it re-introduced reliance on a third party to protect keys, a serious vulnerability.⁵⁵ To make matters worse, under the Clipper Chip scheme, this third party would be the government, which was especially troubling for privacy advocates who already questioned the government’s respect for personal privacy.⁵⁶

Relatedly, some industry commenters were concerned about how the Clipper Chip could affect future business, given the government’s explicit intent to use its market

power to shape the business environment and concerns that it might eventually make the technology mandatory.⁵⁷ And regardless, in the meantime, any company that wanted to do business directly with the government would be forced to adhere to the Clipper standard.⁵⁸ The chips themselves were expensive and, by design, could only be purchased from one supplier, which eliminated the potential for competition in production or pricing.⁵⁹ There was also a risk that other products might not be compatible with Clipper-enabled devices.⁶⁰ As journalist Steven Levy wrote in 1994, “the Government’s stated intent is to manipulate the marketplace so that it will adopt an otherwise unpalatable scheme and make it the standard. Existing systems have to cope with... incompatibility with the new Government Clipper standard. Is it fair to call a system voluntary if the Government puts all sorts of obstacles in the way of its competitors?”⁶¹

Finally, there was speculation that Clipper was the first step toward prohibition of other forms of encryption that did not rely on key escrow or provide other means of backdoor access to communications.⁶² Corporations and individuals that had already adopted encryption technology feared that their tools might be rendered less effective — or even declared illegal — if the Clipper Chip took off.⁶³

PUBLIC MOBILIZATION AGAINST THE CLIPPER CHIP

The NIST comment process was not the only place where members of the public expressed concerns about the Clipper Chip. In fact, the proposal sparked an unprecedented wave of coordinated digital activism and lobbying efforts from a multitude of different groups.⁶⁴ Opposition to the Clipper Chip united privacy activists, technologists, academics, hackers, and industry leaders from across the political spectrum in the face of what they considered a significant threat to Internet security, economic competitiveness, and individual civil liberties.

In May 1993, a few weeks after the Clipper Chip proposal was announced, Whit Diffie testified before Congress on “The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology.”⁶⁵ Diffie’s testimony offered a window into the significance of the issue. “[S]uch a proposal is at best premature and at worst will have a damaging effect on both business

security and civil rights without making any improvement in law enforcement,” he told the chamber.

Two weeks later, 26 of the nation's largest computer companies issued a statement through their trade organization, the Computer and Business Equipment Manufacturers Association, criticizing the economic viability of the Clipper plan. The group, which included Apple, AT&T, Hewlett Packard, IBM, and Xerox, told the Computer System Security and Privacy Advisory Board⁶⁶ that “encryption issues no longer can be treated as the province of only a small circle of national security, law-enforcement and technology experts.”⁶⁷

These efforts were only the beginning of a sustained effort by a diverse, loose-knit coalition of companies and activists to demonstrate the potential harms of the government's key escrow proposal. Key to that movement were the Cypherpunks, a “confederation of computer hackers, hardware engineers and high-tech rabble-rousers” who saw the proposal as a fundamental threat to electronic privacy.⁶⁸ As one of the Cypherpunk founders, Eric Hughes, said not long after the Clipper Chip was announced, “This plan creates the ears of Big Brother, just as Orwell warned.”⁶⁹ The introduction of the Chip confirmed their fears that the government's mission was to cripple strong cryptography and keep it out of the public's hands.⁷⁰ Comprised mainly of technologists, the Cypherpunks embraced electronic mailing lists and online newsgroups to organize and disseminate their message.⁷¹ They planned boycotts of AT&T — which had agreed to include the Clipper Chip in its new encrypted phone — and organized media campaigns, cooperating with new digital rights advocacy groups as part of their strategy to protect encryption.⁷²

A wide range of individuals and organizations joined the Cypherpunks in the public campaign against the Clipper Chip. Recognizing the clear threat to the right to privacy, nascent digital rights groups like the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC) rallied against the proposal.⁷³ They organized experts to speak on panels, testified before Congress, and circulated electronic petitions, including one that garnered over 50,000 signatures — an unprecedented number in the early days of Internet activism.⁷⁴ Decades before popular online advocacy campaigns like the one that stopped the Protect IP Act (PIPA) and Stop Online Piracy Act (SOPA) in 2012,⁷⁵ these

groups used Internet-enabled tools like email and online forums to spread and amplify their messages and force a public conversation about the merits of the Clipper proposal.⁷⁶

A key part of the organizing strategy involved bringing together diverse groups of constituents to articulate the threats posed by the Clipper Chip. A group called the Computer Professionals for Social Responsibility (CPSR), which was founded in 1981 to “promote the responsible use of computer technology,”⁷⁷ coordinated many of these efforts, organizing letters and online petitions to demonstrate both widespread and expert opposition to the proposal. In January 1994, for example, CPSR brought together more than three dozen leading cryptographers, security experts, and privacy advocates in a letter to the Clinton Administration urging it to abandon the Clipper Chip scheme.⁷⁸ The signatories included many of the fathers of public cryptography — Diffie, Hellman, Rivest, Zimmermann, and Ralph Merkle among them — as well as trusted privacy and security experts like Bruce Schneier and Jerry Berman. The letter contained an ominous warning: “If the plan goes forward, commercial firms that hope to develop new products will face extensive government obstacles. Cryptographers who wish to develop new privacy enhancing technologies will be discouraged. Citizens who anticipate that the progress of technology will enhance personal privacy will find their expectations unfulfilled.”⁷⁹

Privacy advocates also teamed up with allies in industry to highlight the economic ramifications of the proposal. In May 1993, the Digital Privacy and Security Working Group — a coalition that included both privacy advocates and communications and computer companies like Apple, AT&T, Hewlett-Packard, IBM, Lotus Development Corporation, Microsoft, RSA Data Security, and Sun Microsystems — submitted a letter to President Clinton expressing concerns about the Clipper program. “While we recognize the importance of authorized national security and law enforcement needs,” the letter stated, “we believe that there are fundamental privacy and other constitutional rights that must be taken into account.”⁸⁰ These were some of the country's most powerful tech companies telling the White House that they were concerned about its sweeping new policies — the same companies who were expected to build products that employed key escrow systems.

Finally, a number of prominent politicians from both sides of the political spectrum joined the fray, including Senators John Kerry and Patrick Leahy and Representatives Maria Cantwell, Sam Gejdenson, and Ed Markey.⁸¹ As Senator Patrick Leahy, one of the most vocal critics of Clipper, pointed out, one had to wonder if it would even be effective given the existence of alternatives like PGP. “I

have serious questions about whether any sophisticated criminal or terrorist organization is going to use the one code endorsed by the U.S. Government and for which U.S. Government agents hold the decoding keys,” he said in a 1994 hearing. “There are a multitude of alternative encryption methods commercially available.”⁸²

MARCHING TOWARD CLIPPER’S DEMISE

Despite growing opposition to the proposal, officials seemed intent on moving forward with it. In February 1994, the federal government officially adopted the technology behind the Clipper Chip as a Federal Information Processing Standard. Formally known as the Escrowed Encryption Standard (EES), its stated goal was to “facilitate the acquisition of devices that implement escrowed encryption techniques by Federal government agencies.”⁸⁴

The decision to move forward did little to reassure a skeptical public. By March 1994, according to a *CNN/TIME* poll, eighty percent of Americans opposed the Clipper Chip.⁸⁵ So the government went into public relations overdrive. In an attempt to engage directly with the opposition, the NSA’s Chief Counsel Stewart Baker published an article in *Wired*, a tech-focused magazine, called “Don’t Worry Be Happy: Why Clipper Is Good For You.”⁸⁶ He also participated in an online Q&A on the subject, attempting to address the most pervasive myths about the Clipper Chip. Dorothy Denning also went on the offensive to advocate for the program, writing journal articles and op-eds, debating prominent critics online, and becoming one of the government’s most vociferous advocates.⁸⁷ But these spirited defenses gained little traction in comparison to the diverse coalition of groups that had come together opposing Clipper.

The final death blow for the Clipper Chip came in June 1994 from Matt Blaze, a computer scientist at AT&T Bell Laboratories. In a technical paper titled “Protocol Failure in the Escrowed Encryption Standard,” Blaze revealed that he had found a serious flaw in the Clipper Chip’s security.⁸⁸ Simply put, Blaze demonstrated that the technology did not work as advertised: with the help of a brute force attack, a user could avoid transmitting the LEAF and circumvent the law-enforcement surveillance mechanism entirely.⁸⁹ Consequently, “some communications... can be encoded so that not even the government, decrypting keys in hand, can unscramble them.”⁹⁰ The circumvention

THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA)

It is difficult to tell the history of the Crypto Wars without telling the story of the Communications Assistance for Law Enforcement Act (CALEA), which Congress passed in 1994. CALEA was written in response to concerns from the FBI that, as telecommunications services were transitioning from analog to digital systems, they needed to preserve and enhance their ability to access communications transmitted by those services when they had lawful wiretap demands. After fierce debate between privacy advocates and law enforcement officials, both sides came to a compromise which included key concessions related to the use of encryption and pro-privacy updates to the Electronic Communications Privacy Act (ECPA). In particular, law enforcement, under heavy pressure from privacy advocates, had to accept that the law’s mandate of intercept capability neither prevented telecommunications users from employing encryption nor required service providers to block or break such user-generated encryption. The law, at 47 USC § 1002(b)(3), explicitly states that a “telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.” Further clarification can be found in the legislative history, which explicitly notes that “nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access” and “Nothing in the bill is intended to limit or otherwise prevent the use of any type of encryption within the United States.”⁹¹ The insertion of this language was a key win for the pro-encryption side in the Crypto Wars.

of Clipper's "backdoor" was the most damning evidence yet, confirming fears that the encryption standard had significant unforeseen vulnerabilities.⁹¹ What's more, the fact that the government could be shut out of its own surveillance protocol suggested that it was not qualified to be dictating technical mandates like the Clipper Chip at all. *The New York Times* headline about Blaze's research simply read: "Flaw Discovered in Federal Plan for Wiretapping."⁹²

Blaze's discovery, coupled with the growing wave of public opposition, proved fatal to the original Clipper Chip proposal. In a January 1995 *Wall Street Journal* article about a new, much stronger chip being developed by AT&T and a semiconductor manufacturer, one analyst called the Clipper Chip "dead." As James Bidzos, the president of RSA Data Security, suggested, "the NSA must see that they're losing the battle."⁹³

THE CLIPPER CHIP IS DEAD! LONG LIVE KEY ESCROW!

*"This convergence of technology — cheap ubiquitous PCs, modems, FAX, digital phones, information superhighways, et cetera — is all part of the information revolution... All these devices will be using encryption... Trying to stop this is like trying to legislate the tides and the weather... even with the NSA and the FBI on their side, it's still impossible."*⁹⁴

- Phil Zimmermann, Congressional Testimony (1996)

Although the initial Clipper proposal flopped, the idea that the government could find a compromise that would allow it to access the keys to a widely implemented encryption standard lived on throughout the 1990s. Many policymakers clung to hopes that it was possible to securely implement a key escrow system for phone calls, emails, and other communications and storage applications.⁹⁵ In short, the government did not abandon its attempts to control cryptography after 1994 — it simply changed tactics. The evolution was toward the concept of "software key escrow," sometimes called "commercial key escrow" (CKE).⁹⁶ Later, some would also refer to these as "key recovery" schemes.⁹⁷

Commercial key escrow was different from the Clipper Chip in a number of respects. Rather than focusing on the inclusion of a physical chip in hardware, the idea was to convince companies to implement a key escrow system

themselves, a much more flexible alternative which could also be used for software products containing strong encryption. Instead of requiring the use of a single cryptographic algorithm, like the government had tried with Skipjack, new proposals simply limited the key length to 64 bits.⁹⁸ Under the new scheme, private escrow agents — certified by the government, of course — would hold the keys, rather than simply putting everything in the hands of the Treasury Department and NIST.⁹⁹ To sweeten the deal, the government offered the software industry a significant carrot: they would relax encryption export controls in exchange for agreeing to these criteria (a debate which we will discuss in further depth in the next part of this paper).

Subsequent iterations of the proposal, introduced in 1995 and 1996, attempted to use the new commercial key escrow model to address the concerns of U.S. companies.¹⁰⁰ However, although marginally improved and repackaged, these key escrow proposals were ultimately no more palatable than the original Clipper Chip (and some even referred to them dismissively as "Clipper II" and "Clipper III"). Opponents maintained serious reservations about the potential abuse of power by the trusted third party in the absence of a strong mechanism for oversight and concerns about the security of the escrow system.¹⁰¹ In May 1996, Senator Conrad Burns lambasted the Administration's third, and ultimately final, attempt: "[T]he third version of the administration's Clipper Chip proposal is a swing and a miss. It's time to quit relying on government mandates for what is truly a matter of great concern to the private sector: the expansion of commerce on the Internet and other computer networks."¹⁰²

COMMERCIAL KEY ESCROW: "A SWING AND A MISS"

During the first Clipper debate there had been a vocal, if small, group of lawmakers opposing to the proposal in both the House and Senate. But as the debate expanded to more complex attempts to regulate encryption, those concerns grew and began to encompass broader value questions. How should privacy be protected in the digital age? How could the United States balance its interest in national security with its commitment to economic development and strong civil liberties when dealing encryption technology? Congress held hearings on the merits of key escrow, often led by Clipper opponents like Senator Leahy, Senator Ashcroft, Senator Burns, and

Representative Bob Goodlatte.¹⁰³ None of them seemed willing to accept the Administration's software key escrow proposals.

Some, like Senator Burns, argued that decisions about the use of encryption should be left up to businesses. In a letter to "the Internet community" in May 1996, he criticized the Administration for acting "without regard to the harm this policy has on American businesses' ability to compete in the global marketplace or the ability of American citizens to protect their privacy online. Until we get the federal government out of the way and encourage the development of strong cryptography for the global market, electronic commerce and the potential of the Internet will not be realized."¹⁰⁴ At the same time, Burns introduced legislation that would, among other things, prohibit mandatory key escrow and limit the Commerce Department's ability to impose encryption standards on non-government entities, as they had attempted to do with the Clipper Chip.¹⁰⁵ The Promotion of Commerce Online in the Digital Era (Pro-CODE) Act, along with similar proposed legislation like the Security and Freedom Through Encryption (SAFE) Act (which we discuss in detail in Part III) demonstrated the lengths to which some members of Congress were willing to go to stop the Administration's quest for key escrow.¹⁰⁶

Other lawmakers stressed the importance of civil liberties in the digital era, clearly concerned about the impact of mandatory backdoors on those fundamental rights. In 1997, for example, John Ashcroft made an impassioned defense of online privacy, arguing that, "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?"¹⁰⁷

Meanwhile, additional evidence against the adoption of these proposals continued to pile up. After an extensive study, the National Research Council (NRC) issued a 700-plus page report in 1996 on the policy challenges that encryption posed, strongly endorsing its availability. The report's primary recommendation stated that:

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.¹⁰⁸

The report also found that the "debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis," undermining the claims made by those who invoked classified information to bolster their arguments.¹⁰⁹ Overall, the NRC's conclusions were overwhelmingly pro-encryption and had a powerful impact on the debate.

Around that time, the foreign governments whom the U.S. had also been lobbying to adopt a key recovery approach overseas also rejected the idea. In early 1997, the U.S. had attempted to get the Organisation for Economic Co-operation and Development (OECD) to adopt a recommendation supporting key escrow and key recovery. But instead of supporting it, the OECD's final recommendation turned into a statement against the idea.¹¹⁰ A European Commission report later that year went even further, declaring that, "In order to make good use of the commercial opportunities offered by electronic communication via open networks, a secure and trustworthy environment is... necessary. Cryptographic technologies are nowadays widely recognised as the essential tool for security and trust in electronic communication."¹¹¹ The Commission rejected the American proposals for key recovery on the basis that they undermined privacy, threatened economic growth, and were likely to be simply ineffective. "The report appears to all but doom efforts by the Clinton Administration and the Federal Bureau of Investigation to establish a global system in which people who use cryptography would have to deposit a 'key' for unlocking their codes with an independent outside organization," explained the *The New York Times* in October 1997.¹¹²

One of the final nails in the coffin for key escrow proposals came from a group of almost a dozen technical experts convened by the Center for Democracy and Technology that included Matt Blaze, Whit Diffie, Ronald Rivest, Bruce Schneier, John Gilmore, and Steve Bellovin.¹¹³ In a paper examining a range of proposals for key recovery,

key escrow and “trusted third party” encryption, they concluded that the “deployment of key-recovery-based encryption infrastructures to meet law enforcement’s stated specifications will result in substantial sacrifices in security and greatly increased costs to the end user.” Their analysis suggested that the task would be “enormously complex” and “far beyond the experience and current competency of the field.” What’s more, they argued that, “Even if such infrastructures could be built, the risks and costs of such an operating environment may ultimately prove unacceptable.”¹¹⁴ The paper concluded that: “Key recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature. The massive deployment of key-recovery-based infrastructures to meet law enforcement’s specifications will require significant sacrifices in security and convenience and substantially increased costs to all users of encryption.”¹¹⁵

This final barrage of reports condemning the very idea of key escrow represented the closing shots in the battle that began with the Clipper Chip. However, by that point the Crypto Wars were also raging on another front, as pro- and anti-encryption forces battled over the government’s role in restricting the availability of encryption overseas.

III. THE BATTLE OVER ENCRYPTION EXPORT CONTROLS

As the domestic fight over key escrow wore on, another battle was brewing on the international front over U.S. export controls and encryption technology. The question at the center of that debate was whether American technologies containing strong encryption should be made available overseas — which would in turn have a significant effect on the domestic availability and use of encryption tools as well.

TESTING THE WATERS: THE CASES OF KARN, BERNSTEIN, AND ZIMMERMANN

In 1994, an engineer named Phil Karn tried to send a copy of Bruce Schneier's book, *Applied Cryptography*,¹⁶ and an accompanying floppy disk containing an electronic copy of the book text, outside of the United States.¹⁷ At the time, products containing encryption were regulated as munitions exports under the International Traffic in Arms Regulations (ITAR), so Karn submitted a request to the Department of State to find out if the book was subject to any restrictions. The verdict that came back seemed paradoxical: although the book could be freely exported without restriction, the disks — which included the same encryption source code printed in Part Five of the physical book — were designated under a defense category subject to strict export controls.¹⁸ Karn appealed the decision on the basis that the export restriction violated his First Amendment rights.

Although a judge ultimately dismissed Karn's claims in 1996, other high-profile legal incidents related to the export restrictions on encryption technology arose in the mid-1990s as well — part of a loosely coordinated effort to highlight growing concerns with the U.S. regulations as commercial encryption spread. For example, many are familiar with the case of Daniel Bernstein, a PhD candidate at UC Berkeley who fought a series of court challenges after he attempted to publish his public key encryption algorithm, "Snuffle," in both paper and online format.¹⁹ Or Phil Zimmermann, the creator of PGP, who found himself under a three year investigation by the Justice Department for possible export violations because his cryptographic software program ended up in the hands of foreign Internet users, even though it was only uploaded to sites based in the United States.²⁰ The simple act of posting software to the Internet (or otherwise publishing source code) was considered an export, creating substantial legal hurdles for any individual or company that wished to sell products containing strong encryption abroad, or even make them freely available.

ENCRYPTION SOURCE CODE AS A WEAPON

"For the past two decades or more, a major goal of U.S. cryptography policy... has been to prevent strong mass-market cryptography from becoming widely available abroad, with export controls being the primary tool used to achieve this end."

- Michael Fromkin, "It Came from Planet Clipper" (1996)

Because they had historically been used by military and intelligence agencies almost exclusively, cryptographic tools were originally classified as munitions. Prior to 1996, all products using encryption were controlled under the International Traffic in Arms Regulations (ITAR) and listed on the U.S. Munitions List (USML).²¹ Products with strong encryption were considered "dual use" technologies, meaning that they had both civilian and military applications, akin to nuclear technology or chemicals that could be weaponized. The export controls were based on the strength of the encryption — that is, the cryptographic key length²² — and applied not only to hardware but also to encryption software and source code. In 1994, for example, products with "strong encryption" were those with key lengths greater

than 40 bits.¹²³ Under the ITAR regime, most applications to export cryptographic software with longer keys would be denied, although the restrictions were more lax when it came to “special” categories of applications like those that protected financial information.¹²⁴ Notably, the restrictions did not prevent people from sending encrypted messages abroad, but they prohibited the export of tools that provided the means to encrypt and decrypt those messages.

By the mid-1990s, as commercial use of encryption was taking off, the place of these tools on the USML became increasingly difficult to justify. Yet the U.S. government had a strong incentive to maintain strict encryption export controls. Limiting the ability of American companies to sell certain cryptographic products in foreign markets allowed the government to delay the spread and adoption of strong encryption technology abroad, which many officials feared could reduce their ability to gather intelligence on foreign targets.¹²⁵ Big companies like Apple, Microsoft, and Lotus knew that they often could not get licenses to sell strong cryptography overseas, so they were forced to make separate versions of their products for foreign markets. In these products, the encryption features were either stripped out entirely or relied on a weaker, “export-grade” version that was easier to crack. Journalist Steven Levy described export-grade encryption as “crypto lite”: it was “strong enough to protect communications from casual intruders but not from the [g]overnment itself.”¹²⁶ Or, as EFF put it in a 1997 bulletin, “the government has limited the key size of encryption to be exported to that which the NSA could crack.”¹²⁷

The implications of such a policy on the development of the worldwide cryptographic market were far-reaching. As a report by EPIC explained, export controls could reduce or weaken the availability of encryption in common programs, make it difficult to develop international encryption standards and build interoperable programs, and weaken the security of the Internet overall by forcing the development of local encryption alternatives that may not have gone through extensive peer review.¹²⁸

Although export controls are generally not meant to have a direct impact on domestic economic activity — they are, after all, aimed at foreign sales — the encryption restrictions had broader consequences as well. By requiring American companies to seek approval

before exporting cryptographic technologies, the U.S. government could continue to monitor and indirectly influence the development of commercial cryptography. The government could decide, for example, that it looked favorably on licenses for a particular tool or algorithm (perhaps, one might cynically suggest, because they already knew how to crack it) and thus create an incentive for U.S. companies to integrate that tool into their products instead of another method for which it might be harder to obtain a license. And while some large companies had enough of a business interest to produce different domestic and export versions of their products, for many it was too costly. Consequently, preventing the export of strong cryptography could actually restrict domestic use, forcing customers inside the United States to use the same weaker, export-grade cryptography that was required for foreign products.¹²⁹

THE CAMPAIGN FOR CRYPTO WITHOUT BORDERS

By the mid-1990s, industry opposition to these restrictions had grown fairly strong. The computer industry argued that encryption export controls hampered technological development because the policies forced them to develop two distinct products for every piece of software — one for domestic use, and another for foreign consumption.¹³⁰ In the long term, business analysts also worried that the restrictions would hinder the American tech industry’s overall competitiveness, given increasing demand for strong cryptography overseas as e-commerce spread and the development of foreign encryption alternatives expanded. A report from the U.S. Department of Commerce and the National Security Agency in 1996 acknowledged that some American businesses “believe that not being able to participate at the early stage of market development will be a tremendous obstacle to their future international competitiveness” and predicted that “export sales could increase significantly if allowed to export stronger algorithms — some by orders of magnitude.”¹³¹

A separate study by the Economic Strategy Institute in 1998 translated the predictions into specific numbers, projecting anywhere between \$35 billion and \$95 billion in losses over the next five years as a result of encryption export controls.¹³² “The record shows that these controls have had no discernible impact on national security, but have demonstrably compromised America’s economic

security,” the report concluded. “Foreign encryption products are present in the free international market, their competitiveness is increasing at the expense of American companies, and their products are outside U.S. regulatory authority. In this light, export controls are indefensible.”¹³³

Overall, the economic stakes were clear: encryption export controls were hurting U.S. businesses and undermining America’s economic interests.

*“Prohibiting the use of a particular form of cryptography for the express purpose of making communication intelligible to law enforcement officers is akin to prohibiting someone from speaking a language not understood by law enforcement officers.”*¹³⁴

- Shari Steele and Danny Weitzner (1996)

Export controls were also being legally challenged through a series of court cases which focused on the question of whether encryption source code should be recognized as “speech” subject to the protections of the First Amendment. The challenges mounted by Daniel Bernstein¹³⁵ and Phil Karn¹³⁶ in the mid-1990s — along with a third case, *Junge v. Daley*¹³⁷ — were premised on the argument that if code was speech, requiring an individual to register and obtain a license to publish code outside of the United States was an unconstitutional prior restraint on that speech.

Although two of the three cases were resolved much later — and with mixed rulings¹³⁸ — the debate about whether software code was speech shed light on some of the broader civil liberties issues at stake. As EFF’s John Gilmore explained in an interview in 1994:

There’s a whole continuum between a book about cryptography, a book listing source code, an on-line copy of that book, a piece of actual source code, a piece of binary code stored on diskette, a piece of binary code loaded into a general-purpose computer, and a machine that does nothing but encoding and decoding. Somewhere along that continuum, you go from having full rights to anything you want, to having no export rights. It’s not clear where the line should be drawn. The government benefits from leaving

this line fuzzy, since people who actually have the right to export are afraid that they don’t, and don’t do it.¹³⁹

Beyond the free speech issues, encryption export controls raised significant privacy questions. Many of the concerns voiced by privacy advocates were quite similar to those brought up in the domestic Clipper Chip debate (which we describe in the previous section of this paper) but a few were unique to the export controls conflict. In particular, some argued that restrictions on the export of encryption worldwide effectively created two different standards for privacy, providing a higher degree of protection for communications between Americans within the United States. This essentially meant that the Fourth Amendment right to be secure in one’s digital “papers and effects” stopped at the U.S. border, even for American citizens communicating with colleagues and loved ones abroad.¹⁴⁰ These concerns were exacerbated by the fact that there had been several high-profile demonstrations of how easy it had become to crack export-grade crypto by the late 1990s.¹⁴¹

Finally, a growing body of evidence suggested that by the end of the twentieth century, encryption export controls were no longer very effective at stopping the spread of strong encryption overseas. “Strong cryptography only gets easier to implement — and harder to regulate — over time,” wrote Ron Rivest, one of the developers of the RSA algorithm, in 1998.¹⁴² 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.¹⁴³ Furthermore, the report found that on average the quality of the foreign encryption products was comparable to those built in the United States.¹⁴⁴ As Alan Davidson, a staff attorney at the Center for Democracy and Technology, explained to Congress, “world-class strong cryptography is now widely available outside the United States. The result is that criminals, terrorist organizations, and rogue governments all have access to the strongest encryption, while law-abiding individuals around the world still do not have strong encryption in the mass-market products they use.”¹⁴⁵ The logic of Davidson’s argument echoed the famous statement by Phil Zimmermann in his explanation of why he created PGP: “If privacy is outlawed, only outlaws will have privacy.”¹⁴⁶

FROM WEAKENING CRYPTO TO WEAKENED RESTRICTIONS: THE LIBERALIZATION PROCESS

"The vigorous application of cryptography may also improve national security: the encryption of communications, for example, protects U.S. businesses from industrial espionage. Paradoxically, we may create a safer society by promoting a technology that somewhat hampers law enforcement."

- Ronald Rivest, "The Case Against Regulating Encryption Technology" (1998)

In the fall of 1996, the Clinton Administration took a small but significant first step toward recognizing the challenges that export controls presented for the spread of commercial encryption products. Vice President Al Gore, who had championed the Clipper Chip just a few years earlier, delivered the news on October 1, 1996, as part of a broader encryption-related initiative. In a statement, Gore acknowledged the value of encryption in protecting privacy and enabling secure online transactions, as well as the overall benefits to Internet security and American competitiveness in the technology sector:

The Administration's initiative will make it easier for Americans to use stronger encryption products — whether at home or abroad — to protect their privacy, intellectual property, and other valuable information. It will support the growth of electronic commerce, increase the security of the global information, and sustain the economic competitiveness of U.S. encryption product manufacturers during the transition to a key management infrastructure.¹⁴⁷

Gore went on to describe a temporary relaxation of export controls as "part of a broader encryption policy effort designed to promote electronic information security and public safety." The change meant that commercial encryption products would no longer be considered munitions, and would instead become part of the more extensive push by the administration to implement commercial key recovery legislation. He described the policy change as "broadly consistent with the recent recommendations of the National Research Council"¹⁴⁸ and suggested that it addressed "many of the objectives of pending Congressional legislation."

Six weeks later, the White House issued Executive Order 13026, which officially transferred the control of the export of non-military encryption items on the USML from the Department of State to the Department of Commerce's Export Administration Regulations (EAR) and placed them on the Commerce Control List (CCL).¹⁴⁹ Commerce created a new category of foreign policy and national security controls for "encryption items" (EI), which would allow the commercial distribution of several classes of software, including products used in financial transactions, encryption software that employed key lengths of less than 64 bits, and retail products exported to individual consumers.¹⁵⁰ The shift was generally met with support by privacy advocates and companies alike, who saw this as a first step in a broader liberalization of encryption export controls. But because these items still required a license — and because they came as part of a broader effort to implement key recovery proposals — the change left a number of the concerns expressed by industry, civil liberties advocates, and technical experts unresolved.¹⁵¹

"Only 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."

- Representative Bob Goodlatte (1999)

Around the same time that the Clinton Administration was tentatively taking its first steps toward liberalization, a broader legislative effort — which Vice President Gore referred to in his October 1996 speech — was underway to shift U.S. policy more dramatically in the direction of a positive encryption agenda. Representative Bob Goodlatte first introduced the Security and Freedom Through Encryption (SAFE) Act in Congress in March 1996. The bill's overall goal was simple: "to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption."¹⁵² It aimed to prevent the government from creating a mandatory key-escrow system¹⁵³ and remove export restrictions on most encryption, including lifting the existing limits on key length.¹⁵⁴ Multiple versions of the legislation were re-introduced in the House and Senate throughout the late 1990s. Eventually, the SAFE Act garnered sponsorship from a majority of the members of the House of Representatives — 258, to be exact — reflecting a broad and bipartisan consensus on the importance of

promoting and protecting access to strong encryption tools. A similar effort was undertaken by Senator Conrad Burns in the Pro-CODE Act (which we describe in Part II).

With the pressure to relax encryption export controls growing on the Hill, in the courts, and in the court of public opinion, a vigorous debate was underway within the Clinton Administration in 1997 and 1998 about how to adapt while still protecting the interests of law enforcement. In September 1998, after “several months of intensive dialogue between the government and U.S. industry, the law enforcement community and privacy groups,” Vice President Gore announced additional concessions relating to the export of strong encryption for purposes like financial transactions, electronic banking, and health records.¹⁵⁵ Under the new policy, hardware and software products containing 56-bit encryption could be exported without a license, and the requirement that companies submit key recovery plans in exchange for permission export those products was removed.¹⁵⁶ But as a CNET reporter described it, “The plan announced today continues the administration’s piecemeal strategy of easing some of the export controls without fully lifting the limits as many high-tech companies and civil liberties groups would like.”¹⁵⁷ They continued to fight for more significant export control relief.

In August 1999, the President’s Export Council Subcommittee on Encryption¹⁵⁸ made a number of more aggressive recommendations related to revising encryption export regulations, including raising the key length limit for mass market hardware and software to 128 bits, which had become the standard for electronic commerce at that point. The report was unequivocal in its arguments that,

The U.S. government should recognize market realities... [and] the difficulty of controlling mass-market products once they are allowed to be exported even to limited sectors. Furthermore, mass-market products play an important role in protecting the communications and data of individuals—a segment of the encryption user community that has been neglected in recent liberalizations to the U.S. export policy.¹⁵⁹

Shortly thereafter, on September 16, 1999, the White House made a major announcement: in the coming months, it would update its encryption policies to remove

virtually all restrictions on the export of retail encryption products, regardless of key length.¹⁶⁰ The government’s intent was to “significantly update and simplify export controls on encryption,” and it emphasized that, “The updated guidelines will allow U.S. companies new opportunities to sell their products to most end users in global markets.” Guidance published by the Commerce Department that same day offered additional details, including the fact that they would continue to restrict exports to sanctioned countries and foreign government and military end users.¹⁶¹

The announcement caught many encryption advocates by surprise, but they nonetheless quickly leapt to support it. *The New York Times* called the new policy change a “reversal,” declaring: “Bucking pressure from the Justice Department, the F.B.I. and intelligence agencies, the White House yesterday essentially eliminated its complex controls on the export of data-scrambling hardware and software, handing a surprise victory to Congressional, high-technology and privacy groups that have spent years fighting for the change.”¹⁶²

Representative Bob Goodlatte, who had championed the SAFE Act for a number of years, called it “huge news” and a “tremendous victory.”¹⁶³ As Steven Levy put it succinctly: “It was official: public crypto was our friend.”¹⁶⁴

The following January, the Commerce Department officially released the revised regulations, which amended the EAR “to allow the export and reexport of any encryption commodity or software to individuals, commercial firms, and other non-government end-users in all destinations.”¹⁶⁵ Although a handful of prohibitions remained in place, the change swept away the vast majority of the restrictions that had been the focus of the debate in the previous decade.

One of the key steps in this liberalization process was the creation of an exemption for the export of free and open source cryptography. The January 2000 changes made “unrestricted encryption source code” exportable under License Exception TSU, which covers a range of generally available and mass-market technology and software.¹⁶⁶ This eliminated the ambiguity surrounding the export of products like PGP, removing them from legal limbo in which it was uncertain whether they met the criteria included in the free and open source exemption.

Although the truce declared at the end of 1999 took many encryption proponents by surprise,¹⁶⁷ both industry and civil liberties advocates got virtually everything for which they had asked. As Rubinstein and Hintze summarize, American “export policy [had] evolved from case-by-case licensing of individual encryption exports, to policies designed to encourage ‘key escrow’ or ‘key recovery’ encryption systems, to broad approvals for exports to certain preferred industry sectors, and finally to nearly free exportability of most products.”¹⁶⁸

After the last shots had been fired, the Crypto Wars ended with a broad policy consensus: ensuring Americans’ ability to use and distribute strong encryption free of government backdoors was critical to maintaining the nation’s economic security and information security, as well as maintaining Americans’ constitutional rights to privacy and free speech.

IV. POST-WAR: HOW THE CRYPTO WARRIORS WERE PROVEN RIGHT

The Crypto Wars of the 1990s offer a compelling tale about the convergence of technical experts, business interests, civil liberties advocates, and political leaders to articulate why encryption benefits Internet security, the information economy, and civil liberties. In the decades since the conflict ended, many of the crypto warriors' predictions have been proven right, while new arguments in favor of strong encryption have also emerged as the technology continues to change.

THE INTERNET AND THE INFORMATION ECONOMY HAVE GROWN EXPONENTIALLY SINCE THE CRYPTO WARS

The resolution of Crypto Wars in favor of robust encryption for everyone played a significant role in jumpstarting the nascent Internet economy in the early 21st century. In 1996, the National Research Council wrote that it was "widely believed that encryption [would] be broadly adopted and embedded in most electronic communications products and applications for handling potentially valuable data."¹⁶⁹ Just as they predicted, the late 1990s and early 2000s witnessed the emergence of a vibrant marketplace of new Internet services based on secure digital communications and the widespread migration of sensitive communications online. Many of the major titans of the Internet economy were founded in the five-year period immediately following the demise of the Clipper Chip proposal, including Ebay, Paypal, and Amazon. Their business models depended on their customers' ability to conduct secure transactions online and to trust that connections advertised as secure actually were.¹⁷⁰ Indeed, since the Crypto Wars ended, electronic commerce in the United States has risen steadily.¹⁷¹

One of the most important protocols to emerge during this period was the Secure Sockets Layer (SSL) specification, which eventually became "the secure communications protocol of choice for a large part of the Internet community."¹⁷² SSL and its successor, Transport Layer Security (TLS), rely on encryption to provide, among other things, secure connections between Internet browsers and the websites with which they communicate.¹⁷³ The Secure Shell Protocol (SSH), although lesser known, quickly became an equally indispensable tool for remotely administering large numbers of servers — an essential prerequisite for the rise of the modern data-center.¹⁷⁴ At the same time as these protocols were being refined, entirely new industries were being formed to both support and leverage the new ecosystem of secure digital communications. Companies like VeriSign¹⁷⁵ (a spinoff of RSA Security) and Comodo¹⁷⁶ were formed to manage public key infrastructure, issuing the digital certificates used for encryption. Their products provide independent verification to consumers that the secure sites they are visiting have not been tampered with and are not being impersonated by malicious actors. In addition to bolstering consumer confidence, the added protection provided by encryption also prevents a substantial number of real attacks that would otherwise be extremely easy to carry out.

In the early 21st century, the emergence of these foundational technologies allowed the encrypted web to expand rapidly to include electronic banking, electronic medical records systems, online bill payment tools, home automation systems, e-filing systems for taxes, and VPNs. Additionally, SSL was embedded in a huge number of physical products, including smartphones, home routers, and media streaming devices — products and services that now represent billion dollar industries unto themselves. Those who argued during the Crypto Wars that encryption would be a foundational technology for the growth of the digital economy have undeniably been proven right.

STRONG ENCRYPTION HAS BECOME A BEDROCK TECHNOLOGY THAT PROTECTS THE SECURITY OF THE INTERNET

The evolution of the ecosystem for encrypted communications has also enhanced the protection of individual communications and improved cybersecurity. Today, strong encryption is an essential ingredient in the overall security of the modern network, and adopting technologies like HTTPS is increasingly considered an industry best-practice among major technology companies.¹⁷⁷ Even the report of the President's Review Group on Intelligence and Communications Technologies, the panel of experts appointed by President Barack Obama to review the NSA's surveillance activities after the 2013 Snowden leaks, was unequivocal in its emphasis on the importance of strong encryption to protect data in transit and at rest. The Review Group wrote that:

Encryption is an essential basis for trust on the Internet; without such trust, valuable communications would not be possible. For the entire system to work, encryption software itself must be trustworthy. Users of encryption must be confident, and justifiably confident, that only those people they designate can decrypt their data.... Indeed, in light of the massive increase in cyber-crime and intellectual property theft on-line, the use of encryption should be greatly expanded to protect not only data in transit, but also data at rest on networks, in storage, and in the cloud.¹⁷⁸

The report further recommended that the U.S. government should:

Promote security[] by (1) fully supporting and not undermining efforts to create encryption standards; (2) making clear that it will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption; and (3) supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.¹⁷⁹

Moreover, there is now a significant body of evidence that, as Bob Goodlatte argued back in 1997, “Strong encryption

prevents crime.”¹⁸⁰ This has become particularly true as smartphones and other personal devices that store vast amount of user data have risen in popularity over the past decade. Encryption can stop or mitigate the damage from crimes like identity theft and fraud targeted at smartphone users.¹⁸¹

Meanwhile, recent incidents have confirmed the dangers of promoting policies that weaken encryption. In March 2015, a team of researchers discovered a bug that “for more than a decade has made it possible for attackers to decrypt HTTPS-protected traffic passing between Android or Apple devices and hundreds of thousands or millions of websites.”¹⁸² The researchers called it a “FREAK” attack, which stands for “Factoring attack on RSA-EXPORT Keys,” a deliberate reference to the export-grade encryption that was developed by some companies in the 1990s to comply with encryption export controls. An attack occurs when an attacker forces a vulnerable browser to use weak 512-bit RSA keys,¹⁸³ which can now be cracked in a matter of hours, and then steals passwords and other personal information.¹⁸⁴ Although most engineers abandoned the use of export-grade keys after export controls were liberalized, it appears that this functionality continued to exist, largely unnoticed, in certain devices and servers for decades.¹⁸⁵ In May 2015, researchers uncovered a similar type of attack called Logjam which exploits a weakness in TLS to downgrade encryption keys to weaker export-grade key lengths.¹⁸⁶ In both the FREAK and Logjam cases, the vulnerabilities were a direct result of the decision to split functionality into domestic grade and export-grade encryption. The attacks serve as a powerful reminder about the vulnerabilities that may be created by policies that restrict the export of strong encryption.

STRONG ENCRYPTION HAS BECOME AN INTEGRAL TOOL IN THE PROTECTION OF PRIVACY AND THE PROMOTION OF FREE EXPRESSION ONLINE

The end of the Crypto Wars ushered in an age where the security and privacy protections afforded by the use of strong encryption also help promote free expression. As the American Civil Liberties Union recently explained in a submission to the UN Human Rights Council, “encryption and anonymity are the modern safeguards for free expression. Without them, online communications are effectively unprotected as they traverse the Internet, vulnerable to interception and review in bulk.

Encryption makes mass surveillance significantly more costly.”⁸⁷

The human rights benefits of strong encryption have undoubtedly become more evident since the end of the Crypto Wars. Support for strong encryption has become an integral part of American foreign policy related to Internet freedom, and since 2010, the U.S. government has built up a successful policy and programming agenda based on promoting an open and free Internet.⁸⁸ These efforts include providing over \$120 million in funding for “groups working to advance Internet freedom,” much of which specifically funds circumvention tools that rely on strong encryption — which makes Internet censorship significantly harder — as part of the underlying technology.⁸⁹ Similarly, a June 2015 report by David Kaye, the UN Special Rapporteur for Freedom of Expression and Opinion found that, “Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks.”⁹⁰ The report goes on to urge all states to protect and promote the use of strong encryption, and not to restrict it in any way.

Over the past fifteen years, a virtuous cycle between strong encryption, economic growth, and support for free expression online has evolved. Some experts have dubbed this phenomenon “collateral freedom,” which refers to the fact that, “When crucial business activity is inseparable from Internet freedom, the prospects for Internet freedom improve.”⁹¹ Free expression and support for human rights have certainly benefited from the rapid expansion of encryption in the past two decades.

THE ORGANIZING EFFORTS CARRIED OUT IN SUPPORT OF INTERNET OPENNESS DURING THE CRYPTO WARS HAVE HELPED SHAPE MODERN INTERNET ADVOCACY CAMPAIGNS

It is important to remember that the successful resolution of the Crypto Wars was neither a foregone conclusion nor a happy accident of aligned interests. Advocates worked tirelessly to build a strong case in favor of the benefits of encryption, bringing together technical experts alongside a broad coalition of privacy advocates and companies to engage in a coordinated effort of public education and targeted lobbying. They also worked closely with

members of Congress, building support across the political spectrum through organizations like the non-profit Internet Caucus Advisory Committee⁹² and the Americans for Computer Privacy.⁹³

The success of this campaign during the Crypto Wars has informed a number of subsequent advocacy campaigns, including the Internet blackout and coordinated protests that stopped the 2012 Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) as well as the months-long push to get the Federal Communications Commission to adopt strong net neutrality rules after the 2014 Verizon v. FCC court decision. Organizers of both the SOPA/PIPA and net neutrality campaigns employed a number of similar tactics to convince policymakers to heed their advice, bringing together broad coalitions of stakeholders from both the public interest and the private sector and emphasizing the technical, legal, and economic impacts of the decisions at hand.⁹⁴ Thus, history has not only validated the substance of the crypto warriors’ arguments, but also confirmed the wisdom of their strategy — one that may need to be implemented again as new threats to encryption are on the rise.

CONCLUSION: ENCRYPTION UNDER THREAT... AGAIN

Unfortunately, in the past few years the consensus that strong encryption is good for security, liberty, and economic growth has come under threat. The June 2013 revelations about the U.S. National Security Agency's pervasive surveillance programs — not to mention the NSA's direct attempts to thwart Internet security to facilitate its own spying — dramatically shifted the national conversation, highlighting the vulnerabilities in many of the tools and networks on which we now rely for both everyday and sensitive communications. While ordinary individuals, civil liberties advocates, and major technology companies have since embraced greater use of encryption as a necessary step to address a wide range of modern threats from both government and nongovernment actors, intelligence agencies and law enforcement officials have also become increasingly outspoken against measures to strengthen these systems through encryption. To make their case, they have revived many of the arguments they made about encryption in the 1990s, seeming to have forgotten the lessons of the past. In response, encryption proponents have countered with many of the same arguments that they made in the 1990s, along with a few new ones.⁹⁵

It seems like we may once again be on the verge of another war: a Crypto War 2.0. But it would be far wiser to maintain the peace than to begin a new and unnecessary conflict. We already had a robust public debate that resolved this dispute, and nothing has changed since the 1990s that would cast doubt on the policy conclusions we reached then; indeed, the post-war period has only reinforced those conclusions. Although there are numerous individual lessons from the Crypto Wars, the overarching takeaway is that weakening or otherwise undermining encryption is bad for our economy, our economic security, and our civil liberties — and there is no reason to repeat our previous mistakes.

ENDNOTES

1. Craig Timberg, "Apple will no longer unlock most iPhones, iPads for police, even with search warrants," *The Washington Post*, September 18, 2014, http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718ede9b2f_story.html (accessed June 15, 2015); Craig Timberg, "Newst Androids will join iPhones in offering default encryption, blocking police," *The Washington Post*, September 18, 2014, <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/> (accessed June 15, 2015).
2. Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cybersecurity," *New America's Open Technology Institute*, July 2014, https://static.newamerica.org/attachments/184-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-and-cybersecurity/Surveillance_Costs_Final.pdf (accessed June 15, 2015).
3. End-to-end encryption is a system in which "messages are encrypted in a way that allows only the unique recipient of a message to decrypt it, and not anyone in between." With end-to-end encryption, you encrypt the contents of a message on your local machine or device. That data is then transmitted as ciphertext by the email provider to the intended recipient, who is the only person who can decrypt and read it. Danielle Kehl, "Encryption 101," *Slate*, February 24, 2015, http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html (accessed June 15, 2015).
4. Andy Greenberg, "Whatsapp Just Switched On End-to-End Encryption for Hundreds of Millions of Users," *Wired*, November 18, 2014, <http://www.wired.com/2014/11/whatsapp-encrypted-messaging/> (accessed June 15, 2015); Andrea Peterson, "Yahoo's plan to get Mail users to encrypt their e-mail: Make it simple," *The Washington Post*, March 15, 2015, <http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/15/yahoos-plan-to-get-mail-users-to-encrypt-their-e-mail-make-it-simple/> (accessed June 15, 2015).
5. Craig Timberg and Greg Miller, "FBI blasts Apple, Google for locking police out of phones," *The Washington Post*, September 25, 2014, http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html (accessed June 15, 2015); "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *The Brookings Institution*, October 16, 2015, event recording available at <http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi> (accessed June 15, 2015); Cyrus Vance Jr., "Apple and Google threaten public safety with default smartphone encryption," *The Washington Post*, September 26, 2014, http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphoneencryption/2014/09/25/43af9bfo-44ab-11e4-b437-1a7368204804_story.html (accessed June 15, 2015).
6. David E. Sanger and Matt Apuzzo, "James Comey, FBI Director, Hints at Action as Cell Phone Data is Locked," *The New York Times*, October 16, 2014, http://www.nytimes.com/2014/10/17/us/politics/fbi-director-in-policy-speech-calls-dark-devices-hindrance-to-crime-solving.html?_r=1 (accessed June 15, 2015); "FBI Director Continues Crusade Against Encryption, Calls on Congress to Act," *The District Sentinel*, March 25, 2015, <https://www.districtsentinel.com/fbi-director-continues-crusade-against-encryption-calls-on-congress-to-act/> (accessed June 15, 2015).
7. Craig Timberg, "Holder urges tech companies to leave device backdoors open for police," *The Washington Post*, September 30, 2014, <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/30/holder-urges-tech-companies-to-leave-device-backdoors-open-for-police/> (accessed June 15, 2015).
8. Ellen Nakashima and Barton Gellman, "As encryption spreads, U.S. grapples with clash between privacy, security," *The Washington Post*, April 10, 2015, 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 (accessed June 15, 2015); "VIDEO: ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute," *Office of the Director of National Intelligence: IC on the Record*, February 4, 2015, <http://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on> (accessed June 15, 2015).
9. For a fairly comprehensive list of articles and new stories, see Andi Wilson, "Updated #Cryptodebate Bibliography," *New America's Open Technology Institute*, June 16, 2015, <http://www.newamerica.org/oti/updated-cryptodebate-bibliography/>. For specific discussions of the

- technical feasibility see, e.g., Jeffrey Vagle and Matt Blaze, "Security 'Front Doors' vs. 'backdoors': A Distinction Without a Difference," *Just Security*, October 17, 2014, <http://justsecurity.org/16503/security-front-doors-vs-back-doors-distinction-difference/> (accessed June 15, 2015); Bruce Schneier, "Stop the hysteria over Apple encryption," *CNN*, October 31, 2014, <http://www.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/index.html> (accessed June 15, 2015); Tim Greene, "RSA: Panel calls NSA access to encryption keys a bad idea," *Network World*, April 22, 2015, <http://www.networkworld.com/article/2913280/security/rsa-panel-calls-nsa-access-to-encryption-keys-a-bad-idea.html> (accessed June 15, 2015); Joseph Lorenzo Hall, "The NSA's Split-Key Encryption Proposal is Not Serious," *Center for Democracy & Technology*, April 20, 2015, <https://cdt.org/blog/the-nsas-split-key-encryption-proposal-is-not-serious/> (accessed June 15, 2015); Andrea Peterson, "Congressman with computer science degree: Encryption back-doors are 'technologically stupid,'" *The Washington Post*, April 30, 2015, <http://www.washingtonpost.com/blogs/the-switch/wp/2015/04/30/congressman-with-computer-science-degree-encryption-back-doors-are-technologically-stupid/> (accessed June 15, 2015).
10. Julian Sanchez, "Old Technopanic in New Bottles," *Cato at Liberty*, September 23, 2014, <http://www.cato.org/blog/old-technopanic-new-bottles> (accessed June 15, 2015);
 11. For a succinct look back on the debate, see Matt Blaze, "Key Escrow from a Safe Distance: Looking Back at the Clipper Chip," *University of Pennsylvania*, December 2011, <http://www.crypto.com/papers/escrow-acscac11.pdf> (accessed June 15, 2015).
 12. A good source for historical information is David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (Scribner: 1996). See also "Statement of Cindy A. Cohn, Testimony on Encryption as Constitutionally Protected Speech," before the Senate Judiciary Committee's Subcommittee on Constitution, Federalism and Property Rights, Washington, D.C., March 17, 1998, available at <http://gos.sbc.edu/c/cohn.html> (accessed June 15, 2015).
 13. Kahn, *The Codebreakers*.
 14. "History of Encryption," *The SANS Institute*, 2001, available at <http://www.sans.org/reading-room/whitepapers/vpms/history-encryption-730> (accessed June 15, 2015).
 15. "Encryption is an essential tool in providing security in the information age. Encryption is based on the use of mathematical procedures to scramble data so that it is extremely difficult — if not virtually impossible — for anyone other than authorized recipients to recover the original 'plaintext.' Properly implemented encryption allows sensitive information to be stored on insecure computers or transmitted across insecure networks." Hal Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 1997, available at <https://www.schneier.com/paper-key-escrow.pdf> (accessed June 15, 2015). For a simple explanation of how encryption works to protect online security today, see Kehl, "Encryption 101," *Slate*, February 24, 2015.
 16. "History of Encryption."
 17. Also sometimes called the Diffie-Hellman key exchange.
 18. Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, Nov. 6, November 1976, <http://www.cs.tau.ac.il/~bchor/diffie-hellman.pdf> (accessed June 15, 2015). It was later called the Diffie-Hellman Key Exchange.
 19. Keith Palmgren, "Diffie-Hellman Key Exchange: A Non-mathematician's explanation," *ISSA: The Global Voice of Information Security*, October 2006, available at http://academic.regis.edu/cias/1a/Palmgren_-_Diffie-Hellman_Key_Exchange.pdf (accessed June 15, 2015).
 20. Steven Levy, *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age* (New York: Penguin Books, 2002), 71.
 21. Peter Wayner, "A Patent Falls, and the Internet Dances," *New York Times*, September 6, 1997, <https://www.ics.ucl.edu/~ics54/doc/security/pkhistory.html> (accessed June 15, 2015). ("Before public key cryptography, anyone who wanted to use a secret code needed to arrange for both sides to have a copy of the key used to scramble the data, a problem that requires either trusted couriers or advance meetings. PKC, as it is sometimes known, erased this problem by making it possible for two people, or more properly their computers, to agree upon a key by performing some complicated mathematics. There is no publicly known way for an eavesdropper to pick up the key by listening in.")

22. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Crypto Systems," *Massachusetts Institute of Technology*, April 4, 1977, available at <http://people.csail.mit.edu/rivest/Rsapaper.pdf> (accessed June 15, 2015). ("The era of "electronic mail" may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are private, and (b) messages can be signed. We demonstrate in this paper how to build these capabilities into an electronic mail system.")
23. *Ibid.*, 2
24. Jay Stowsky, "Secrets or Shields to Share? New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age," UCAIS Berkeley Roundtable on the International Economy, Working Paper Series, February 21, 2003, available at <http://econpapers.repec.org/paper/cdlucbrle/q18974908.htm> (accessed June 15, 2015).
25. Levy, *Crypto*, 130.
26. Other factors included the increased use of portable and mobile devices (which meant that sensitive data was being sent or carried to a wide variety of locations, including on media that could be lost or stolen easily) and the increased use of public and wireless networks.
27. Lotus Corporation's groupware products required built-in encryption systems to "ensure the confidentiality of the electronic messages that Lotus Notes' major corporate users would exchange by the thousands across computer networks." Stowsky, "Secrets or Shields to Share?"
28. Levy, *Crypto*, 149-125; Stowsky, "Secrets or Shields to Share?"
29. Stowsky, "Secrets or Shields to Share?"
30. Zimmermann, "Why I Wrote PGP."
31. *Ibid.*
32. Levy, *Crypto*, 106-107.
33. Henry Corrigan-Gibbs, "Keeping Secrets," *Stanford Magazine*, November/December 2014, available at <http://www.henrycg.com/files/academic/papers/stanfordmag14keeping.pdf> (accessed June 15, 2015).
34. Stowsky, "Secrets or Shields to Share?"
35. One of the primary ways that the U.S. government could exert control over the development of cryptographic standards was through limits on funding for academics working in cryptography. Many academics received funding from organizations like the National Science Foundation (NSF), which would send research proposals about encryption technology to the NSA.
36. John Markoff, "Paper on Codes Is Sent Despite U.S. Objections," *The New York Times*, August 9, 1989, <http://www.nytimes.com/1989/08/09/us/paper-on-codes-is-sent-despite-us-objections.html> (accessed June 15, 2015). ("Over the past 12 years the National Security Agency has consistently opposed the publication or transmission of research on encryption technology. The agency is concerned that advances in cryptography will make it harder to break coded transmissions sent by foreign intelligence agents in the United States to their governments.")
37. Section 2201 of S. 266, The Comprehensive Counter-Terrorism Act of 1991, available at https://w2.eff.org/Privacy/Surveillance/7f-s266_91.comments.txt (accessed June 15, 2015). A few months later, after an outpouring of backlash from civil liberties groups, Biden quietly withdrew the bill. Levy, *Crypto*, 198.
38. Levy, *Crypto*, 228.
39. "Statement by the Press Secretary," *The White House*, April 16, 1993, available at https://www.epic.org/crypto/clipper/white_house_statement_4_93.html ("1993 WH Clipper Chip Announcement") (accessed June 15, 2015).
40. A. Michael Froomkin, "It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow," *Chicago Legal Forum Law of Cyberspace* (1996), available at http://osaka.law.miami.edu/~froomkin/articles/planet_clipper.htm (accessed June 15, 2015).

41. 1993 WH Clipper Chip Announcement.
42. *Ibid.*
43. Levy, *Crypto*, 249.
44. Froomkin, "It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow."
45. Skipjack was viewed as stronger than the most popular alternative, the Data Encryption Standard (DES). DES is a symmetric key encryption algorithm that was designed by IBM researchers in the early 1970s. When the U.S. government made it a Federal Information Processing Standard in 1977, DES became the algorithm of choice for the encryption of commercial and sensitive yet unclassified government computer data. Many industries, like financial services and banking, quickly adopted DES to protect their sensitive data. The design of DES keys limits their length to an effective 56-bits, which some researchers felt wasn't adequately secure. Some are suspicious that the National Security Agency weakened IBM's original algorithm, reducing it from 112-bits to 56. Even so, DES was revised and adopted as federal standard again three more times (in 1983, 1988, and 1993) before it was withdrawn as a standard. Skipjack, the algorithm selected for use in the Clipper Chip, was also symmetric but it had an 80-bit key which made it significantly more secure than the DES algorithm. As a result of this increased key length, Skipjack encryption has 2^{80} possible keys, compared to DES's 2^{56} possible keys. This made it much less feasible to perform an exhaustive (brute-force) search for the key used to secure a particular communication.
46. Ernest F. Brickell, Dorothy E. Denning, Stephen T. Kent, David P. Maher, and Walter Tuchman, "Skipjack Review Interim Report," July 28, 1993, available at <http://faculty.nps.edu/dedenin/publications/SkipjackReview.txt> (accessed June 15, 2015).
47. The Law Enforcement Access Field (LEAF) was the core component of a novel specification for allowing easy — though theoretically restricted — third-party access to communication systems that were otherwise secured with strong crypto. Every device that made up a LEAF-equipped "secure" communications system had the digital equivalent of a skeleton key, which could be used to access anything that particular device ever sent. Specifically, this meant that every communication was required to begin with the transmission of a LEAF message, which would contain the ID number of the originating device, along with an encrypted copy of the "session key" used to encipher the rest of the communication. The skeleton key for any given device (literally just another cryptographic key) would grant access to any session key that the device had ever generated.
48. Levy, *Crypto*, 249-253.
49. Brickell et al., "Skipjack Review Interim Report."
50. See, e.g., Dorothy E. Denning, "Concerning Hackers Who Break Into Computer Systems," presented at the 13th National Security Conference in Washington DC, October 1-4, 1990, available at http://cpsr.org/prevsite/cpsr/privacy/crime/denning_hackers.html/ (accessed June 15, 2015).
51. Steven Levy, "Clipper Chick," *Wired*, September 1996, http://archive.wired.com/wired/archive/4.09/denning_pr.html; Dorothy E. Denning, "The Case for Clipper (Clipper Chip offers escrowed encryption)," *MIT's Technology Review*, July 1995, available at http://encryption.policies.tripod.com/us/denning_0795_clipper.htm (accessed June 15, 2015).
52. Denning, "The Case for Clipper."
53. Brickell et al., "Skipjack Review Interim Report."
54. Whitfield Diffie and Susan Eva Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption, Updated and Expanded Edition* (Cambridge, MA: MIT Press, 2010), 236.
55. Steven Levy, "Battle of the Clipper Chip," *The New York Times*, June 11, 1994, <http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all> (accessed June 15, 2015).
56. *Ibid.*

57. Department of Commerce's National Institute of Standards and Technology, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)," Federal Register Vol. 59, No. 27, February 9, 1994, available at https://epic.org/crypto/clipper/fips_185_clipper_feb_94.html (accessed June 15, 2015).
58. Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip* (New Haven, CT: Yale University Press, 1997), 40.
59. Diffie and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 237.
60. Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow." ("If the government could not prevent the public from using nonconforming products, perhaps it could set the standard by purchasing and deploying large numbers of escrowed products. People who wanted to interoperate with the government's machines would naturally buy the same equipment. The existence of a large functioning user base would create further incentives for others to buy the same equipment.")
61. Levy, "Battle of the Clipper Chip."
62. NIST, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)."
63. Shari Steele and Daniel J. Weitzner, "Chipping Away at Privacy," *BBS Magazine*, September 1993, available at https://w2.eff.org/Privacy/Key_escrow/Clipper/clipper.summary (accessed June 15, 2015).
64. Diffie and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 236.
65. "Testimony of Whitfield Diffie, The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology," May 11, 1993, available at <http://cpsr.org/prevsite/program/clipper/diffie-testimony.html/> (accessed June 15, 2015).
66. The Computer System Security and Privacy Advisory Board (now known as the Information Security and Privacy Advisory Board) is a government review panel that identifies emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy, advises the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, and reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and the appropriate committees of the Congress. For more information about ISPAB, see <http://csrc.nist.gov/groups/SMA/ispab/index.html> (accessed June 15, 2015).
67. John Markoff, "Computer Code Plan Challenged," *The New York Times*, May 29, 1993, <http://www.nytimes.com/1993/05/29/business/company-news-computer-code-plan-challenged.html> (accessed June 15, 2015).
68. "The most important means to the defense of privacy is encryption. To encrypt is to indicate the desire for privacy. But to encrypt with weak cryptography is to indicate not too much desire for privacy. Cypherpunks hope that all people desiring privacy will learn how best to defend it. Cypherpunks are therefore devoted to cryptography. Cypherpunks wish to learn about it, to teach it, to implement it, and to make more of it. Cypherpunks know that cryptographic protocols make social structures. Cypherpunk know how to attack a system and how to defend it. Cypherpunks know just how hard it is to make good cryptosystems." Eric Hughes, "Welcome to the Cypherpunks Email," *Cyphernomicron*, September 10, 1994, available at <http://www.cypherpunks.to/faq/cyphernomicron/chapter4.html> (accessed June 15, 2015).
69. John Markoff, "Big Brother and the Computer Age," *The New York Times*, May 6, 1993, <http://www.nytimes.com/1993/05/06/business/big-brother-and-the-computer-age.html> (accessed June 15, 2015).
70. Andy Greenberg, *This Machine Kills Secrets* (New York: Penguin Group, 2012), 85.
71. *Ibid.*, 85.
72. *Ibid.*, 81-85.

73. In its initial analysis of the Clipper Proposal, for example, EFF laid out three serious concerns, largely related to how quickly the government was moving forward with an untested proposal that might have serious security vulnerabilities. "Initial EFF Analysis of Clinton Privacy and Security Proposal," *Electronic Frontier Foundation*, April 16, 1993, <https://w2.eff.org/Privacy/Newin/Cyberpunks/930416.eff.initial.analysis> (accessed June 15, 2015).
74. "Electronic Petition to Oppose Clipper," *Computer Professionals for Social Responsibility*, January 24, 1994, available at https://www.epic.org/crypto/clipper/cpsr_electronic_petition.html (accessed June 15, 2015).
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).
76. Gurak, *Persuasion and Privacy in Cyberspace*, 34.
77. About CPSR, "Computer Professionals for Social Responsibility," <http://cpsr.org/about/> (accessed June 15, 2015).
78. "Letter to the President," *Computer Professionals for Social Responsibility*, January 24, 1994, available at <http://cpsr.org/prevsite/program/clipper/cpsr-clipper-letter.html/> (accessed June 15, 2015).
79. Ibid.
80. "A Letter from the Digital Privacy and Security Working Group to President Clinton," May 7, 1993, available at <https://www.eff.org/effector/5/8> (accessed June 15, 2015).
81. Levy, *Crypto*, 254, 264-268, 304; Markoff, "Big Brother and the Computer Age" (quoting Ed Markey, "There are many ways the N.S.A. is trying to put the cryptography genie back in the bottle, but it's already available for everyone openly.").
82. "Statement Of Senator Patrick J. Leahy, Chairman, Technology And The Law Subcommittee Hearing On The Administration's Clipper Chip Key Escrow Encryption Program," May 3, 1994, available at https://w2.eff.org/Privacy/Key_escrow/Clipper/leahy_clipper_050394.testimony (accessed June 15, 2015).
83. "Telecommunications Carrier Assistance to the Government," 103rd Congress 2nd Session, Report 103-827, October 4, 1994, available at https://epic.org/privacy/wiretap/calea/H_Rpt_103_827.txt (accessed June 15, 2015). Also see Christopher Soghoian, "CALEA and encryption," *Slight Paranoia*, September 28, 2010, <http://paranoia.dubfire.net/2010/09/calea-and-encryption.html> (accessed June 15, 2015).
84. NIST, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)."
85. Philip Elmer-Dewitt, "Who Should Keep the Keys?" *TIME Magazine*, March 14, 1994, <http://content.time.com/time/magazine/article/0,9171,164002,00.html> (accessed June 15, 2015). ("In a Time/CNN poll of 1,000 Americans conducted last week by Yankelovich Partners, two-thirds said it was more important to protect the privacy of phone calls than to preserve the ability of police to conduct wiretaps. When informed about the Clipper Chip, 80% said they opposed it.")
86. Stewart A. Baker, "Don't Worry Be Happy: Why Clipper Is Good For You," *Wired*, May 1994, available at <http://groups.csail.mit.edu/mac/classes/6.805/articles/baker-clipper.txt> (accessed June 15, 2015).
87. Dorothy Denning debated John Perry Barlow, a cofounder of the EFF, on America Online. Levy, "Clipper Chick."
88. Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," *AT&T Bell Laboratories*, 1994, <http://www.crypto.com/papers/eesproto.pdf> (accessed June 15, 2015).
89. John Markoff, "Flaw Discovered in Federal Plan for Wiretapping," *The New York Times*, June 2, 1994, <http://www.nytimes.com/1994/06/02/us/flaw-discovered-in-federal-plan-for-wiretapping.html> (accessed June 15, 2015).
90. Sharon Begley, "Folling the Clipper Chip," *Newsweek*, June 12, 1994, <http://www.newsweek.com/foiling-clipper-chip-188912> (accessed June 15, 2015).

91. Markoff, "Flaw Discovered in Federal Plan for Wiretapping."
92. Ibid.
93. Jared Sandberg and Don Clark, "AT&T, VLSI Technology to Develop Microchips That Offer Data Security," *The Wall Street Journal*, January 31, 1995.
94. "Testimony of Philip R. Zimmermann," before the Subcommittee on Science, Technology, and Space of the U.S. Senate Committee on Commerce, Science, and Transportation, June 29, 1996, available at <https://www.philzimmermann.com/EN/testimony/index.html> (accessed June 15, 2015).
95. In a letter to Representative Maria Cantwell in July 1994, Vice President Al Gore referred repeatedly to "future escrow systems" and efforts with industry and academia to design and create such systems. "Letter from Vice President Al Gore to the Honorable Maria Cantwell," July 20, 1994, available at https://epic.org/crypto/key_escrow/Gore_letter_1994.html (accessed June 15, 2015).
96. Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow."
97. "By the summer of 1996, 'key escrow' had amassed so much criticism that proponents of the idea started using the term 'key recovery' to mean essentially the same thing. There have been several attempts to explain the difference, usually by companies that have developed key escrow schemes. The explanation usually boils down to 'Key escrow was that old unacceptable idea, but this particular feature of our product includes makes it recovery rather than escrow.'" Notes from Ethics and the Law on the Electronic Frontier (2005), "1995-1997: From Clipper to Key Recovery," *MIT Open Courseware*, http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-805-ethics-and-the-law-on-the-electronic-frontier-fall-2005/readings/encrypt_4/ (accessed June 15, 2015).
98. Froomkin, "It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow." For comparison, it's worth noting that Skipjack had an 80-bit key length. See notes 45 and 184 for an explanation of the significance of key length.
99. Froomkin, *Ibid.*
100. Giampiero Giacomello, *National Governments and Control of the Internet: A Digital Challenge* (New York: Routledge, 2005), 44.
101. For a good description of the opposition to the Clipper II and Clipper III proposals, see Notes from Ethics and the Law on the Electronic Frontier, "1995-1997: From Clipper to Key Recovery."
102. Giacomello, *National Governments and Control of the Internet*, 44.
103. Diffe and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 246-247.
104. "Open Letter to the Internet Community from Senator Conrad Burns," May 2, 1996, available at https://www.epic.org/crypto/legislation/burns_letter.html (accessed June 15, 2015).
105. "Pro-CODE Encryption Legislation," *The Electronic Privacy Information Center*, n.d., https://epic.org/crypto/legislation/pro_code.html (accessed June 15, 2015).
106. Original text of S.1726, "Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996," introduced July 27, 1996, available at <https://www.congress.gov/bills/104th-congress/senate-bill/1726> (accessed June 15, 2015).
107. "Keep Big Brother's Hands off the Internet," Remarks of Senator John Ashcroft as Chairman of the Senate Commerce Subcommittee on Consumer Affairs, Foreign Commerce and Tourism, 1997, available at <http://rense.com/general31/keepbigbrothershands.htm> (accessed June 15, 2015).
108. Kenneth W. Dam and Herbert S. Lin, eds., "Cryptography's Role in Securing the Information Society," National Research Council's Committee to Study National Cryptography Policy, May 30, 1996, at 7, available at <http://www.nap.edu/catalog/5131.html> (accessed June 15,

2015). The National Research Council members were drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

109. *Ibid.*, 4.

110. The final recommendation said that “governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade,” and warned against governments initiating “legislation which limits user choice.” “Recommendation of the Council Concerning Guidelines for Cryptography Policy,” (*Organisation for Economic Co-operation and Development*), C(97)62/FINAL, March 27, 1997, available at <http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=115&InstrumentPID=111&Lang=en&Book=> (accessed June 15, 2015).

111. “Towards a European Framework for Digital Signatures and Encryption,” *European Commission*, October 8, 1997, available at <http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/eu-october-8-97.html> (accessed June 15, 2015).

112. Edmund Andrews, “Europeans Reject U.S. Plan on Electronic Cryptography,” *The New York Times*, October 9, 1997, <http://partners.nytimes.com/library/cyber/week/00997encrypt-side.html> (accessed June 15, 2015).

113. Abelson et al., “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption.”

114. *Ibid.*

115. *Ibid.*

116. The book “details how programmers and electronic communications professionals can use cryptography — the technique of enciphering and deciphering messages — to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them in cryptographic software, and shows how they can be used to solve security problems.” Among other things, it includes actual source code for a number of encryption algorithms. “Applied Cryptography,” *Schneier on Security*, available at https://www.schneier.com/books/applied_cryptography/ (accessed June 15, 2015).

117. Karn’s action was likely motivated by a desire to challenge the export controls on encryption software. Other early acts of resistance included a decision in 1994 by MIT to publish PGP source code and run a key server on the Internet, which could well have been interpreted as a violation of export controls because the software was made available to anyone in the world. See “MIT PGP Announcement,” available at <http://town.hall.org/cyber94/pgp.html> (accessed June 15, 2015).

118. Keith Aoki, “Privacy and Encryption Export Controls: A Crypto Trilogy (Bernstein, Junger & Karn),” *University of Oregon School of Law*, August 24, 2000, available at <http://www.cyberspace.law.org/aoki/> (accessed June 15, 2015).

119. *Ibid.*

120. Levy, *Crypto*, 197-8, 287-8. Zimmermann was investigated by the Justice Department for three years relating to possible export control violations because PGP had been posted online. In 1996, the Justice Department announced it would not seek an indictment due to insufficient evidence. Ira S. Rubenstein and Michael Hintze, “Export Controls on Encryption Software,” *Coping with U.S. Export Controls 2000*, Practising Law Institute, Commercial Law and Practice Course Handbook Series (December 2000) available at http://encryption_policies.tripod.com/us/rubinstein_2000_software.htm (accessed June 15, 2015), § 2(e) PGP. Also see Ronald J. Stay, “Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann,” *Georgia State University Law Review*, Vol. 13: Issue 2, Article 14, available at <http://readingroom.law.gsu.edu/gslr/vol13/iss2/14/> (accessed June 15, 2015).

121. Category XIII, Auxiliary Military Equipment, for example, includes “Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems.” 22 CFR Section 121 XIII(b)(1).

122. The length of the key is central to determining its level of security. Adding one “bit,” or digit, to the key doubles the number of distinct values the key could potentially hold, and thereby also doubles the amount of time a hypothetical attacker would need to guess the actual value of the key. A two-bit key can hold four possible values, a three-bit key can hold eight, and so on.
123. A 40-bit symmetric encryption key can hold approximately 1.1 trillion values. Although the exact time required to guess a key depends on how much computing power is available, in the mid-1990s, a 40-bit key could be guessed in eight to ten days, according to experiments performed by graduate students at MIT and UC Berkeley. Today, a 40-bit key could be cracked in a matter of hours (or even minutes).
124. “Under the current ITAR regime, applications to export cryptographic software designed to encrypt messages with keys stronger than forty bits are generally denied, although authentication products that cannot be adapted for encryption, or which are designed for specific favored applications such as banking, tend to receive official export clearance. Applications to export DES, which uses fifty-six-bit encryption, are also often denied. Applications for stronger products are considered to have little chance of approval.” Froomkin, “It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow.”
125. As Vice Admiral Bobby Ray Inman, who served as director of the NSA from 1977 to 1981, explained, “We were worried that foreign countries would pick up and use cryptography that would make it exceedingly hard to decrypt and read their traffic.” Quoted in Corrigan-Gibbs, “Keeping Secrets.”
126. Levy, “Battle of the Clipper Chip.”
127. “Decoding the Encryption Debate,” *Electronic Frontier Foundation*, 1997, <https://www.eff.org/effector/10/10> (accessed June 15, 2015).
128. “Cryptography and Liberty 1999: An International Survey of Encryption Policy,” *Electronic Privacy Information Center*, 1999, available at <http://gila.org/crypto/crypto-survey-99.html> (accessed June 15, 2015). (“Internationally, export controls are the strongest tool used by governments to limit development of encryption products. Export controls reduce the availability of encryption in common programs such as operating systems, electronic mail and word processors, especially from American companies. The restrictions make it difficult to develop international standards for encryption and interoperability of different programs. Countries must develop their own local programs, which do not inter-operate well (if at all) with other programs developed independently in other countries. They may not be as secure because of a lack of peer-review. Because markets are smaller, companies and individuals are not as interested in developing programs because of smaller potential profits.”)
129. Froomkin, “It Came from Planet Clipper: The Battle Over Cryptographic Key Escrow.” Recent incidents have demonstrated the dangerous vulnerabilities that can be created as a result, which we will discuss in greater depth in the final section of this report.
130. Jeanne J. Grimmett, “Encryption Export Controls,” *Congressional Research Services*, updated January 11, 2001, at CRS-3, available at http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30273_01112001.pdf (accessed June 15, 2015). (“With the growth of the global economy, the business community has continued to express a need for strong encryption for domestic use and cross-border communications and transactions. While there are no statutory restrictions on the domestic use of encryption, the computer industry argues that restrictive export controls have hampered U.S. technological development since it is impracticable to develop separate products for the domestic and foreign market.”)
131. U.S. Department of Commerce & National Security Agency, “A Study of the International Market for Computer Software With Encryption” at V-5 (1996), available at https://www.bis.doc.gov/index.php/formsdocuments/doc_view/24-a-study-of-the-international-market-for-computer-software-with-encryption-nsa-1995 (accessed June 15, 2015).
132. Erik R. Olbeter and Christopher Hamilton, “Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy,” *Economic Strategy Institute*, April 1998, available at http://members.tripod.com/encryption_policies/us/olbeter_0498_key.htm (accessed June 15, 2015).
133. Jeri Clausing, “Study Puts Price on Encryption Controls,” *The New York Times*, April 1, 1998, <http://partners.nytimes.com/library/tech/98/04/cyber/articles/01encrypt.html> (accessed June 15, 2015). The full study, “Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy,” detailed four primary types of impact on the U.S. economy as a result of the restrictions: lost encryption

product sales, slower growth in encryption-dependent industries, foregone cost savings and efficiency gains from the use of the Internet and networked technologies, and indirect spillover effects into broader American industries. Erik R. Olbeter and Christopher Hamilton, "Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy," *Economic Strategy Institute*, April 1998, available at http://members.tripod.com/encryption_policies/us/olbeter_0498_key.htm (accessed June 15, 2015).

134. Shari Steele and Daniel J. Weitzner, "A Government Computer Encryption System Would Threaten Civil Liberties," in *The Information Highway*, Ed. Charles P. Cozie (San Diego: Greenhaven Press, 1996) at 191-194, available at http://www.dikseo.teimes.gr/spoudastirio/E-NOTES//Information_Highway_The_Viewpoints.pdf (accessed June 15, 2015).

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

136. *Karn v. U.S. Dept. of State*, 925 F.Supp. 1 (D.D.C. 1996).

137. In *Junger v. Daley*, Case Western Law Professor Peter Junger found himself at odds with the Commerce over whether he was allowed to post some of his work related to computers and regulation to the World Wide Web. *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000).

138. There are numerous academic articles about the free speech implications of these three cases, but for a concise summary of how they were resolved, see Grimmer, "Encryption Export Controls," CRS-3. ("Federal district courts addressing this issue over the last three years have both upheld and dismissed First Amendment challenges to export licensing schemes for encryption.")

139. Quoted in Rubinstein and Hintze, "Export Controls on Encryption Software," § 4(a) The Karn and Bernstein Cases.

140. "Testimony of Alan B. Davidson, Staff Counsel, Center for Democracy and Technology," before the House Committee on International Relations Subcommittee on International Economic Policy and Trade, May 18, 1999, available at <https://www.cdt.org/files/testimony/990518davidson.shtml?page=15&issue=75> (accessed June 15, 2015) ("Davidson Encryption Testimony"). ("By limiting the spread of U.S. encryption outside the U.S., they make it harder for people in the U.S. to communicate securely with colleagues, business partners, family members, and others abroad. By 'dumbing down' the security standards being built into the common products, they slow the use of encryption by law-abiding citizens in the U.S. By limiting the technical means of protecting information online, they leave our privacy unprotected in a world where Fourth Amendment protections stop at the border and information is not legally protected worldwide.")

141. In August 1995, several European researchers demonstrated that they could break the 40-bit encryption algorithm used in Netscape's SSL ("the only encryption algorithm generally approved for export from the U.S., and claimed by the Administration to be adequate for commercial applications") in eight days. In 1997, a grad student at UC Berkeley used a network of computers to crack a 40-bit key in under four hours. Notes from Ethics and the Law on the Electronic Frontier, "1995-1997: From Clipper to Key Recovery"; "Exportable Cryptography Totally Insecure: Challenge Cipher Broken Immediately," UC Berkeley, January 28, 1997, available at <http://www.isaac.cs.berkeley.edu/isaac/press-release> (accessed June 15, 2015).

142. Ronald L. Rivest, "The Case Against Regulating Encryption Technology," *Scientific American*, October 1998, available at <http://people.csail.mit.edu/rivest/pubs/Riv98e.pdf> (accessed June 15, 2015).

143. 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> (accessed June 15, 2015). See also "Statement of Lance J. Hoffman, Professor, The George Washington University," before the U.S. Senate Committee on Commerce, Science, and Transportation, June 10, 1999, available at http://www.seas.gwu.edu/~lanceh/senate_testimony_pdf.pdf.

144. Hoffman et al., "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations." ("On average, the quality of foreign and U.S. products is comparable. There are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality.")

145. Davidson Encryption Testimony.

146. Zimmermann, "Why I wrote PGP."

147. "Statement of Vice President Al Gore," *The White House*, October 1, 1996, available at https://epic.org/crypto/key_escrow/clipper4_statement.html (accessed June 15, 2015).
148. For an explanation of the National Research Council's findings, see footnote 108 above.
149. Full text of Executive Order 13026, "Administration of Export Controls on Encryption Products" (November 15, 1996), is available at <http://www.gpo.gov/fdsys/pkg/FR-1996-11-19/pdf/96-29692.pdf> (accessed June 15, 2015).
150. L. Jean Camp and Ken Lewis, "Code as Speech: a Discussion of Bernstein vs. USDOJ, Karn v. USDOJ, and Junger v. Daley in light of the U.S. Supreme Court's recent shift to Federalism," *Ethics and Information Technology*, March 2001, Vol. 1, No. 2. Also see Rubenstein and Hintze, "Export Controls on Encryption Software."
151. "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/9990225bg.htm> (accessed June 15, 2015).
152. Original text of H.R. 3011, the Security and Freedom Through Encryption (SAFE) Act in the 104th Congress, introduced March 5, 1996, available at <https://www.congress.gov/bills/104/3011/text?q=%7B%22search%22%3A%5B%22Security+and+Freedom+through+Encryption+Act%22%5D%7D>. (accessed June 15, 2015)
153. Specifically, the bill stated that "No person in lawful possession of a key to encrypted information may be required by Federal or State law to relinquish to another person control of that key." There was an exception, however, which stipulated that the key-escrow prohibition "shall not affect the authority of any investigative or law enforcement officer, acting under any law in effect on the effective date of this chapter, to gain access to encrypted information." H.R. 3011.
154. The SAFE Act amended the Export Administration Regulations to allow the export without a license of most generally available software and hardware containing encryption unless there was substantial evidence that it would be used for military purposes.
155. "Press Briefing by the Vice President, Deputy Chief of Staff John Podesta, Principal Associate Deputy Attorney General Robert Litt, Assistant Director of the FBI Carolyn Morris, Undersecretary of Commerce William Reinsch," *The White House*, September 16, 1998, available at <http://fas.org/irp/offdocs/EncryptionWH.htm> (accessed June 15, 2015).
156. By the late 1990s, even 56-bit encryption keys were demonstrated to be insecure. On the heels of the cracks of export-grade encryption, in 1998 the Electronic Frontier Foundation demonstrated that the supposed "gold standard" of domestic encryption algorithms was vulnerable to attack. For less than \$250,000, EFF built the first unclassified hardware for cracking the DES algorithm. It took under three days to decode a message, which the government had previously claimed would take months and require multimillion-dollar networks of computers. "EFF has proved what has been argued by scientists for twenty years, that DES can be cracked quickly and inexpensively," said John Gilmore, EFF co-founder and project leader. 'Now that the public knows, it will not be fooled into buying products that promise real privacy but only deliver DES. This will prevent manufacturers from buckling under government pressure to 'dumb down' their products, since such products will no longer sell.' EFF Executive Director Barry Steinhardt added, 'If a small nonprofit can crack DES, your competitors can too. Five years from now some teenager may well build a DES Cracker as her high school science fair project.'" For more on how DES works, see note 45. "EFF DES Cracker Machine Brings Honesty To Crypto Debate," *Electronic Frontier Foundation*, July 17, 1998, https://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html.
157. Courtney Macavinta, "White House eases crypto limits," *CNET News*, September 16, 1998, <http://news.cnet.com/2100-1023-215577.html> (accessed June 15, 2015).
158. The President's Export Council was first created in 1973 to advise the President on export enhancement and work with industry to encourage U.S. companies to increase exports and enter new markets. The Subcommittee on Encryption, established in 1979, was created to advise on future key recovery issues, including evaluating the developing global key architecture, assessing lessons learned from key recovery implementation, advising on technical confidence issues, addressing interoperability and standards issues, and identifying other technical, policy, and program issues for government action. U.S. Department of Commerce: International Trade Administration. "President's Export Council History," *U.S. Commerce Department's International Trade Division*, available at <http://trade.gov/pec/history.asp>.

159. "Liberalization 2000: Recommendations for Revising the Encryption Export Regulations," *President's Export Council Subcommittee on Encryption*, August 25 1999, available at <http://cryptome.org/1.B42.htm> (accessed June 15, 2015).
160. "Administration Announces New Approach to Encryption," *The White House*, September 16, 1999, available at https://epic.org/crypto/legislation/cesa/WH_release_9_16.html (accessed June 15, 2015).
161. "Update to Encryption Policy," *U.S. Commerce Department*, September 16, 1999, available at https://epic.org/crypto/export_controls/commerce_q8a_q_99.html (accessed June 15, 2015).
162. Jeri Clausing, "In a Reversal, White House Will End Data-Encryption Export Curbs," *The New York Times*, September 17, 1999, <http://www.nytimes.com/1999/09/17/business/in-a-reversal-white-house-will-end-data-encryption-export-curbs.html> (accessed June 15, 2015).
163. *Ibid.*
164. Levy, *Crypto*, 307.
165. "Revised U.S. Encryption Export Control Regulations," *U.S. Commerce Department*, January 2000, available at https://epic.org/crypto/export_controls/regs_1_00.html (accessed June 15, 2015).
166. 15 CFR § 740.13 "Technology and Software Unrestricted (TSU)" License Exception, which is described at https://www.bis.doc.gov/index.php/forms-documents/doc_view/986-740 (accessed June 15, 2015).
167. Clausing, "In a Reversal, White House Will End Data-Encryption Export Curbs." (Quoting Representative Goodlatte, "'I am surprised that they moved this much this quickly,' Mr. Goodlatte said. 'But we are very pleased that they have done so and that they have come this close. There is no doubt that this announcement is a direct result of the fact that we had 258 co-sponsors.'")
168. Rubinstein and Hintz, "Export Controls on Encryption Software."
169. Dam and Lin, eds., "Cryptography's Role in Securing the Information Society."
170. Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 4. ("Without a secure and trusted infrastructure, companies and individuals will become increasingly reluctant to move their private business or personal information online.")
171. For example, U.S. electronic commerce expanded from around \$28 billion in the year 2000 to \$143 billion in 2009. D. Steven White, "U.S. E-Commerce Growth 2000-2009," available at <http://dstevenwhite.com/2010/08/20/u-s-e-commerce-growth-2000-2009/> (accessed June 15, 2015). These statistics were drawn from "E-Stats - Measuring the Electronic Economy," *United States Census Bureau*, May 22, 2014, <http://www.census.gov/econ/estats/index.html> (accessed June 15, 2015).
172. Holly Lynne McKinley, "SSL and TLS: A Beginners Guide," *The SANS Institute*, 2003, <https://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029> (accessed June 15, 2015).
173. "What is SSL (Secure Sockets Layer) and What Are SSL Certificates?" *Digicert*, <https://www.digicert.com/ssl.htm> (accessed June 15, 2015).
174. "History of SSH (SSH, The Secure Shell: The Definitive Guide)," *University of Arkansas College of Engineering*, 2002, http://csce.uark.edu/~kal/Info/private/ssh/choi_05.htm (accessed June 15, 2015).
175. In 2010, Verisign sold its SSL certificate and related authentication businesses to Symantec.
176. For more information, see <https://www.comodo.com/> (accessed June 15, 2015).
177. See, e.g., EFF's "Encrypt the Web" Scorecard, which surveys the practices of 18 major Internet companies and providers, several categories related to support for and use of HTTPS. The latest version of the report is available at <https://www.eff.org/encrypt-the-web-report> (accessed June 15, 2015).

178. "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," *The White House*, December 12, 2013, at 216-217, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed June 15, 2015).
179. *Ibid.* 22.
180. Bob Goodlatte, "Let's Open Up Encryption," *The Washington Post*, June 12, 1997, <http://www.washingtonpost.com/wp-srv/politics/special/encryption/stories/ocro61297.htm> (accessed June 15, 2015). ("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.")
181. 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. The vast amount of personal information on those devices makes them especially attractive targets for criminals aiming to commit identity theft or other crimes of fraud. "Smart phone thefts rose to 3.1 million last year, Consumer Reports finds," *Consumer Reports*, May 28, 2014, <http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm> (accessed June 15, 2015). Many now argued that encryption actually makes us all safer. See, e.g., Nuala O'Connor, "Encryption Makes Us All Safer," *Center for Democracy & Technology*, October 8, 2014, <https://cdt.org/blog/encryption-makes-us-all-safer/> (accessed June 15, 2015).
182. Dan Goodlin, "'FREAK' flaw in Android and Apple devices cripples HTTPS crypto protection," *Ars Technica*, March 3, 2015, <http://arstechnica.com/security/2015/03/freak-flaw-in-android-and-apple-devices-cripples-https-crypto-protection/> (accessed June 15, 2015). The full report by Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cedric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre Yves-Strub, Santiago Zanella-Beguelin, Jean-Karim Zinzindohoue, and Benjamin Beurdouche is available at <https://www.smacktls.com/#freak> (accessed June 15, 2015). The vulnerability is officially catalogued as CVE-2015-0204, available at <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204> (accessed June 15, 2015).
183. There are two types of key lengths: those of symmetric keys and those of asymmetric keys (for cryptosystems where separate keys are used to encrypt and decrypt), and direct comparison of their key lengths is meaningless. Prior to 2000 there were limits on the length of both types of keys, making the encryption weaker and easier to break. The 40-bit, 56-bit, and 128-bit keys discussed earlier in the paper were all used in symmetric encryption algorithms, like DES and AES. Government controls initially limited the export of keys above 40-bits, then above 56-bits, while keys used today for strong symmetric encryption are 128-bits, 192-bits, or 256-bits long. Asymmetric encryption requires much longer key lengths, such as the vulnerable 512-bit RSA keys threatened by the FREAK attack. As a comparison, strong RSA keys used today are either 2048 bits or 4096 bits long. Because the security of a key of either type increases exponentially as it gets longer, the difference between the time necessary to brute force a 40-bit key and a 256-bit key, or between a 512-bit RSA key and a 4096-bit RSA key, is the difference between a few hours and many times the length of the history of the universe. Arjen K. Lenstra, "Key Lengths," in *Handbook of Information Security*, ed. Hossein Bidgoli (Hoboken, NJ: Wiley, 2006), available at <http://infoscience.epfl.ch/record/164539/files/NPDF-32.pdf>.
184. For a good technical explanation of how a FREAK Attack works, see Matthew Green, "Attack of the week: FREAK (or 'factoring the NSA for fun and profit')." *A Few Thoughts on Cryptographic Engineering*, March 3, 2015, <http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html> (accessed June 15, 2015).
185. Craig Timberg, "'FREAK' flaw undermines security for Apple and Google users, researchers discover," *The Washington Post*, March 3, 2015, <http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/03/freak-flaw-undermines-security-for-apple-and-google-users-researchers-discover/> (accessed June 15, 2015).
186. Dan Goodin, "HTTPS-crippling attack threatens tens of thousands of Web and mail servers," *Ars Technica*, May 20, 2015, <http://arstechnica.com/security/2015/05/https-crippling-attack-threatens-tens-of-thousands-of-web-and-mail-servers/> (accessed June 15, 2015). Also see "The Logjam attack, available at <https://weakdh.org/>, (accessed June 15, 2015).
187. "ACLU Submission to the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression and Opinion," *American Civil Liberties Union*, February 10, 2015, https://www.aclu.org/sites/default/files/assets/aclu_submission_to_special_rapporteur_-_encryption_and_anonymity.pdf (accessed June 15, 2015).

188. Hillary Clinton gave two major addresses on Internet Freedom during her tenure as Secretary of State, becoming the first global leader to emphasize Internet Freedom as a foreign policy priority and urging “countries everywhere... to join us in the bet we have made, a bet that an open Internet will lead to stronger, more prosperous countries.” Hillary Clinton, “Internet Rights and Wrongs: Choices and Challenges in a Networked World,” *U.S. Department of State*, February 15, 2011, available at <http://blogs.state.gov/stories/2011/02/15/Internet-rights-and-wrongs-choices-and-challenges-networked-world>. (accessed June 15, 2015). Also see the U.S. State Department’s Internet Freedom page, available at <http://www.humanrights.gov/issues/Internet-freedom/>. (accessed June 15, 2015).
189. Scott Busby, “10 Things You Need to Know About U.S. Support for Internet Freedom,” *IIP Digital*, May 29, 2014, <http://iipdigital.usembassy.gov/st/english/article/2014/05/20140530300596.html#axzz3zvEtH3Cg>. (accessed June 15, 2015).
190. “Report of the Special Rapporteur on promotion and protection of the right to freedom of expression and opinion, David Kaye,” A/HRC/29/32, May 22, 2015, available at <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>.
191. A 2013 study of the experiences of 1,175 Chinese Internet users circumventing their country’s Internet censorship found that the “circumvention tools that work best for these users are technologically diverse, but they are united by a shared political feature: the collateral cost of choosing to block them is prohibitive for China’s censors. Our survey respondents are relying not on tools that the Great Firewall can’t block, but rather on tools that the Chinese government does not want the Firewall to block. Internet freedom for these users is collateral freedom, built on technologies and platforms that the regime finds economically or politically indispensable.” David Robinson et al., “Collateral Freedom: A Snapshot of Chinese Internet Users Circumventing Censorship,” *Open Internet Tools Project*, April 2013, <https://openitp.org/pdfs/CollateralFreedom.pdf> (accessed June 15, 2015).
192. For more information, see “Advisory Committee to the Congressional Internet Caucus,” available at <http://www.netcaucus.org/> (accessed June 15, 2015).
193. “Americans for Computer Privacy (ACP) is a broad-based coalition that brings together more than 100 companies and 40 associations representing financial services, manufacturing, telecommunications, high-tech and transportation, as well as law enforcement, civil-liberty, pro-family and taxpayer groups. ACP supports policies that advance the rights of American citizens to encode information without fear of government intrusion, and advocates the lifting of export restrictions on U.S.-made encryption products.” “Who We Are,” *Americans for Computer Privacy*, available at <http://www.computerprivacy.org/who/index.html> (accessed June 15, 2015).
194. See, e.g., Craig Aaron, “How We Won Net Neutrality,” *The Huffington Post*, February 26, 2015, http://www.huffingtonpost.com/craig-aaron/how-we-won-net-neutrality_b_6759132.html (accessed June 15, 2015).
195. See, e.g., “Statement of Kevin S. Bankston, Policy Director of New America’s Open Technology Institute and Co-Director of New America’s Cybersecurity Initiative, at the Hearing on Encryption Technology and U.S. Policy Responses,” before the U.S. House of Representatives Subcommittee on Information Technology of the Committee on Oversight and Government Reform, April 29, 2015, available at https://static.newamerica.org/attachments/2982-at-crypto-hearing-best-arguments-against-backdoor-mandates-come-from-members-of-congress-themselves/Bankston_Written_Testimony.5876d326c5fc4e0cb17b59e8d53384f.pdf. (accessed June 15, 2015).





State of Connecticut
DIVISION OF CRIMINAL JUSTICE

OFFICE OF
THE CHIEF STATE'S ATTORNEY

KEVIN T. KANE
CHIEF STATE'S ATTORNEY

300 CORPORATE PLACE
ROCKY HILL, CONNECTICUT 06067
PHONE (860) 258-5800 FAX (860) 258-5858

July 10, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to seek the help of the United States Senate to ensure that law enforcement officials can properly and lawfully obtain critical evidence to protect the American public and enforce our laws. As we move deeper into the digital age more and more information is created and stored on smartphones and other electronic devices. The advantages of these technological advances are undeniable, but unfortunately those who mean harm to our fellow citizens also have moved into the digital age. No longer can law enforcement track threats and uncover evidence of crimes through traditional searches of physical property and wiretaps. The increasing use of digital devices requires that we have the ability – through proper court orders – to access data created and stored on electronic devices.

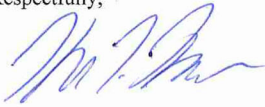
Congress has traditionally given law enforcement the legal tools it needs to meet technological changes and protect the public. We now need your help again. As you know, Apple and Google are producing smartphones that allow the subscriber to encrypt data in such a way that the information cannot be retrieved even when a judicial officer has found probable cause to believe that the data is evidence of a crime. Absent an ability to penetrate these protections, information that that might expose an imminent threat of terrorist attack or the safety of a vulnerable victim will be beyond the reach of law enforcement.

We all fully understand and respect the tremendous value of privacy. But the risk to public safety and crime victims posed by these impenetrable encryptions must also be considered. Simply put, if terrorists, human traffickers, and others who mean harm to our fellow citizens can hide evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement – even after a judicial officer has authorized law enforcement to retrieve such data, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the “arms race” between criminals and law enforcement, the criminals will have won.

U.S. Senate Committee on the Judiciary
Page 2
July 10, 2015

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,



KEVIN T. KANE
CHIEF STATE'S ATTORNEY

Raymond W. Kelly
Attorney at Law
1290 Avenue of the Americas
New York, NY 10104

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

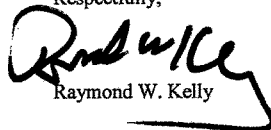
Dear Senators:

As the longest serving Commissioner for the New York City Police Department and former Undersecretary of Enforcement for the U.S. Treasury Department, I am writing to express my concern about the efforts that major technology companies have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that these companies' actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. If criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if these companies are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,


Raymond W. Kelly



State of Rhode Island and Providence Plantations

DEPARTMENT OF ATTORNEY GENERAL

150 South Main Street • Providence, RI 02903
(401) 274-4400 - TDD (401) 453-0410

Peter F. Kilmartin, Attorney General

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Peter F. Kilmartin
Attorney General



JACKIE LACEY
LOS ANGELES COUNTY DISTRICT ATTORNEY

HALL OF JUSTICE
211 WEST TEMPLE STREET LOS ANGELES, CA 90012 (213) 974-3500

July 6, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, DC 20510-6050

Re: **Going Dark: Encryption, Technology, and the Balance Between Public Safety
and Privacy**

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,


JACKIE LACEY
District Attorney

kp



Nicholas "Nico" LaHood
Criminal District Attorney
Bexar County, Texas

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

A handwritten signature in blue ink, appearing to read "Nico LaHood", written over the word "Nicholas".

Nicholas "Nico" LaHood

Paul Elizondo Tower • 101 W. Nueva, Seventh Floor • San Antonio, Texas 78205-3030
(210) 335-2311

For Victim Assistance call (210) 335-2105



OFFICE OF THE DISTRICT ATTORNEY
RICHMOND COUNTY

DANIEL L. MASTER, JR.
ACTING DISTRICT ATTORNEY

130 STUYVESANT PLACE
STATEN ISLAND, NEW YORK 10301
TELEPHONE (718) 876-6300

July 15, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

**Re: *Going Dark: Encryption, Technology, and
the Balance between Public Safety and
Privacy***

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Sincerely,

Daniel L. Master, Jr.
Acting District Attorney



**Office of the
District Attorney
County of Rockland**

THOMAS P. ZUGIBE
DISTRICT ATTORNEY

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

While I support efforts to guarantee the privacy rights of all citizens, it is imperative that law enforcement, with appropriate judicial supervision and approval, maintain its ability to access and recover digital evidence in order to protect the public and successfully prosecute those guilty of crimes.

Private Sector companies have made their smartphones impervious to search warrants and similar judicial orders.

At the local level, the cities, towns and villages across the country, law enforcement's efforts to conduct investigations are being seriously impaired. This is not solely about terrorism, this has become a major factor in law enforcement's ability to keep communities safe from all types of criminal activity.

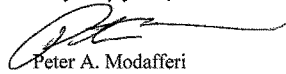
If criminal wrongdoers are granted a "safe haven" to conduct their activity and hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

I urge you to explore all aspects of this issue but please place the safety of our communities at the highest level importance.

To be clear law enforcement is not asking for new surveillance capabilities above and beyond what is currently authorized by the United States Constitution.

Thank you for your attention to this matter.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Peter A. Modafferi', with a long horizontal flourish extending to the right.

Peter A. Modafferi
Chief of Detectives
Chair, IACP Police Investigative Operations Committee



Maricopa County Attorney
BILL MONTGOMERY

301 WEST JEFFERSON STREET, SUITE 800
PHOENIX, ARIZONA 85003
WWW.MARICOPACOUNTYATTORNEY.ORG

PH. (602) 506-1260
TDD (602) 506-4352
FAX (602) 506-8102

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts of Apple and Google to upgrade the encryption features of the software for their mobile devices that would render them impervious to law enforcement efforts to secure information pursuant to search warrants and similar judicial authorization.

While I fully understand and appreciate the tremendous value of individual privacy as a touchstone of liberty and a right protected by our constitution subject to specific requirements before it may be intruded upon, the terrible impact that Apple's and Google's actions will render on crime victims and public safety across the country must also be considered. Simply put, when criminal wrongdoers can hide the evidence of their crimes on their mobile devices and when that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will be victorious.

For example, mobile devices with the new technology could easily be used to securely store evidence we are able to currently obtain in the following types of cases: creation and/or sharing of child pornography images or videos; sexual conduct with a minor, images or videos of the defendant's sexual contact with a victim; and, homicides where text messages prove a defendant's pre-meditation or rebut a claim of self-defense or simply disprove assertions of an alibi or the involvement of accomplices.

At the same time, it is difficult to believe that Apple, Google, or any other company can actually develop encryption software that will be permanently impenetrable. History provides numerous examples of codes that proved only temporarily impenetrable, yet few, if any, examples of codes that were never decrypted. Thus, it is likely that this new encryption technology will eventually be compromised. In the meantime, however, crime victims and public safety will suffer.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, strike a balance between enforcement of the law and protection of individual liberty. They require probable cause and warrants issued by judges – not prosecutors – before mobile devices may be searched. Accordingly, I encourage this Committee to adopt a solution to this challenge that strikes an appropriate balance between

individual liberty and law enforcement. Permitting Apple and Google to make their mobile devices impervious to *lawful* governmental searches clearly does not strike an appropriate balance and public safety will suffer if they are allowed to adopt these measures.

Respectfully,

A handwritten signature in blue ink, appearing to read "Bill Montgomery", with a long horizontal flourish extending to the right.

Bill Montgomery
Maricopa County Attorney



HILLAR C. MOORE, III

DISTRICT ATTORNEY, 19TH JUDICIAL DISTRICT
EAST BATON ROUGE PARISH

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to urge you to take the necessary measures to prevent Apple and Google from making their smartphones absolutely inaccessible to law enforcement.

I value every citizen's right to privacy and fully support the fourth amendment to the United States Constitution and the resulting requirement of a search warrant in order for law enforcement to search smartphones. The protection that citizens enjoy from unreasonable search of the information on their smartphones is already as stringently protected as is the protection afforded from unreasonable search of their homes. It is inconceivable to me, that we as a country, would elect to afford criminals who consistently use their smartphones; to aid in the commission of their crimes, to hide evidence of crime, and to even intimidate witnesses to their crimes; an absolute protection against law enforcement discovery of evidence and use of evidence against them.

As technology continuously improves, criminals figure out new ways to use their smartphones to aid in their criminal enterprises. Please do not let Apple and Google hinder law enforcement from protecting the public. It is irresponsible for Apple and Google to provide this technology without any check on its use to prey on potential victims. The evidence obtained from phones has been vital to the prosecution of murder, rape, and racketeering cases in my office. This evidence has also been used by local law enforcement to clear individuals suspected of crimes.

Law enforcement is already feeling the effects of these changes. The case described below and reported in Baton Rouge City Police file number 36160-15 is only one example of a homicide that may go unsolved due to the inability of law enforcement to access the information on a cell phone.

On Friday, April 24, 2015, at approximately 2238 hours, Uniform Patrol Officers responded to a Baton Rouge address in reference to a pregnant black female who had been shot. The victim was approximately 8 months pregnant and was rushed to the hospital with life threatening gunshot wounds. Detectives learned during the investigation that the victim and her 9 year old daughter had just arrived at home when an unknown person knocked on the front door. The 9 year old saw the victim open the door and heard an unknown black male ask

OFFICE OF THE DISTRICT ATTORNEY
222 ST. LOUIS STREET • 5TH FLOOR • BATON ROUGE, LA 70802
WWW.EBRDA.ORG • PHONE: 225-389-3400 • FAX: 225-389-5482

the victim to use her car. The victim told the subject "no", at which time he fired several shots striking the victim. The victim's daughter hid in the bathroom until police arrived. The child told police that she did not see who was at the door and didn't recognize the voice. The doctors removed the newborn from the victim's womb and then the victim died during surgery. The newborn was initially stable but died one week later.

The victim's iPhone 5 was seized during the execution of a search warrant at her residence and is passcode protected. The victim's family consented to the search of the phone and gave investigators several codes that they thought the victim might use. None of the passcodes worked and detectives were unable to access the phone.

As of July 2, 2015 no arrest has been made in this matter. The victim's family indicated that she recorded all activity on her phone and join law enforcement in their frustration due to the inability to access this phone, that would in all likelihood provide information necessary to obtain justice and remove this murderer from the street.

Respectfully,

By


HILLAR C. MOORE, III


National District Attorneys Association

99 Canal Center Plaza, Suite 330, Alexandria, Virginia 22314

703.549.9222 / 703.836.3195 Fax

www.ndaa.org

July 7, 2015

The Honorable Charles Grassley
 Chairman
 Senate Judiciary Committee
 135 Hart Senate Office Building
 Washington, DC 20510

Dear Chairman Grassley,

On behalf of the National District Attorneys Association (NDAA), the largest prosecutor organization representing 2500 elected and appointed District Attorneys across the United States as well as 40,000 assistant district attorneys, I want to bring to your attention our growing concern over Apple and Google's latest operating systems' use of encryption, which prevents law enforcement from accessing vital information used in investigations throughout this country. Although our members share their concerns regarding the security of information of their customers and the desire to prevent hackers from accessing personal information, we also see the potential danger this could cause to the investigative process and lawful access by law enforcement of evidence used to prosecute cases.

In today's courtrooms, more and more evidence is in a digital form as smartphones and other electronic devices continue to flood the market and continue to grow as a tool for criminals to commit all kinds of crimes including fraud, drug trafficking, child abduction, domestic violence and distribution of child pornography. Law enforcement must be able to collect crucial digital evidence from today's smartphones, while ensuring that privacy rights are maintained and lawful judicial oversight is executed. 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.

I hope that as you listen to testimony as part of Wednesday's hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy", you will consider the challenges faced by law enforcement to keep our communities safe and the necessity of lawful access to an increasingly large amount of digital evidence in our cases. Given our nation's proud history of innovation, our members hope that law enforcement and experts in the technology industry can come together to find a balanced solution to maintain the privacy rights of individuals across the country, while still ensuring that law enforcement can obtain the evidence it needs to take criminals off the street and protect the citizens of this country.

Respectfully,

Michael Moore
 President
 National District Attorneys Association

To Be the Voice of America's Prosecutors and to Support Their Efforts to Protect the Rights and Safety of the People



State of North Carolina
General Court of Justice
Twenty-Sixth Prosecutorial District
 MECKLENBURG COUNTY

R. ANDREW MURRAY
 DISTRICT ATTORNEY

MECKLENBURG COUNTY
 DISTRICT ATTORNEY'S OFFICE
 700 EAST TRADE ST.
 CHARLOTTE, NC 28202
 TELEPHONE: 704-686-0700
 FAX: 704-686-0712
 OR 704-686-0718

July 7, 2015

United States Senate Committee on the Judiciary
 224 Dirksen Senate Office Building,
 Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy

Dear Senators:

I am writing to express my grave concern about Apple's and Google's significant efforts to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

In my district we have had numerous cases that have been solved, including murder cases, with the search of cell phones pursuant to search warrants. Without the capability of searching these phones I would still have murderers on the streets of Charlotte that have already displayed their willingness to senselessly take the life of another.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches. I implore you to prevent this lunacy and to maintain a proper balance between privacy rights and the need to investigate evidence where probable cause exists in order to protect the victims and citizens of this great country.

Respectfully,

R. Andrew Murray,
 District Attorney
 Mecklenburg County, NC (Charlotte)



NATIONAL SHERIFFS' ASSOCIATION

JONATHAN F. THOMPSON
Executive Director

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

On behalf of the National Sheriffs' Association and the more than 3,000 elected sheriffs nationwide, I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Sincerely,

A handwritten signature in black ink, appearing to read "Jonathan F. Thompson".

Jonathan F. Thompson

Hamilton County District Attorney
Hon. Marsha King Purdue
P.O. Box 277
Indian Lake, New York, 12842
(518) 648-5113
Fax (518) 648-5724
Service by fax not accepted
districtattorney@hamiltoncountyny.gov

District Attorney
Marsha King Purdue

Assistant District Attorney
Sterling T. Goodspeed

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

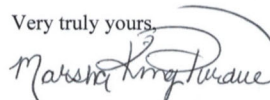
Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Very truly yours,



Marsha King Purdue
District Attorney



ASHLEY M. RICH

DISTRICT ATTORNEY
STATE OF ALABAMA
Thirteenth Judicial Circuit

July 15, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered.

Hundreds of crimes each year in Mobile County are solved when law enforcement does their job and secures a valid search warrant subject to the constitution and the law and is able to search a cell phone. Hundreds of victims of crime have been provided Justice and their perpetrator has been convicted of the criminal acts they committed because of lawful search warrants of smart phones.

If your efforts are successful then you will be responsible for giving criminals another avenue by which they can thwart the justice system and you are saying to the victims of crime that you just don't care about their rights and the fact that they don't deserve to be hurt by these criminals. You are also saying loud and clear that you choose criminals over victims.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Ashley M. Rich



STATE ATTORNEY
ELEVENTH JUDICIAL CIRCUIT OF FLORIDA
E. R. GRAHAM BUILDING
1350 N.W. 12TH AVENUE
MIAMI, FLORIDA 33136-2111

KATHERINE FERNANDEZ RUNDLE
STATE ATTORNEY
KatherineFernandezRundle@MiamiSAO.com

TELEPHONE (305) 547-0100
www.miamiSAO.com

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the
Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Sincerely,

KATHERINE FERNANDEZ RUNDLE
State Attorney

KFR:apm



Please Recycle

2 Lafayette Street 3rd Floor NY NY 10007
T 212.577.7700 F 212.385.0331 www.safehorizon.org



July 1, 2015

Hon. Charles Grassley, Chair
Judiciary Committee
United States Senate
135 Hart Senate Office Building
Washington, D.C. 20510

Hon. Patrick Leahy, Ranking Member
Judiciary Committee
United States Senate
437 Russell Senate Office Building
Washington, D.C. 20510

RE: Smart phone encryption and the impact on crime victims

Dear Chairman Grassley and Ranking Member Leahy:

On behalf of Safe Horizon, the nation's leading victim assistance organization and New York City's largest provider of services to victims of violence and abuse, I write to express my serious concern that smart phone encryption practices currently in use in the overwhelming majority of mobile devices will put victims of child abuse, sexual assault and other crimes at grave risk of further harm. In short, law enforcement officials are unable to recover evidence of criminal activity from password protected devices. It is my sincere hope that you and your colleagues on the Senate Judiciary Committee will insist that companies such as Apple and Google immediately revisit their policies that ultimately prevent law enforcement officials across the country from keeping children and adults safe from dangerous predators. We advocate in concert with New York County District Attorney Cyrus Vance, Jr. and prosecutors around the country who are increasingly unable to retrieve needed evidence that would keep families and communities safe and bring offenders to justice.

Staff across many programs at Safe Horizon have seen absolutely horrific images and text messages related to violent physical and sexual abuse that traditionally have led to the arrest and prosecution of individuals whose devices housed these images. But since September of 2014, the most recent smart phone operating systems do not allow these companies to access data on password protected devices. With nearly every device now protected in this way, the aforementioned companies are unable to bypass the user's password and access images and text that could provide convincing evidence of some of our nation's most serious crimes.

To help illustrate our concern, I would like to share with you just one example of child abuse evidence that was sent to me from staff in our nationally recognized Child Advocacy Centers. With

the new operating systems in place, the evidence described below would remain hidden from our law enforcement partners:

In early 2014, a mother noticed troubling posts on her 12-year old daughter's Facebook page indicating incidents of abuse. When the mother asked for more information later that evening, the daughter tearfully recounts being raped by someone she just met. The mother and daughter immediately went to the nearest precinct and an investigation into the incident ensued. After providing a description of her assailant and the location where the crime took place, the police eventually found and arrested him. Because the victim had earlier noted that he took images of her performing sexual acts, the police obtained a warrant to search all of the assailant's electronic devices – including his phone. Horrifyingly enough, his phone's screensaver was an image of him sexually assaulting this young girl. Additionally, the police found many other vile and disturbing images that further tied him to this crime.

As the investigation unfolded, the police found images of other children and learned the assailant was a recruiter for a large human trafficking ring that involved many, many victims, most under the age of 12. With evidence from the phones and testimony from the victims, the operators of the trafficking ring are now facing justice.

If this same case were to happen today under current smart phone encryption practices, these images of childhood sexual abuse might never have been found. Furthermore, it was because of the search of the assailant's electronic devices that a critical piece of evidence that tied the initial defendant to the larger human trafficking ring was uncovered. As a result, many other child victims were discovered who otherwise may not have been.

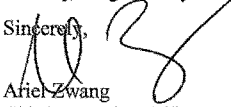
This is just one chilling example of many I could sadly share with you. Stories like these clearly demonstrates why Apple and Google must immediately take steps to ensure that law enforcement officials with judicial warrants can bypass encrypted electronic devices and obtain concrete evidence of criminal activity. While we respect the concern for privacy, allowances must be made to ensure that evidence of criminal activity can be discovered and that communities can remain safe. I reiterate my earlier plea for the Senate to lead the way in compelling these and other companies to reverse their current encryption policies.

On behalf of our staff, our Board of Directors and most of all the more than 250,000 New Yorkers affected by crime whose lives we touch each year, I thank you in advance for your consideration of our request.

If you have any questions or would like more information about our concerns, please feel free to contact my colleague Michael Polenber, Vice President of Government Affairs, at (212) 577-7735.

Thank you again for your attention to this matter.

Sincerely,


Ariel Zwang
Chief Executive Officer

About Safe Horizon

Safe Horizon is the nation's leading victim assistance organization and touches the lives of over 250,000 people each year who have been affected by violence. Our mission is to provide support, prevent violence and promote justice for victims of crime and abuse, their families and communities. We will lead the way by empowering victims of domestic violence, child abuse, sexual assault and human trafficking to move from crisis to confidence. Safe Horizon provides the practical tools, emotional support, education and advocacy to help victims and their families heal and rebuild their lives. For more information, please visit us online at www.safehorizon.org



Polk County Attorney

JOHN P. SARCONI
County Attorney

July 15, 2015

ADDRESS REPLY TO:
212 Fifth Avenue
Des Moines, IA 50399-4025
(515) 286-3137
Fax (515) 286-3428

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Re: *Going Dark: Encryption, Technology, and the Balance Between
Public Safety and Privacy*

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Sincerely,

A handwritten signature in cursive script, appearing to read "John P. Sarcone".
JOHN P. SARCONI
Polk County Attorney

JPS:rcp



OFFICE OF THE ERIE COUNTY DISTRICT ATTORNEY

FRANK A. SEDITA, III
DISTRICT ATTORNEY

July 14, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

As the immediate past President and Board Chairman of the District Attorney's Association of the State of New York (DAASNY), I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

Digital evidence plays a crucial role in many criminal cases across our state, and, indeed, across the nation. Because so many people put extensive information on their smartphones and hand-held devices, those devices may contain photos, texts, voice messages, or emails that will constitute relevant evidence in virtually every kind of case. We have lawfully used material from smartphones to prosecute murders, rapes, kidnappings, fraud, and larceny, among other crimes.

For law enforcement to access the contents of a smartphone or similar device, we typically need and obtain a search warrant. A search warrant cannot be issued unless the applicant demonstrates, to a judge, that there is both probable cause to believe a crime has been committed and probable cause to believe the device contains evidence of that crime.

If a smartphone is protected by a passcode, however, then even though the search warrant gives us the legal right to access the contents of the phone, we cannot review the material on the phone because we cannot get "through" the passcode.

Historically, in such instances we have been able to seek the aid of the mobile operating system providers. Upon our presentation to them of the warrant, they have been able to unlock the phones, and provide the information on the phone that was responsive to the warrants.

United States Senate Committee on the Judiciary
 July 14, 2015
 Page Three

In the past few months, however, companies have deliberately designed software, entire operating systems, and mobile devices such that even *they* cannot unlock passcode-protected phones. These companies have touted this development, explicitly advertising their inability to comply with lawful government requests. As a consequence, the search warrant becomes a nullity, because even law enforcement officers possessing valid search warrants or court orders cannot access the contents of passcode-protected smartphones. In other words, criminals using passcode-protected devices have been granted license to evade a lawful order of a court and are thus quite literally, protected in their criminal endeavors.

It is as if the police get a search warrant for a safe deposit box at a bank because they have reason to believe that the safe deposit box has evidence of a crime -- but they cannot open the box because the bank has thrown away its own key. Indeed, this situation is even worse because whereas a safe deposit box can, ultimately, be opened by force, a passcode-protected smartphone is virtually impregnable, unless the companies maintain the ability to open the phones that it manufactures.

Although companies tout their new software as a boon for their users' privacy, users' privacy is adequately protected by the Fourth Amendment, and specifically the requirement that a judge or magistrate -- that is, a neutral party -- issue a search warrant only upon a showing of probable cause that the phone will contain evidence of a crime.

The fact is that, although the new software may enhance privacy for some users, it severely hampers law enforcement's ability to aid victims. All of the evidence contained in smartphones and similar devices will be lost to law enforcement, so long as the criminals take the precaution of protecting their devices with passcodes.

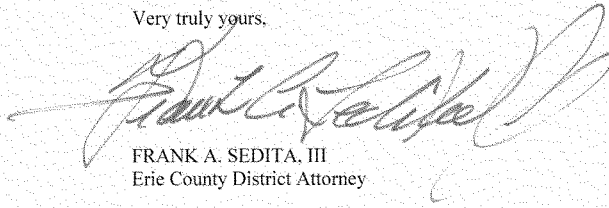
As previously mentioned, The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges -- not prosecutors -- before smartphones may be searched. Those warrants will be a nullity if companies such as Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches. In short, passcode-protected devices render lawful court orders meaningless and encourage criminals to act with impunity.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. If criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

United States Senate Committee on the Judiciary
July 14, 2015
Page Three

Thank you for the courtesy of considering my concerns on this important issue.

Very truly yours,

A handwritten signature in dark ink, appearing to read "Frank A. Sedita, III", is written over a background of a repeating wavy pattern.

FRANK A. SEDITA, III
Erie County District Attorney

FAS/dms

Harms Caused by Edward Snowden

In his theft of over one million sensitive U.S. intelligence documents,¹ Edward Snowden:

- **Indiscriminately released classified intelligence information that goes far beyond Snowden’s professed concerns with so-called domestic surveillance programs.** In a John Oliver interview,² Snowden admitted that he did not actually read the documents before turning them over to journalists.
- **Exposed sensitive operations against Al Qaeda—operations that had no relevance to privacy concerns in the U.S.—a mistake even Snowden described as a “f***-up”.**³ According to the AP, some of the leaked documents exposed the names of at least six intelligence workers.⁴
- **Damaged the reputation of the U.S. and strained relationships with foreign allies.** According to Director of National Intelligence James Clapper, as a result, “we’ve lost critical foreign intelligence collection sources, including some shared with us by valued partners.”⁵
- **Alerted terrorists to the methods used by intelligence services and enabled them to take countermeasures to escape our intelligence gathering.** According to then-NCTC Dir. Matthew Olsen, there have been “specific instances where [terrorist groups

¹¹ Michael B Kelley, *NSA: Snowden Stole 1.7 Million Classified Documents and Still Has Access to Most of Them*, BUSINESS INSIDER, (Dec. 13, 2013, 4:52 PM), <http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12>.

² LastWeekTonight, *Last Week Tonight with John Oliver: Government Surveillance (HBO)*, YouTube (Apr. 5, 2015), https://www.youtube.com/watch?v=XEVlyP4_11M.

³ Justin Wm. Moyer, *John Oliver’s Hilarious Interview with Edward Snowden*, THE WASHINGTON POST (Apr. 6, 2015), <http://www.washingtonpost.com/news/morning-mix/wp/2015/04/06/john-olivers-hilarious-interview-with-edward-snowden/>.

⁴ Raphael Satter, *Media Sometimes Try, Fail to Keep NSA’s Secrets*, THE ASSOCIATED PRESS (Feb. 8, 2015), available at <http://news.yahoo.com/media-sometimes-try-fail-keep-nsa-39-secrets-133744876.html>.

⁵ James R. Clapper, Director of National Intelligence, Remarks on Worldwide Threat Assessment Delivered to the Senate Select Committee on Intelligence (Jan. 29, 2014) available at http://www.dni.gov/files/documents/WWTA%20Opening%20Remarks%20as%20Delivered%20to%20SSCI_29_Jan_2014.pdf

have] changed the ways in which they communicate to avoid being surveilled or being subject to our surveillance tactics.”⁶

- **Put at risk important collection methods.** According to Director of National Intelligence James Clapper: “Critical intelligence capabilities in which the United States has invested billions of dollars are at risk, or likely to be curtailed or eliminated either because of compromise or conscious decision.”⁷ Then-DIA Dir. Lt. Gen. Michael Flynn echoed these concerns: “The cost [is] to our nation in treasure, in capabilities that are going to have to be examined, reexamined and potentially adjusted.”⁸
- **Endangered the lives of our troops.** Then-DIA Dir. Lt. Gen. Michael Flynn stated: “I think that potentially the greatest cost is unknown today, but we will likely face, is the cost in human lives in tomorrow's battlefield in someplace where we put our military forces in harm's way.”⁹

⁶ James Gordon Meek, Luis Martinez & Alexander Mallin, *Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security*, ABC News (Jan. 29, 2014), <http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388&singlePage=true>.

⁷ Clapper, *supra* note 4.

⁸ Meek, *supra* note 5.

⁹ *Id.*



MADELINE SINGAS
ACTING DISTRICT ATTORNEY

OFFICE OF
THE DISTRICT ATTORNEY
NASSAU COUNTY

July 15, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

RE: Going Dark: Encryption, Technology, and the
Balance between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders. I currently serve as the acting District Attorney in Nassau County, New York. Nassau County is a large suburban county, immediately adjacent to the five boroughs of New York City, with an estimated resident population of 1.35 million (making it more populous, as a county, than ten of the fifty States and the District of Columbia). Furthermore, sitting in the geographic middle of Long Island, Nassau serves as a major conduit between the city, with its 8.5 million residents, and Suffolk County, with its 1.5 million residents. Accordingly, Nassau County has its share of enterprise crime, gang activity, narcotics trafficking, human trafficking, cyber-crime (including child pornography enterprises), and other complex criminal ventures. Accordingly, I am no stranger to complex investigations and high-tech evidence collection.

The above efforts of Apple and Google will devastate both crime prevention strategy and criminal enforcement strategy in my county and state. The perpetrators of the categories of crime that I just listed above will attain and hold the upper hand permanently. This means children exploited for pornography, women exploited in the sex trade, rampant gang violence, undetectable organized crime, and untraceable drug networks. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go unpunished, and the safety of all of our citizens will be diminished. In the “arms race” between criminals and law enforcement, the criminals will have won.

Over the past century – we have gone from filing cabinets, to desktop computers, to pocket smart-phones. As the manner of data and document storage has evolved, however, the Fourth Amendment of the United States Constitution has remained constant – and serves the steadfast protection of a citizen’s privacy. This amendment, and similar provisions in state constitutions, require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

This is not a matter of unfettered discretion or power to search and seize intimate details of a

person's private life. This is a matter of public safety. The technological efforts of Apple and Google to frustrate law enforcement, in a world which is only becoming more smart-phone dependent, will cripple law enforcement in the 21st Century.

Respectfully yours,

A handwritten signature in black ink, reading "Madeline Singas". The signature is fluid and cursive, with the first name "Madeline" and last name "Singas" clearly distinguishable.

Madeline Singas
Acting District Attorney
Nassau County

State of South Carolina
OFFICE OF THE SOLICITOR
FOURTEENTH JUDICIAL CIRCUIT

ALLENDALE, BEAUFORT
COLLETON, HAMPTON AND
JASPER COUNTIES



POST OFFICE BOX 1880
BLUFFTON, SOUTH CAROLINA 29910
TELEPHONE: (843) 255-5880
FACSIMILE: (843) 255-9512

Isaac McDuffie Stone, III
SOLICITOR

July 10, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

**Re: Going Dark: Encryption, Technology, and the Balance Between Public
Safety and Privacy**

Dear Senators:

I am deeply concerned about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Gang members and other criminals use cell phones to plan and execute murders, armed robberies, human trafficking and many other crimes. They use these phones as tools of their trade. If criminals can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Isaac McDuffie Stone, III



Kenneth P. Thompson
District Attorney

DISTRICT ATTORNEY
KINGS COUNTY
350 JAY STREET
BROOKLYN, NY 11201-2908
(718) 250-2000
WWW.BROOKLYNDA.ORG

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

Re: Going Dark: Encryption, Technology, and the Balance Between Public
Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to lawful governmental searches.

Respectfully,

A handwritten signature in black ink, appearing to read "K. Thompson".

Kenneth P. Thompson
Brooklyn District Attorney



ROD UNDERHILL, District Attorney for Multnomah County
1021 SW Fourth Avenue • Room 600 • Portland, OR 97204-1193
Phone: 503 988-3162 • Fax: 503 988-3643 • www.mcda.us

July 2, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: **Going Dark: Encryption, Technology, and the Balance Between Public
Safety and Privacy**

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

ROD UNDERHILL
District Attorney
Multnomah County, Oregon



OFFICE OF THE DISTRICT ATTORNEY GENERAL

30th JUDICIAL DISTRICT ~ SHELBY COUNTY, TENNESSEE
 201 Poplar Avenue, Third Floor, Memphis, TN 38103-1947
 Tel. 901-222-1300 ~ Fax 901-222-1305
www.scdag.com

AMY P. WEIRICH
District Attorney General

July 6, 2015

United States Senate Committee on the Judiciary
 224 Dirksen Senate Office Building,
 Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

 AMY P. WEIRICH
 District Attorney General

APW/cjg



WEEDEN A. WETMORE
District Attorney

DISTRICT ATTORNEY'S OFFICE
COUNTY OF CHEMUNG
226 Lake Street
P.O. Box 588
Elmira, New York 14902-0588

Phone: (607) 737-2944
Fax: (607) 737-2965

July 14, 2015

JOHN R. THWEATT
Chief Assistant

JASON COOK
STEPHEN R. HOFFMANN
JEREMY HOURIHAN
SOPHIE MARMOR
KEVIN M. O'SHEA
SUSAN RIDER-ULACCO
DAMIAN M. SONSIRE
JORDAN J. YORKE
Assistant District Attorneys

MICHAEL MARRONE
JAMES J. WILLIAMS
Investigators

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: **Going Dark: Encryption, Technology, and the Balance Between
Public Safety and Privacy**

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminal wrongdoers can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Weeden A. Wetmore



DISTRICT ATTORNEY'S OFFICE
THREE SOUTH PENN SQUARE
PHILADELPHIA, PENNSYLVANIA 19107-3499
(215) 686-8000

R. SETH WILLIAMS
DISTRICT ATTORNEY

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to encrypt their smartphones in a manner that will make data on these devices inaccessible to law enforcement, even if we have received a search warrant or similar judicial orders.

Such a decision will help criminals stay many steps ahead of law enforcement. Moreover, the decision will allow criminals – even the less sophisticated ones – to hide the evidence of their criminal activity on their smartphones. Because of the encryption, the evidence will be beyond the reach of law enforcement even when we have a search warrant. The real winners from this decision by Apple and Google are the criminals – child pornographers, gang members, and sophisticated illegal drug enterprises. As we deal with the increasing storage of child pornography on cellphones, with tech-savvy drug dealers employing cellphones as a tool in the heroin trade, with gang leaders using their cellphones to store valuable information that could help us solve brutal killings, and instances of witness intimidation, why would anyone take affirmative steps to hand them tools to make it easier to create more victims?

I fully understand the concerns that many have about bulk collection of data. These concerns are legitimate and worthy of continued debate. But what Apple and Google have proposed will effectively nullify search warrants, which meet the standards of the Fourth Amendment and in my state, the Pennsylvania Constitution.

The concerns raised by, among others, District Attorney Vance, FBI Director Comey, and Police Commissioner Bratton must be taken seriously. I do not want to have to face a victim of a violent crime and tell him or her that we cannot prosecute the offender because critical information on their smartphone is inaccessible.

As with so many other things in the criminal justice system, there is a balance. I hope we can collectively find such a balance on this critical issue.

Respectfully,

R. Seth Williams
District Attorney
City of Philadelphia



**CLARK COUNTY
OFFICE OF THE DISTRICT ATTORNEY**

Administration Division

STEVEN B. WOLFSON
District Attorney

200 Lewis Avenue • Las Vegas, NV 89101 • 702-671-2500 • Fax: 702-455-2294 • TDD: 702-385-7486

MARY-ANNE MILLER
County Counsel

CHRISTOPHER LALLI
Assistant District Attorney

ROBERT DASKAS
Assistant District Attorney

JEFFREY WITTHUN
Director D.A. Family Support

July 7, 2015

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the terrible cost that Apple's and Google's actions will have on state and local law enforcement, and on crime victims across the country, must also be considered. Simply put, if criminals can hide the evidence of their crimes on their smartphones, and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free, and the safety of all of our citizens will be diminished. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,

Steven B. Wolfson
Clark County District Attorney



ANDREW J. WYLIE
District Attorney

OFFICE OF THE
CLINTON COUNTY
DISTRICT ATTORNEY
Clinton County Government Center
137 Margaret Street, Suite 201
Plattsburgh, New York 12901



Tel. (518) 565-4770
Fax. (518) 565-4777

United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building,
Washington, D.C. 20510-6050

Re: Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy

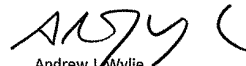
Dear Senators:

I am writing to express my concern about the efforts that Apple and Google have made to make their smartphones impervious to search warrants and similar judicial orders.

While I fully understand and appreciate the tremendous value of privacy, the excessive cost that Apple's and Google's actions will have on state and local law enforcement, as well as on crime victims across the country, must also be considered. Simply put, if a perpetrator can hide the evidence of their crimes on their smartphones and if that evidence is forever beyond the reach of law enforcement, then crimes will go unsolved, criminals will go free and the safety of all of our citizens will be put in jeopardy. In the "arms race" between criminals and law enforcement, the criminals will have won.

The Fourth Amendment of the United States Constitution, and similar provisions in state constitutions, protect citizens' privacy. They require probable cause and warrants issued by judges – not prosecutors – before smartphones may be searched. Those warrants will be a nullity if Apple and Google are permitted to make their smartphones impervious to *lawful* governmental searches.

Respectfully,


Andrew J. Wylie
Clinton County District Attorney

AJW/mw