

S. HRG. 114-739

COUNTERTERRORISM, COUNTERINTELLIGENCE, AND THE CHALLENGES OF “GOING DARK”

HEARING BEFORE THE SELECT COMMITTEE ON INTELLIGENCE OF THE UNITED STATES SENATE ONE HUNDRED FOURTEENTH CONGRESS FIRST SESSION

WEDNESDAY, JULY 8, 2015

Printed for the use of the Select Committee on Intelligence



Available via the World Wide Web: <http://www.fdsys.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

27-896 PDF

WASHINGTON : 2018

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

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*
DIANNE FEINSTEIN, California, *Vice Chairman*

JAMES E. RISCH, Idaho	RON WYDEN, Oregon
DANIEL COATS, Indiana	BARBARA A. MIKULSKI, Maryland
MARCO RUBIO, Florida	MARK WARNER, Virginia
SUSAN COLLINS, Maine	MARTIN HEINRICH, New Mexico
ROY BLUNT, Missouri	ANGUS KING, Maine
JAMES LANKFORD, Oklahoma	MAZIE K. HIRONO, Hawaii
TOM COTTON, Arkansas	

MITCH McCONNELL, Kentucky, *Ex Officio*
HARRY REID, Nevada, *Ex Officio*
JOHN McCain, Arizona, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
DAVID GRANNIS, *Minority Staff Director*
DESIREE THOMPSON-SAYLE, *Chief Clerk*

CONTENTS

JULY 8, 2015

OPENING STATEMENTS

Burr, Hon. Richard, Chairman, a U.S. Senator from North Carolina	1
Feinstein, Hon. Dianne, Vice Chairman, a U.S. Senator from California	58

WITNESS

Comey, Hon. James B., Director, Federal Bureau of Investigation	59
Prepared statement	63

SUPPLEMENTAL MATERIAL

Computer Science and Artificial Intelligence, Laboratory Technical Report dated July 6, 2015, entitled “Keys Under Doormats”	4
Letter from the American Civil Liberties Union dated July 7, 2015	38
Letter from the Business Software Alliance dated July 8, 2015	47
Remarks of Director Comey to the Brookings Institution on October 16, 2014 .	50

COUNTERTERRORISM, COUNTERINTELLIGENCE, AND THE CHALLENGES OF “GOING DARK”

WEDNESDAY, JULY 8, 2015

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:33 p.m. in Room SH-216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Committee Members Present: Burr, Feinstein, Risch, Coats, Collins, Blunt, Lankford, Cotton, McCain, Wyden, Mikulski, Warner, Heinrich, and Hirono.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. Good afternoon. I call this hearing to order. I'd like to welcome our witness today, Director of the Federal Bureau of Investigation, James Comey. I would note that Director Comey appeared this morning before the Senate Judiciary Committee. Jim, I appreciate your appearing before us now and enduring a long day of Congressional testimony. I know the Vice Chair has had an opportunity to have a bite at you, but she wanted one more, she told me.

As we often conduct hearings in closed session, I'd like to take this opportunity to publicly commend the Director and the men and women of the FBI for their outstanding efforts in keeping our country safe. It is due in no small part to FBI vigilance in concert with the intelligence community partners that our Nation's enjoyed peaceful and safe Independence Day celebrations this past weekend.

Director Comey, as you're well aware, extremists fueled by anti-Western propaganda remain intent on inflicting harm on U.S. interests at home and abroad. Over the past year we've witnessed the Islamic State of Iraq and the Levant, also referred to as "ISIL" or the "Islamic State" or "Daesh," attempt to inspire a wide range of individuals to conduct attacks against innocent civilians.

Largely as a result of ISIL's media savvy, the number of U.S.-based individuals in 2015 seeking to conduct attacks in the homeland or overseas to join ISIL has already exceeded the combined number of individuals attempting these activities in 2013 and 2014.

Unfortunately, the threats facing our Nation are not limited to terrorist actors. Foreign governments remain intent on stealing our country's most valuable trade, intellectual property and national security secrets. The FBI is charged with confronting all these threats as well and is continually challenged by the capabilities and tradecraft employed by these nation-state actors.

In addition to these fairly unique jurisdictional issues, the FBI conducts routine law enforcement investigations of drug trafficking, theft of government property, child pornography, robbery, extortion, murder, and the list goes on and on and on. These criminals are also turning to encrypted communications as a means of evading detection. These two issues that might at first glance appear unrelated are in fact closely linked.

Communications between a terrorist organization's operational commanders and field soldiers require enabling technology. Communications between a foreign state and its spies also requires enabling technology. In both cases, the enabling technology used by terrorists and foreign state spies is increasingly secure encrypted communications. Both of these adversaries are taking advantage of the rapid advances in secure communications that are employing advanced—that are employing advanced commercially available encryption.

Director, as I understand the issue, even when law enforcement has the legal authority to intercept and access communications pursuant to a court order, you may lack the technical ability to do so. This is what you've referred to and others have referred to as "Going Dark." You've described it as one of the biggest challenges facing your agency and law enforcement generally. This challenge falls at the intersection of technology, law, freedom, and security.

It results from the adoption of universal encryption. These applications are designed so that only the user has the key to decode their content. In these cases, when the FBI or any other law enforcement agency requests access to a user's communications via a lawful warrant, it is inaccessible or unreadable. It does not matter whether the user is a suspected terrorist, a child molester, a spy or a drug trafficker; law enforcement's blind and becoming so, and as a result we're less safe.

I, like all Americans, desire privacy. As Americans we're guaranteed the right to be secure pursuant to the Fourth Amendment in our persons, houses, papers and effects. I'm also concerned, though, as are our fellow members, about the terrorist, counterintelligence and other criminal threats to those very same things. I strongly believe that we must identify a solution that first protects American privacy, but also allows for lawful searches under valid court orders.

Director Comey, you said that the encryption now readily available—and I quote—"is equivalent to a closet that can't be opened or a safe that can't be cracked," unquote. You have an opportunity today to speak to the Committee and to the American people and to convince us that in order to keep the American people safe, you need to be able to open the closet or to crack the safe. There are no easy answers and we're embarking on what will be a robust debate that I think it was initiated by you and I think that's a good thing.

Director, you wrote on Monday that part of your job is to make sure the debate is informed by a reasonable understanding of the cost. I look forward to your testimony, this discussion, and I appreciate you being here.

Before I turn to the Vice Chairman for her remarks, I'd like to ask unanimous consent to enter several documents into the record. The first is the Computer Science and Artificial Intelligence Laboratory Technical Report dated July 6th, 2015, entitled "Keys Under Doormats."

[The material referred to follows:]



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, Matt Blaze, Whitfield Diffie,
John Gilmore, Matthew Green, Susan Landau,
Peter G. Neumann, 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, Matt Blaze,
Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann,
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.

July 7, 2015

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 arc

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 *forge* 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 Heartbleed 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.

Chairman BURR. The second letter, from the American Civil Liberties Union to the Committee, dated July 7th, 2015, on the topic of this hearing.

[The material referred to follows:]

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."

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL.
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0732
WWW.ACLU.ORG

MICHAEL W. MACLEOD-BALL
ACTING DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 16TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

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

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 US 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/ammem/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-be34-11e2-89c9-3be8095fe767_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%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/f8c1f590-3e81-11e4-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 Guliani
Legislative Counsel
American Civil Liberties Union
915 15th St., NW, Washington, DC 20005
202.675.2322
nguliani@aclu.org

The third is a letter from the Business Software Alliance dated July the 8th, 2015, again to this Committee and the Senate Judiciary Committee, on the topic of today's hearing.
[The material referred to follows:]



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 Richard Burr
Chairman
U.S. Senate Select Committee on Intelligence
221 Hart Senate Office Building
Washington, D.C. 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 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.

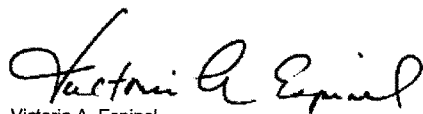
Calls for the weakening of encryption controls may also have international repercussions, which would further degrade many security measures protecting U.S. consumers. It is a reality that national borders do not limit threats to our citizens. Criminals, terrorists and other determined actors from around 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

And the fourth is the transcript of the Director's remarks to the Brookings Institute dated October 16th, 2014. Without objection, those four documents will be entered into the record.

[The material referred to follows:]

James B. Comey
 Director
 Federal Bureau of Investigation
 Brookings Institution
 Washington, D.C.
 October 16, 2014

Remarks as delivered.

Good morning. It's an honor to be here.

I have been on the job as FBI Director for one year and one month. I like to express my tenure in terms of months, and I joke that I have eight years and 11 months to go, as if I'm incarcerated. But the truth is, I love this job, and I wake up every day excited to be part of the FBI.

Over the past year, I have confirmed what I long believed—that the FBI is filled with amazing people, doing an amazing array of things around the world, and doing them well. I have also confirmed what I have long known: that a commitment to the rule of law and civil liberties is at the core of the FBI. It is the organization's spine.

But we confront serious threats—threats that are changing every day. So I want to make sure I have every lawful tool available to keep you safe from those threats.

An Opportunity to Begin a National Conversation

I wanted to meet with you to talk in a serious way about the impact of emerging technology on public safety. And within that context, I think it's important to talk about the work we do in the FBI, and what we need to do the job you have entrusted us to do.

There are a lot of misconceptions in the public eye about what we in the government collect and the capabilities we have for collecting information.

My job is to explain and clarify where I can with regard to the work of the FBI. But at the same time, I want to get a better handle on your thoughts, because those of us in law enforcement can't do what we need to do without your trust and your support. We have no monopoly on wisdom.

My goal today isn't to tell people what to do. My goal is to urge our fellow citizens to participate in a conversation as a country about where we are, and where we want to be, with respect to the authority of law enforcement.

The Challenge of Going Dark

Technology has forever changed the world we live in. We're online, in one way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us.

And with that comes a desire to protect our privacy and our data—you want to share your lives with the people you choose. I sure do. But the FBI has a sworn duty to keep every American safe from crime and terrorism, and technology has become the tool of choice for some very dangerous people:

Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.

We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, e-mail, and live chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos—or what we call "data at rest." And both real-time communication and stored data are increasingly encrypted.

Let's talk about court-ordered interception first, and then we'll talk about challenges posed by different means of encryption.

In the past, conducting electronic surveillance was more straightforward. We identified a target phone being used by a bad guy, with a single carrier. We obtained a court order for a wiretap, and, under the supervision of a judge, we collected the evidence we needed for prosecution.

Today, there are countless providers, countless networks, and countless means of communicating. We have laptops, smartphones, and tablets. We take them to work and to school, from the soccer field to Starbucks, over many networks, using any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, to target victims, and to cover up what they're doing. And that makes it tough for us to keep up.

If a suspected criminal is in his car, and he switches from cellular coverage to Wi-Fi, we may be out of luck. If he switches from one app to another, or from cellular voice service to a voice or messaging app, we may lose him. We may not have the capability to quickly switch lawful surveillance between devices, methods, and networks. The bad guys know this; they're taking advantage of it every day.

In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. And unfortunately, the idea that the government has access to all communications at all times has extended—unfairly—to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.

Some believe that the FBI has these phenomenal capabilities to access any information at any time—that we can get what we want, when we want it, by flipping some sort of switch. It may be true in the movies or on TV. It is simply not the case in real life.

It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight. But even with lawful authority, we may not be able to access the evidence and the information we need.

Current law governing the interception of communications requires telecommunication carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance. But that law, the Communications Assistance for Law Enforcement Act, or CALEA, was enacted 20 years ago—a lifetime in the Internet age. And it doesn't cover new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide lawful intercept capabilities to law enforcement.

What this means is that an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can't comply, because they have not developed interception capabilities. Other providers want to provide assistance, but they have to build interception capabilities, and that takes time and money.

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren't seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks—all designed to increase security and privacy.

With Apple's new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple's announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.

Both companies are run by good people, responding to what they perceive is a market demand. But the place they are leading us is one we shouldn't go to without careful thought and debate as a country.

At the outset, Apple says something that is reasonable—that it's not that big a deal. Apple argues, for example, that its users can back-up and store much of their data in "the cloud" and that the FBI can still access that data with lawful authority. But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement.

And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data.

Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?

Correcting Misconceptions

Some argue that we will still have access to metadata, which includes telephone records and location information from telecommunications carriers. That is true. But metadata doesn't provide the content of any communication. It's incomplete information, and even this is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't.

There is a misconception that building a lawful intercept solution into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit.

But that isn't true. 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 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.

Another misperception is that we can somehow guess the password or break into the phone with a so-called "brute force" attack. Even a supercomputer would have difficulty with today's high-level encryption, and some devices have a setting whereby the encryption key is erased if someone makes too many attempts to break the password, meaning no one can access that data.

Finally, a reasonable person might also ask, "Can't you just compel the owner of the phone to produce the password?" Likely, no. And even if we could compel them as a legal matter, if we had a child predator in custody, and he could choose to sit quietly through a 30-day contempt

sentence for refusing to comply with a court order to produce his password, or he could risk a 30-year sentence for production and distribution of child pornography, which do you think he would choose?

Case Examples

Think about life without your smartphone, without Internet access, without texting or e-mail or the apps you use every day. I'm guessing most of you would feel rather lost and left behind. Kids call this FOMO, or "fear of missing out."

With Going Dark, those of us in law enforcement and public safety have a major fear of missing out—missing out on predators who exploit the most vulnerable among us...missing out on violent criminals who target our communities...missing out on a terrorist cell using social media to recruit, plan, and execute an attack.

Criminals and terrorists would like nothing more than for us to miss out. And the more we as a society rely on these devices, the more important they are to law enforcement and public safety officials. We have seen case after case—from homicides and car crashes to drug trafficking, domestic abuse, and child exploitation—where critical evidence came from smartphones, hard drives, and online communication.

Let's just talk about cases involving the content of phones.

In Louisiana, a known sex offender posed as a teenage girl to entice a 12-year-old boy to sneak out of his house to meet the supposed young girl. This predator, posing as a taxi driver, murdered the young boy and tried to alter and delete evidence on both his and the victim's cell phones to cover up his crime. Both phones were instrumental in showing that the suspect enticed this child into his taxi. He was sentenced to death in April of this year.

In Los Angeles, police investigated the death of a 2-year-old girl from blunt force trauma to her head. There were no witnesses. Text messages stored on her parents' cell phones to one another and to their family members proved the mother caused this young girl's death and that the father knew what was happening and failed to stop it. Text messages stored on these devices also proved that the defendants failed to seek medical attention for hours while their daughter convulsed in her crib. They even went so far as to paint her tiny body with blue paint—to cover her bruises—before calling 911. Confronted with this evidence, both parents pled guilty.

In Kansas City, the DEA investigated a drug trafficking organization tied to heroin distribution, homicides, and robberies. The DEA obtained search warrants for several phones used by the group. Text messages found on the phones outlined the group's distribution chain and tied the group to a supply of lethal heroin that had caused 12 overdoses—and five deaths—including several high school students.

In Sacramento, a young couple and their four dogs were walking down the street at night when a car ran a red light and struck them—killing their four dogs, severing the young man's leg, and leaving the young woman in critical condition. The driver left the scene, and the young man died.

days later. Using “red light cameras” near the scene of the accident, the California Highway Patrol identified and arrested a suspect and seized his smartphone. GPS data on his phone placed the suspect at the scene of the accident and revealed that he had fled California shortly thereafter. He was convicted of second-degree murder and is serving a sentence of 25 years to life.

The evidence we find also helps exonerate innocent people. In Kansas, data from a cell phone was used to prove the innocence of several teens accused of rape. Without access to this phone, or the ability to recover a deleted video, several innocent young men could have been wrongly convicted.

These are cases in which we had access to the evidence we needed. But we’re seeing more and more cases where we believe significant evidence is on that phone or a laptop, but we can’t crack the password. If this becomes the norm, I would suggest to you that homicide cases could be stalled, suspects could walk free, and child exploitation might not be discovered or prosecuted. Justice may be denied, because of a locked phone or an encrypted hard drive.

My Thoughts

I’m deeply concerned about this, as both a law enforcement officer and a citizen. I understand some of this thinking in a post-Snowden world, but I believe it is mostly based on a failure to understand why we in law enforcement do what we do and how we do it.

I hope you know that I’m a huge believer in the rule of law. But I also believe that no one in this country should be above or beyond the law. There should be no law-free zone in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone’s closet or someone’s cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.

I think it’s time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so mistrustful of government—and of law enforcement—that we are willing to let bad guys walk away...willing to leave victims in search of justice?

There will come a day—and it comes every day in this business—where it will matter a great deal to innocent people that we in law enforcement can’t access certain types of data or information, even with legal authorization. We have to have these discussions now.

I believe people should be skeptical of government power. I am. This country was founded by people who were worried about government power—who knew that you cannot trust people in power. So they divided government power among three branches, with checks and balances for each. And they wrote a Bill of Rights to ensure that the “papers and effects” of the people are secure from unreasonable searches.

But the way I see it, the means by which we conduct surveillance through telecommunication carriers and those Internet service providers who have developed lawful intercept solutions is an

example of government operating in the way the founders intended—that is, the executive, the legislative, and the judicial branches proposing, enacting, executing, and overseeing legislation, pursuant to the rule of law.

Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust. It is time to have open and honest debates about liberty and security.

Some have suggested there is a conflict between liberty and security. I disagree. At our best, we in law enforcement, national security, and public safety are looking for security that enhances liberty. When a city posts police officers at a dangerous playground, security has promoted liberty—the freedom to let a child play without fear.

The people of the FBI are sworn to protect both security and liberty. It isn't a question of conflict. We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve—in every investigation.

Where Do We Go from Here?

These are tough issues. And finding the space and time in our busy lives to understand these issues is hard. Intelligent people can and do disagree, and that's the beauty of American life—that smart people can come to the right answer.

I've never been someone who is a scaremonger. But I'm in a dangerous business. So I want to ensure that when we discuss limiting the court-authorized law enforcement tools we use to investigate suspected criminals that we understand what society gains and what we all stand to lose.

We in the FBI will continue to throw every lawful tool we have at this problem, but it's costly. It's inefficient. And it takes time.

We need to fix this problem. It is long past time.

We need assistance and cooperation from companies to comply with lawful court orders, so that criminals around the world cannot seek safe haven for lawless conduct. We need to find common ground. We care about the same things. I said it because I meant it. These companies are run by good people. And we know an adversarial posture won't take any of us very far down the road.

We understand the private sector's need to remain competitive in the global marketplace. And it isn't our intent to stifle innovation or undermine U.S. companies. But we have to find a way to help these companies understand what we need, why we need it, and how they can help, while still protecting privacy rights and providing network security and innovation. We need our private sector partners to take a step back, to pause, and to consider changing course.

We also need a regulatory or legislative fix to create a level playing field, so that all communication service providers are held to the same standard and so that those of us in law

enforcement, national security, and public safety can continue to do the job you have entrusted us to do, in the way you would want us to.

Perhaps most importantly, we need to make sure the American public understands the work we do and the means by which we do it.

I really do believe we can get there, with a reasoned and practical approach. And we have to get there together. I don't have the perfect solution. But I think it's important to start the discussion. I'm happy to work with Congress, with our partners in the private sector, with my law enforcement and national security counterparts, and with the people we serve, to find the right answer—to find the balance we need.

Thank you for having me here today.

I now turn to the Vice Chairman for any remarks she might make.

**OPENING STATEMENT OF HON. DIANNE FEINSTEIN, VICE
CHAIRMAN, A U.S. SENATOR FROM CALIFORNIA**

Vice Chairman FEINSTEIN. Thanks very much, Senator. And thank you, Mr. Chairman, for holding this hearing. There was a crowded hearing this morning in Judiciary and I think the number of people here today is evidence that this a subject of great interest, so I thank you for holding this open hearing.

Director Comey, welcome again back to the Committee, and let me just repeat what I said this morning in Judiciary. I want to thank you and the men and women of the FBI for really unparalleled service to protect this country and disrupt and prevent attacks. We are very grateful and I hope you will say that to your people, so thank you.

For a period last month there were arrests almost every day as the Bureau worked to thwart attacks around the 4th of July holiday. Counterterrorism has been the top of the FBI's priority list since 9/11. And never has it included so many operations and threats to our country.

The Assistant Attorney General for National Security, John Carlin, said last week in remarks in London that the United States Government was running hundreds of counterterrorism investigations involving every United States State. In addition to the growth in the number of terrorist incidents, the nature of the threat has changed significantly. Hundreds and perhaps thousands of Americans here at home are in contact with ISIL members and affiliates, ranging from those taking direction to those who were inspired by ISIL messages on social media platforms.

As you know, I have been particularly concerned about terrorists' use of the internet to instruct, recruit, and inspire terrorism inside the United States. And you very graphically pointed that out and I hope you will again this afternoon, in what you said this morning. I believe that United States companies, including many founded and headquartered in my home State, have an obligation to do everything they can to ensure that their products and services are not allowed to be used to foment the evil that ISIL embodies.

Last week I read a lengthy feature in the New York Times. The title was "ISIS and the Lonely American," which described in detail how ISIL members used Twitter and other services to recruit a young woman over months to support a militant brand of Islam and try to get her to marry an ISIL fighter and travel to Syria.

As Director Comey notes in his opening statement, quote, "The foreign terrorist now has direct access to the United States like never before," end quote. Foreign terrorist groups, as well as adversarial nation-states today, have greater awareness of how the United States intelligence community conducts its business to collect intelligence needed to protect the people of this country and to inform national security decisions.

This Committee has heard from the FBI, the National Security Agency as late as yesterday afternoon, the National Counterterrorism Center, about how terrorist groups in particular have moved to forms of communications that are harder or impossible for the

intelligence community and law enforcement to access. The increased use of end-to-end strong encryption by both new and established communications companies has exacerbated this trend.

I understand the need to protect records and encryption is one way of doing so. Especially in this area of cyber-penetrations of our government and our private sector companies, encryption is an important safeguard. That doesn't mean, however, that companies should configure their services in a way that denies them the ability to respond to a court warrant, a FISA order, or a similar legal process from the government.

This is not a theoretical issue. The FBI has briefed this Committee on cases where it knows of communications involving ongoing terrorists by ISIL inside the United States, but it has no way to obtain the content of those communications even with a court order based on probable cause.

It seems to me that if companies will not voluntarily comply with lawful court orders for information, then they should be required to be able to do so through legislation in a way that protects security of consumer data against unauthorized access. As Director Comey has said, we are not looking for a back door into American companies; we are looking to be able to use the front door.

So, I welcome today's hearing and look forward to the Director's testimony on the ongoing threat of terrorism against the United States and the need to acquire lawfully and quickly information necessary to stop those threats from becoming real attacks. Thank you very much, Mr. Chairman.

Chairman BURR. Thank you, Vice Chairman.

For members, after the Director's comments members will be recognized for five minutes based upon their order of attendance today. And I would like to remind all members that we're in an open session, which is unusual. Therefore, I would ask you to be particularly careful in the questions that you ask. I trust, Director if in fact you have an answer that can't be given in an open session, you'll just tell the Vice Chairman and I that we'll carry this over to a closed session at an appropriate time, and we'll accommodate you on that.

With that, let me turn it to you, Director Comey, for any of your comments that you'd like to make.

STATEMENT OF HON. JAMES B. COMEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Director COMEY. Great. Thank you, Mr. Chairman, Madam Vice Chair. Thank you for this opportunity. I really do like the use of the word "conversation." I think this is a conversation we have to have as a country and this is a great opportunity to have it, to begin having it. I sometimes hear people talk about the crypto-wars and we're fighting the crypto-wars today, and I don't like that metaphor because I don't feel like I'm fighting anything. I am not here to win anything. I'm here, I hope, to explain the ways in which the change in technology and the change in which bad people are using technology affects the tools the American people through this body have given the FBI.

I think we all care about the same things. We care deeply about the security of our information, of our healthcare, of our finances,

of our innovations, of all the great things that travel over the internet. We all care about that. And I think we all care about public safety. We all care about the ability to keep the folks safe in this country. And so I don't see it as a war, I see it as an opportunity to talk about how one is in tension with the other and what should we do about it.

I really do believe we stand at an inflection point that I felt not long after I became Director, which is why I started talking about this, where the technology has moved to a place where encryption, which was always available over the last 20 years, has become the default. And that change has been accompanied by an explosion in apps that ride on the internet and offer end-to-end encrypted communication. Those things have put us at an inflection point most obviously, given my primary responsibility, with respect to counter-terrorism.

But this Committee knows from closed sessions what I think the American people may know less well, which is the terrorism threat today is very, very different and has changed just in my almost two years as Director. It is not the Al-Qaeda of old. The Al-Qaeda of old was interested in the multipronged, national landmark-based, careful, long-planned attack with carefully vetted operatives. We still face that challenge. The Al-Qaeda of old was very different from what we see today. And the Al-Qaeda of old wanted to proselytize and it did so by posting magazines on websites, and if somebody wanted to consume propaganda they found the website and they went and read the propaganda and if they wanted to talk to a terrorist they sent an email into the magazine and maybe Anwar Awlaki would email you back.

Here's what's changed. ISIL thinks about their terror in a very different way. They're not focused on the national landmark, multipronged, long tail event. They want people to be killed in their name. And they're coming to us with that message, with their propaganda and their entreaty to action through Twitter and other parts of the social media. And that is a very different thing than Al-Qaeda ever did.

They come into our country through thousands and thousands of followers of ISIL tweeters who are based in Syria. They have a physical safe haven and so they broadcast a message, which is two-pronged: come to the Islamic State, join us here in this, you know, our version of paradise, which is a nightmare, but their version of paradise. And second, if you can't come, kill somebody where you are, videotape it. If you can cut their head off and videotape it, great. Please try and kill law enforcement or military; here's a list of names where you could kill somebody.

And this message is pushed and pushed and pushed. Social media companies are worth billions of dollars because pushing to someone's pocket, whether you're selling shoes or cars or terror, works, right. ISIL has invested in this for about the last year and they have about 21,000 English language followers right now, and they're pushing this message. It's as if a devil sits on someone's shoulder all day long, saying kill, kill, kill and the terrorist, if you want to talk to them, is right there in your device.

And so they're reaching and they're calling and they're calling, and it's having an effect on troubled souls in the United States. As

the Vice Chair said, I have hundreds of these investigations in every single State, and we had disrupted just in the last few weeks very serious efforts to kill people in the United States. The challenge to us is, ISIL will find the live ones on Twitter and then we can see them say: Okay, here is my encrypted end-to-end mobile messaging app contact information; contact me there.

And so our task, to find needles in a nationwide haystack, becomes complicated by the fact that the needle at that moment goes invisible, right. I know I'm giving information to bad people. We cannot break strong encryption, right. I think people watch TV and think the Bureau can do lots of things. We cannot break strong encryption.

So, even if I get a court order under the Fourth Amendment to intercept that communication as it travels over the wires, I will get gobbledygook. That needle will remain dark to me. That is a big, big problem for us.

And the second way in which this is enormously challenging is ISIL does something Al-Qaeda would never imagine. They test people by tasking them. Kill somebody and then we'll see whether you really are a believer. And these people react in ways that are very difficult to predict.

What you saw in Boston was what the experts call flash to bang being very close, right. In Boston you had a guy who was in touch in an encrypted way with these ISIL recruiters and we believe was bent on doing something on July 4th. He woke up one morning, June 2nd, and decided he was going to go kill somebody. Right, thank goodness we were able to confront him. He confronted our people with a knife and unfortunately they had to use their weapons. But that's an example of sort of the unpredictability of this.

So you combine the blindness with this broad reach and that flash to bang and we face a challenge that we've not seen before. This is not your grandfather's Al-Qaeda. This is a very new threat that we face.

Now, some people say to me: Well, you have all kinds of other information you can get; we live in the golden age of surveillance; and I think of it differently. I think we live in the golden age of communication. Al-Qaeda—Osama bin Laden would never have dreamed that he could speak simultaneously to hundreds of Americans, find them and task them in ways that American law enforcement could not see and do it at the speed of light. The golden age of communication is posing enormous challenges for us.

I'm not here to scare folks, though. I'm here to tell people there is a problem. I do not know the answer. A whole lot of good people have said: It's too hard; that we can't have any diminution in strong encryption to accomplish public safety, else it'll all fall down and there'll be a disaster. And maybe that's so. But my reaction to that is, I'm not sure that we've really tried. I think Silicon Valley is full of great people who when they were younger were told, your dreams are too hard. They were standing in a garage some place and they were told "Can't be done." Thank goodness they didn't listen.

I think we have the talent to think about this in a good way. My hope from this conversation is that folks will realize this really matters. And the FBI is not the source of innovation. We're just

telling people we've got to talk about this, because I see the present and I see the future, which in many ways is more troubling, because the logic of it is inexorable.

FBI is not some occupying force imposed on the American people from abroad. We belong to the American people. We only have the tools that they have given us through you. I'm here to tell the American people: The tools you've given us are not working the way you expect them to work in the highest stakes matters. I need help figuring out what to do about that. The companies are run by good people. I think they see the challenge, they want to help. We have to figure out a way to solve this, to crack this riddle.

And maybe it's too hard, maybe we end up in that place. But I think this country has never been made up of people who say, "Can't be done." We really ought to talk about it more. So, I appreciate the opportunity to discuss it with the Committee.

[The prepared statement of Director Comey follows:]



Department of Justice

STATEMENT OF

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

BEFORE THE

**SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE**

AT A HEARING ENTITLED

**"COUNTERTERRORISM, COUNTERINTELLIGENCE, AND
THE CHALLENGES OF 'GOING DARK'"**

PRESENTED

JULY 8, 2015

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

**Before the
Select Committee on Intelligence
United States Senate**

**At a Hearing Entitled
“Counterterrorism, Counterintelligence, and the Challenges of ‘Going Dark’”**

**Presented
July 8, 2015**

Good afternoon Chairman Burr, Vice Chairman Feinstein, and members of the Committee. Thank you for the opportunity to appear before you today to discuss the widespread reach of terrorists’ influence, which transcends geographic boundaries like never before. As technology advances so, too, does terrorists’ use of technology to communicate—both to inspire and recruit. The widespread use of technology propagates the persistent terrorist message to attack U.S. interests whether in the Homeland or abroad. As the threat to harm Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our federal, state, local, and international partnerships.

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 FBI and the Intelligence Community as a whole.

Conflicts in Syria and Iraq continue to serve as the most attractive overseas theaters for Western-based extremists who want to engage in violence. We estimate upwards of 200 Americans have traveled or attempted to travel to Syria to participate in the conflict. While this number is lower in comparison to many of our international partners, we closely analyze and assess the influence groups like ISIL have on individuals located in the United States who are inspired to commit acts of violence. Whether or not the individuals are affiliated with a foreign terrorist organization and are willing to travel abroad to fight or are inspired by the call to arms to act in their communities, they potentially pose a significant threat to the safety of the United States and U.S. persons.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. To an even greater degree than al Qaeda or other foreign terrorist organizations, ISIL has persistently used the Internet to communicate. From a homeland perspective, it is ISIL’s widespread reach through the Internet and social media which is most concerning as ISIL has aggressively employed this technology for its nefarious strategy. ISIL blends traditional media platforms, glossy photos, in-

depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life—from career opportunities to family life to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is seen by many who click through the Internet every day, receive social media push notifications, and participate in social networks. Ultimately, many of these individuals are seeking a sense of belonging.

As a communication medium, social media is a critical tool for terror groups to exploit. One recent example occurred when an individual was arrested for providing material support to ISIL by facilitating an associate's travel to Syria to join ISIL. The arrested individual had multiple connections, via a social media networking site, with other like-minded individuals.

There is no set profile for the susceptible consumer of this propaganda. However, one trend continues to rise—the inspired youth. We've seen certain children and young adults drawing deeper into the ISIL narrative. These individuals are often comfortable with virtual communication platforms, specifically social media networks.

ISIL continues to disseminate their terrorist message to all social media users—regardless of age. Following other groups, ISIL has advocated for lone offender attacks. In recent months ISIL released a video, via social media, reiterating the group's encouragement of lone offender attacks in Western countries, specifically advocating for attacks against soldiers and law enforcement, intelligence community members, and government personnel. Several incidents have occurred in the United States and Europe over the last few months that indicate this “call to arms” has resonated among ISIL supporters and sympathizers.

In one case, a Kansas-based male was arrested in April after he systematically carried out steps to attack a U.S. military institution and a local police station. The individual, who was inspired by ISIL propaganda, expressed his support for ISIL online and took steps to carry out acts encouraged in the ISIL call to arms.

The targeting of U.S. military personnel is also evident with the release of hundreds of names of individuals serving in the U.S. military by ISIL supporters. The names were posted to the Internet and quickly spread through social media, depicting ISIL's capability to produce viral messaging. Threats to U.S. military and coalition forces continue today.

Social media has allowed groups, such as ISIL, to use the Internet to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the United States—spot, assess, recruit, and radicalize—either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.

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. As a result, it is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the homeland. We live in a technologically driven society and just as private industry has adapted to modern forms of communication so too have the terrorists. Unfortunately, changing forms of Internet communication are quickly outpacing laws and technology designed to allow for the lawful intercept of communication content. This real and growing gap the FBI refers to as Going Dark is the source of continuing focus for the FBI, it must be urgently addressed as the risks associated with Going Dark are grave both in traditional criminal matters as well as in national security matters. We are striving to ensure appropriate, lawful collection remains available. Whereas traditional voice telephone companies are required by CALEA to develop and maintain capabilities to intercept communications when law enforcement has lawful authority, that requirement does not extend to most Internet communications services. As a result, such services can be developed and deployed without any ability for law enforcement to collect information critical to criminal and national security investigations and prosecutions.

The FBI is utilizing all lawful investigative techniques and methods to combat the threat these individuals may pose to the United States. In conjunction with our domestic and foreign partners, we are rigorously collecting and analyzing intelligence information as it pertains to the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. In partnership with our many federal, state, and local agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to pursue increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the Homeland.

Chairman Burr, Vice Chairman Feinstein, and Committee members, I thank you for the opportunity to testify concerning terrorists' use of the Internet and social media as a platform for spreading ISIL propaganda and inspiring individuals to target the homeland, and the impact of the Going Dark problem on mitigating their efforts. I am happy to answer any questions you might have.

Chairman BURR. Director, thank you. And I think it's safe to restate that we're at the start of the debate, even though we have had the conversations for some time privately. We've watched encryption grow more dominant and more dominant, and really, as you said, become the default. It's almost automatic now. And it places a huge challenge on your ability to fulfill your mandate, and our challenge is to work with you as an extension of the American people to provide you what tools America is comfortable with and I think as we go through this debate we'll figure out where that sweet spot is.

With that, I'm going to turn to the Vice Chairman for her questions, and I would share with the members it would be Feinstein, Wyden, Heinrich, Cotton, Coats, Hirono, Mikulski, Collins, Warner, McCain, Blunt and Lankford in that order. Vice Chairman.

Vice Chairman FEINSTEIN. Thanks very much, Mr. Chairman.

Director COMEY, I think you spoke very eloquently, but can you quantify this at all? Can you tell us how often the FBI acting pursuant to a warrant or other lawful process encounters encrypted information you cannot access?

Director COMEY. Thank you, Senator Feinstein. The answer is I really can't at this point, for a couple of reasons. We're sort of at the beginning of this and we're going to work to try and collect that data.

But the other thing is, it's a bit of like proving a negative. When my folks see that something is encrypted, they move on and try to find some other way to assess this bad guy, this potential bad guy. And so we obviously have incidents, the courts have collected incidents, where wiretaps were issued by courts and then encryption was encountered. But my numbers—I don't have good enough numbers yet.

Vice Chairman FEINSTEIN. Okay. I think it would helpful if the Department could gather some numbers to quantify this.

The next question is BSA, which is known as The Software Alliance, sent a letter to this Committee and the Judiciary Committee stating that calls for weakened encryption, quote, "can create artificial commercial disadvantages for United States companies and barriers to market access." End quote. I'd like to have your reaction to that statement?

Director COMEY. First, I think—again, I'm not an expert. Public safety is my thing, but I think I take issue with the notion of weakening encryption. I also take issue with the whole back door notion. I think what smart people have told me is there are a number of companies already out there that use strong encryption on their data, including data in motion, that have the ability to access the data and comply with court orders, and they're able to do both in a pretty robust way in all different sectors, in the information—in the ISP world as well as in finance and a bunch of other places.

So I don't know that it's going to be a question of weakening encryption. It's simply going to be a way of figuring out how do we comply with a judge's order, we the company, and I don't think the government is, frankly, smart enough to be able to impose a one size fits all solution. But I also think you're right that there are competitive and international implications in this. None of us want

to do anything to damage the innovation of America. It's the great engine of this amazing country.

And so I do think there are international implications that have to be considered. Every country that cares about the rule of law is grappling with this right now. All of them are trying to figure out a way to maximize safety on the internet, right, make sure there's strong encryption, and maximize public safety, and do it under the rule of law. Our friends in the U.K. are doing that right now. So I agree that there are implications to it internationally.

Vice Chairman FEINSTEIN. Well—and let me ask you to respond. This is another quote from the same letter: “Requiring technology that provides law enforcement access to information also risks undermining the security of all electronic communications and digitally stored information.” End quote.

Would you comment on that? As I understand it, what you would be talking about is some kind of a front door key? Is that—is that correct?

Director COMEY. Again, it's part—my reaction to that comment is “Maybe.” And if that's the case, well, I guess we're stuck. But I don't think the great innovative people of America have actually put their mind to this, frankly because they haven't been incentivized to do so.

But again, I believe there are companies that provide significant portions of our internet activity that have encrypted—strongly encrypted data in motion and have the ability, because it's part of their business model, to see the data and comply with court orders.

Vice Chairman FEINSTEIN. So, you're saying that some do and some don't.

Director COMEY. Correct.

Vice Chairman FEINSTEIN. Is that what you're saying?

Director COMEY. Somehow they've managed to do it without the entire system crashing or without their own business being materially vulnerable in some way. But look, here's how I understand it. There's no such thing as secure. There's more secure and less secure. There's vulnerability in every system. The question is: So what can we do to maximize public safety that results in an acceptable level of security? And the answer is I don't know, but I think a lot of smart people should talk to each other to try and figure that out.

Vice Chairman FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator Wyden.

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

Director COMEY, I very much share Director—Chairman Burr's comment with respect to the respect we have for the men and women of the FBI, and you and I have policy differences on that matter, but we are not going to respect the men and women who work for you any less because of those differences.

Every Senator who serves on this Committee understands that it is a dangerous world and the challenge is to make sure that we pursue approaches that promote security while not diminishing our liberty. Too often, we haven't been able to achieve either. And I think as we start this debate I want to emphasize how exactly we

got here. Executive Branch agencies are now dealing with a problem that they largely created.

Senior officials made the choice to secretly twist the law to support an ill-conceived secret program that vacuumed up millions of phone and email records of law-abiding Americans. A number of us spent years warning what the consequences would be, but obviously public confidence was dramatically diminished.

That led to a very serious public backlash and in response to it, just as Senator Feinstein read, our hardware and software companies accelerated their efforts to provide customers with stronger protections.

This obviously creates real challenges for you. But I will tell you, as of this morning statements are being made that do not inspire a lot of confidence. You talk about the need to strike the right balance. There hasn't been a lot of balance in the past, and as of what I heard this morning there still isn't too much balance in the so-called balance.

The Deputy Attorney General, Ms. Yates, seemed to suggest this morning that companies should retain a stockpile of encryption keys for the government to access. Making this a mandatory requirement would obviously present huge problems since any such stockpile would be vulnerable to compromise or abuse. In my judgment, a mandate like that would be a huge gift to foreign hackers and criminals.

So what I want to do with my time for questions is put this into context on a matter we all care about up here, which is cyber security. I've had companies in Oregon hacked for economic espionage and my constituents are not alone. So on the topic of encryption and cyber security, has the Executive Branch done any analysis of the impact that a requirement for U.S. companies to build weaker encryption or stockpile these encryption keys would have on U.S. cyber security?

Director COMEY. Not that I'm aware of, because that forms part of our concern that we not try to impose a solution. I didn't understand her to be saying—obviously, I sat next to her. I didn't understand her to be saying that. I understood her to be saying the end state we want is that companies, however they choose to do it, will be able to comply with judges' orders, but that we don't want to impose a one size fits all; we want companies to work with us to figure what works for you, because it seems that some companies have figured out how to do it.

Senator WYDEN. Well, she was suggesting in my view that there be a stockpile of these keys. She didn't want the government to have it. And once you're going down that route, I think it's trouble.

Now, having said that you're not aware of any study, and that was my sense, is it fair to say that strong encryption improves cyber security and weaker encryption reduces cyber security?

Director COMEY. Yes. Strong encryption is great.

Senator WYDEN. Okay. Now, if a stockpile of encryption keys was created somewhere, because I took Ms. Yates' comment to not be the government but she wanted it somewhere, if you had a stockpile of these keys created somewhere, would you be able to guarantee that these keys would never be stolen by a hostile foreign actor?

Director COMEY. The hypothetical stockpile of keys, surely not. But again, please don't understand me to be suggesting, nor should you listen to me if I suggest, a technical solution. I don't know what the answer is.

Senator WYDEN. But I think you're right. I think that, based on my 14 years of service on this Committee, I don't have a lot of confidence that a stockpile of these encryption keys—and as I say, I heard Ms. Yates said there ought to be some kind of arrangement to have these encryption keys somewhere. I'm not confident it wouldn't be compromised or abused. That's the flaw in the concept. We'll continue to have this debate.

Thank you, Mr. Chairman.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Mr. Chairman, I want to thank you for holding a public hearing on this topic and giving us an opportunity to discuss these issues. If I had one critique it would be that we're missing valuable insight from the technology, privacy and constitutional liberties experts who also have valid concerns around these ideas, potential proposals.

So, you know, one of the things that I would suggest is that we consider holding a follow-up public hearing where we can hear from some of those individuals as well, particularly in the technology space. And in the meantime I ask unanimous consent that a number of letters and background materials that you did not include in your earlier unanimous consent be made part of the hearing record.

Chairman BURR. Without objection.

[The material referred to follows:]

Senator HEINRICH. Let's see. Director Comey, you know, this issue of losing access to encrypted communication is obviously complex, particularly from a technological point of view. And I guess I want to start by just commending you and, as I have NSA Director Rogers, for your willingness to address this publicly and to start the conversation. I think one of the challenges is that it's going to be very hard to address this issue without a specific technological proposal or fix to be able to discuss. And, you know, back in the 1990s we had a first crack at this which really came apart at the seams once it became solidified around the particular piece of technology and that's what I'm concerned about today.

So, in the interest of time, I'm going to submit the rest of my opening statement for the record so I can get to a couple of questions. But I think that's going to be at the crux of this conversation for a while, is that we need to know what a potential fix looks like or in the case of if there are examples—and I'll get to that in my questions—what those look like, to be able to know whether a fix is really better or whether it creates inherent weaknesses that are exploitable by some of these very talented, nefarious actors that you brought up in your testimony.

As you know, yesterday several respected computer and cyber security experts, people who are really well renowned in the area of cryptography, released a report that effectively concluded that you can't reliably provide the government or anyone else with exceptional access to software applications without introducing some critical weaknesses in that encryption.

Given your interest in this issue—and I hope you’ve had a chance to at least familiarize yourself with that report—you know, one of the things I’m concerned about here I guess is that it seems like government and the technology interests are sort of talking past one another, and need to sit down and get at least the technology pieces of this on the table, so that we can all agree that we’re talking about the same thing. And I think it would be a mistake with regard to exceptional access to leave the solution to a Congress that I would argue is not always the best judge of all things technical.

As you mentioned, there are a lot of people in Silicon Valley who are doing a really good job of trying to manage these things. So, can you give some examples of programs that currently use some form of end-to-end encryption, so provide that security, but also are able to respond somehow to the law enforcement warrants that you need to put out there?

Director COMEY. Thank you, Senator. I agree very much, which is why I’m so excited about this opportunity, because I think things like this hearing will drive the conversation, because we need to do it together. They are the source of the innovation and the expertise. We need their help in solving this.

I’d never heard until I read—I read the executive summary and I went through that paper pretty quickly, the rest of it, I’d never heard the term “exceptional access.” My reaction when I read it is I don’t want exceptional access; I want ordinary access where a judge issues an order and folks are able to comply with the order that a judge issues. There are providers who, because of their business model, encrypt, as I understand, strongly encrypt the communications in motion, but they are visible to them on their servers that they control, as part of the business models, because they want to be able to sell you ads and so they need to be able to see the content.

And for those providers, some of whom are huge providers, we are able to serve a judge’s order and get the content in a counter-terrorism case or an espionage case or serious criminal case of communications that the judge has authorized us to do. And I don’t think those folks think that their system is materially vulnerable.

And so I wonder. Again, folks should not be looking to me for technical advice. I wonder whether that isn’t an example that we should use in our conversations with the companies. But every company is going to be different, which is why I don’t think one size fits all, because some of the companies at issue that the terrorist use are three guys in a garage who started this end-to-end encrypted app. And so our ability to work with them may be very different than with some bigger companies.

So, I don’t think we want to be seen as we’re going to impose this fix on all of you. We want to talk to you about how we can solve this. I don’t want to demonize the companies, either. They love their country, they care about public safety. I know that from private conversations, and so it’s about we care about these two things; how do we maximize both of these? Maybe it’s impossible. Maybe the scientists are right. I’m not ready to give up on that yet.

Senator HEINRICH. Well, we’re overtime here, so I’ll wait for the second round. But I guess everybody has this concern about, you

know, just having been one of the people who got a letter from OPM recently, that the government might not be the right folks to be holding the keys for end-to-end encryption. So we need to find a more elegant approach.

Director COMEY. Agreed.

Chairman BURR. Senator Cotton.

Senator COTTON. Thank you, Mr. Chairman.

Thank you, Director, for being here to address this very important problem. To make sure I understand the issue here, what we're talking about is not some kind of extraordinary surveillance, not something that's unknown to the user of a device, but encryption technology that would thwart a lawful court order that has been taken in front of an independent Federal or State judge by law enforcement authorities to get access to data, and then you go to a company and the company says: Sorry, we can't provide you this information because we have designed a system in a way that prevents us from accessing it.

Director COMEY. That's correct. Or with respect to a device that's locked and the same judge issues a search warrant, and they tell us: We can't open it because we designed our system to make the phones—we cannot unlock them.

Senator COTTON. And this is the Intelligence Committee, but I know you testified in front of the Judiciary Committee this morning. This is an issue not just for terrorist operations, but I would presume also for things like child molesters, child pornographers, sex traffickers, kidnappers, is that correct?

Director COMEY. Yes. This is an overwhelming issue in local law enforcement and prosecution, especially the data that's on a device that can't be opened, because they tell me that's a feature of all of the cases you mentioned as well as domestic violence, car accidents. The information on there can show you who the bad guy is, also tell you someone is not guilty, and so it's very important in all their work.

Senator COTTON. In one of the recent Congressional recesses, I spent some time at the Little Rock field office for the FBI. First, I want to commend the agents and employees you have in that field office there for their dedicated public service. It was a very important afternoon for me. They specifically brought up the "Going Dark" issue and the way it has thwarted their operations to keep Arkansans safe.

Furthermore, I was able to see in their lab an effort they had made to get access to a locked device, and they got access and it actually allowed them to recover a young girl who had gone missing. But they said that that was rare and that they were fortunate they were able to do it. I think that's just an example of what I suspect is the case, is that in your opinion in all 50 States of our Union is this an ongoing problem for both Federal law enforcement and local law enforcement?

Director COMEY. Yes.

Senator COTTON. Do the companies with—with whom you deal in private settings, appreciate the fact that the technology that they are creating and marketing is being used by terrorists and some of the most heinous criminals in our society?

Director COMEY. They do and it bothers them, which is why I think we're starting to have more productive conversations, because they're good—they're good people.

Senator COTTON. So we're not the only society to encounter this kind of problem, of course, and one argument you hear from American companies is that they need to compete in the international market because most people don't live in the United States.

Director COMEY. That's true.

Senator COTTON. Have you taken a look at how countries like, let's say, the United Kingdom or France have addressed this issue?

Director COMEY. Yes. They are both grappling with it. They're both a little bit ahead of us. They both have passed legislation that as I understand it will require providers to give access, again with appropriate authority, in the course of investigations. So they—they're grappling with it just as we are. Everybody who cares about the rule of law and public safety has to grapple with the same thing.

Senator COTTON. So about 20 years ago, this Congress passed something called CALEA, the Communications Assistance for Law Enforcement Act, saying, in the old days, essentially on telephones—that telephone companies had to provide the ability to let law enforcement with a lawful court order, a lawful court order, put in a wiretap. Could you look to CALEA or maybe what other countries have done to address the "Going Dark" program with data encryption as a model for this Congress to act?

Director COMEY. It's possible. I mean, it's one of the things that's being talked about, is that a model that can be adapted to deal with this challenge? And so we're still working on that.

Senator COTTON. Okay.

Director COMEY. And by us I mean not just in the government, but I think the private sector has to be part of the conversation.

Senator COTTON. Does the Executive Branch yet have legislative proposals that they are prepared for this Congress to take under advisement?

Director COMEY. Not yet.

Senator COTTON. Is that because you're continuing to work with some of these companies to try to develop the technical, legal, and policy frameworks?

Director COMEY. Yes. Just as I think we all do, the President sees the problem, sees that these two things we care about tremendously are in tension and that's it's a really hard problem. And so he's commissioned a whole lot of work on different streams, but one of them is to figure out what legislation, if we decide to go that route, would make sense, and to get the input from the private sector on, so what would work for you folks?

Senator COTTON. Well, thank you very much, Director, for your testimony. Thank you very much for what you represent, the tens of thousands of agents around the country who keep us safe on days like the 4th of July and every day. I just urge you and the men and women with whom you work in the Executive Branch to get us that kind of proposal as quickly as possible. We all recognize the tension between trying to protect data, which we want to do for American citizens, but also ensure that law enforcement has

the tools they need, not just to stop terrorism but stop the most heinous kinds of crimes imaginable in our society.

Chairman BURR. Senator Coats.

Senator COATS. Thank you, Mr. Chairman.

Director, we're having I think a very worthwhile discussion and I appreciate your being here, and also your open-mindedness in terms of finding humility in a sense in saying we don't know all the answers, but there are a lot of cooperative and smart people out there that can help us find the answers and hopefully attain that balance between privacy and that balance between protecting people's lives.

I don't envy you your job, because every day I pick up the paper or turn on the television and the news, and there's an abducted child, there's a criminal act, there is a threat, terrorist threats from abroad. And the American public is demanding that your agency do everything possible to prevent that from happening, to recover that child, to address the blatant use of communication devices and so forth and so on that result in very, very bad criminal acts.

By the same token, you get hit from the other side by saying, but don't you dare do anything that would give you—that could potentially be used to violate someone's privacy.

And so that's a very narrow path to try to walk down and achieve both of those goals. And I think your statement relative to the fact that we need to turn to those very people that are providing the encryption in order to protect people's privacy are part, a very essential part, of the solution.

My question here though, is that, while we can make patriotic requests to all these technical companies, Silicon Valley, in other words to help us through this and there are patriotic Americans that say, yes, let's see if we can find that sweet spot, we also know that there are countries around the world that have no intent of helping us whatsoever. And within those countries or even some of those lawless areas like you mentioned in terms of ISIL occupying physical territory, the last thing they're going to want to do is cooperate with us in terms of finding a solution to this particular problem.

And so it would be very easy—well, that turns us to the difficulty of, no matter how much we do, we're a global communications system in place, and it's easily to turn somewhere else. We've seen off-shore gambling because we passed laws that say you can't do gambling on the internet here in the United States, and they simply find an island in the Caribbean and set up and through the ether, there it goes.

So I'm wondering how you can continue to have the agency perform its role without some type of authority to allow you to, of course within the legal system, address the problem? And obviously, it's going to take time to develop any kinds of solutions. Do you—what do you have to do relative to manpower costs to fill the gap between now and then?

Director COMEY. Thank you, Senator. And I should have said this earlier, to thank the entire Committee, but Senator Cotton and you, Senator Coats, reminded me. Thank you for the nice things you said about the folks at the FBI. I sent them all a note, an email, before July 4th saying, thank you for the American people.

I know we're grateful, I know that you're bone tired. My folks are bone tired, but they stopped the stuff that was trying to come at us for July 4th. But that—now, it's July 7th and 8th, and they're on to the next thing. So thank you for that. I'm going to pass it along to them. It means a lot to them.

We love walking that fine line right between public safety and privacy and civil liberties, right? Because we care—we've got families, we care about the same stuff. So we like walking that line. We do agree that there's an international component to this, as you said, Senator, that we're going to have to address. The folks, especially in Western Europe and here in North America, who care about the things that we care about, we have to figure out an approach together that makes sense, but America is the big dog. All right. The innovation is here, the energy is here, the infrastructure is here. What we do will set the tone and the pattern for the rest of the world. We can't fix the whole world, but for the world that thinks about things the way we do, values what we do, we can drive it.

But that doesn't mean it's not—that it's an easy thing. We try to fill the gap by—if I can't see the communications of the terrorist, then I got to figure out, okay, can I get an informant in on them? Can I send an undercover in? Can I follow him 24/7—24/7 for weeks and weeks and see if I turn something up?

All I'm telling folks is we will keep doing it. My folks will keep working no matter how tired they are. It's just the tools the American people thought we had are being diminished and I see that only continuing.

Senator COATS. I think we all look forward to working with you trying to achieve that goal.

Thank you, Mr. Chairman.

Chairman BURR. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman.

Thank you, Director, for your work and of course all of the people who work for the FBI and protecting the safety of our citizens.

I'd like to get a little bit more information on where we are now in terms of your ability to see information. For example, in how many cases have you seen a warrant for a device or a warrant that has been thwarted—completely thwarted by encryption? And how many Federal investigations had been unable to progress because of encryption?

Director COMEY. So the answer—as I said earlier, Senator Hirono, I don't know the answer to that. We're going to try and see if there's data we can collect on that. I'm not confident it's going to be very reliable for you, though, because what our investigators do is if they see someone is on an app that we know is encrypted, they're not going to bother seeking a wiretap for that. So we won't be able to count that, I don't think, as a wiretap thwarted. And if we see encryption, we just try and find another way to assess the situation and we try to use the other tools.

We're going to try and do that for you, but I'm not optimistic we're going to be able to get you a great data set. There's no doubt that it is a real feature of our life. I think that's one thing everybody should be able to agree upon, that the logic of this is all of our papers and effects, all of our communications, will at some

point be covered by strong encryption. I hope everybody agrees that will have profound consequences for law enforcement.

Senator HIRONO. I think that's one of the reasons that we have to be very careful in what—in what we decide to do. And so it always helps to define the extent of the problem in the current situation. And then, as you say, no system is secure, so we need to weigh the—what the risks are, et cetera, because at the same time, we have this very august group who have said that forcing companies to—to provide a back door to encryption is going to result in a lot of unintended possibly consequences, including we are told that some of our companies will lose a competitive advantage because of—for example, if we expand CALEA to including encrypted apps, that CALEA only would apply to our companies and therefore, if our companies have to provide a sort of a back door way to get to this information and foreign companies who are in the marketplace don't, then they are at a competitive disadvantage.

So there are a lot of issues that we do have to weigh. And speaking of CALEA, by the way, did I understand you to say that expanding CALEA is just one of the things on the table, because I thought you had said at another forum perhaps that you think CALEA should be expanded to include encryption apps?

Director COMEY. I don't know whether I said that, but if I said it I'm smarter today than I was then. I think that's something that folks are discussing. But I don't know what that answer is. That's why we haven't come to the hearing with a proposal. We're trying to show the humility to say we actually don't know what will be best. But I agree with the competitive harm point, Senator.

Senator HIRONO. As we wrestle with this subject, though, meanwhile the companies are providing more and more encryption apps. I mean, at what point do you think that we will be prepared to take some sort of legislative action that would enable you to get access to information and yet still provide our companies with the—the kind of environment that they would like us to provide?

Director COMEY. I don't know.

Senator HIRONO. And what is the timeframe for that?

Director COMEY. I don't know, because I do think this is a—one of the most complicated problems I've ever seen in government, for the reasons that I have alluded to here, including what you said about competitive harm. We do not want to damage the engine of innovation that is America. And so we have to figure out, so how can we maximize safety on the internet and public safety in a way that makes sense for America.

Now, it probably makes sense, we ought to figure out what kind of people we want to be first, what makes sense for our country. But I do think we've got to do that in league with international partners, so we don't create a situation where America is the only mover and that causes harm to our—our companies.

Senator HIRONO. I think that is a very important aspect of what we need to do going forward on the “Going Dark” problem, because it would be very unfair to our companies, as you say, if we're the only country that requires a back door way to this information. So I'm glad that that's on the table with—in our discussions with our—with other countries.

So the president's review group, that's some—some other people I have already mentioned. But they said very strongly that we should not require a back door way. So in these discussions, is the technical, you know, technology companies, are they going to be at the table as we discuss going forward and what might be appropriate legislative action?

Director COMEY. They have to be, because I think we all think no one size fits all. So you've got to figure out what would work for different companies. And as I said before, I think that is the source of the innovation. That is the source of the creativity that we have to harness.

Senator HIRONO. Thank you, Mr. Chair.

Chairman BURR. Senator Mikulski.

Senator MIKULSKI. Mr. Director, it's very nice to see you again.

Mr. Chairman, thank you for having this hearing, as well as the Vice Chair. I'd like to pick up on Senator Heinrich's recommendation about an additional hearing on this subject from the technical and civil liberties folks. In our briefing materials, I read letters from the ACLU, whose views we so value; The Software Alliance; and I saw a lot of criticism of what we're pursuing here for some type of opportunity to not go dark.

But I didn't see any solutions. I saw a lot of criticisms, a lot of critiques, but I didn't see solutions. Now, I believe, again as Senator Heinrich said and others, we have tremendous technical know-how, and I believe that the people in Silicon Valley are indeed very patriotic people and they don't want drug dealers and international traffickers and child pornographers to be able to get away with nefarious things.

So if we could actually perhaps get from those as well as the civil liberties community, how we can start working to a solution, that would be great.

Mr. Director, in this year's appropriations funding we worked very hard to support you, both when I was chair of the subcommittee that funds you, as now as Senator Shelby. We have now put in \$8.4 billion to fund you for this coming year. And we also put in \$483 million for cyber security. My question to you is, do you feel that those resources and the type of workforce you have is able to be flexible enough to meet the ongoing threat?

This is a—and no, I'm not being critical of what you have, but as you talk about the recruitment tools of ISIL, who are pretty talented using Twitter and other forms of social media, that's a whole different generation. And it's a whole different generation than the original cyber warriors that were hired under your predecessor. So do you feel you have enough resources to be able to recruit the people needed to deal with this, as well as the administrative flexibility to bring in teams? This is not going to be your traditional agent. Could you share with us, because we can have the best law in the world, but unless you have the best workforce and the flexibility and the resources to hire it, we're just creating hollow opportunities?

Director COMEY. Thank you, Senator. I think the answer is yes and no. Yes, I believe that the Senate and this Congress is giving us the resources I need for next year, the money I can responsibly spend. But I face a threat obviously that continues to grow, so I

will be back to ask for additional help. But I think you have given us what we can reasonably spend, reasonably invest in.

And I think the answer is yes, I think I can attract the talent. I cannot compete on dough, but the value proposition is totally different. If you're interested in dough, you don't want to work in the FBI, and that's—you didn't—you don't come here to get rich. But so many young people want to make a difference in the life of this country that they don't care about the dough. They want to be part of addressing these threats. That's pretty exciting, and so I'm optimistic actually.

Now, once I get them in and they're here five, six years, start to have a family and there's no cost of living adjustment, maybe I start to lose their enthusiasm a little bit, but that's a problem I'll deal with down the road. I've got lots of smart young folks who want—

Senator MIKULSKI. But what about the flexibility—so here—there's the—you investigate breaches and a variety of things. You're also counterterrorism. That's the social media world that you're now operating in. Even a modern director like Director Mueller did not face what you have. He faced Al Qaeda; you face a variety of other challenges, as you so clearly said. Do you have the administrative flexibility to bring on people as you need them that might not be the traditional trade routes for recruitment of FBI personnel?

Director COMEY. I think so. There's a couple of things around that that I'm thinking about. But in the main the answer is yes. One of the things we have to consider is should we look at a different career proposition for people. Have them come—once people come to the FBI, they almost never leave. They get addicted to it. But should there be a model where they come, then they go and do something in the private sector, then come back? That's something we haven't done before, but that may be a model I want to look at. But in the main, yes. I have the—you've given me the flexibility.

Senator MIKULSKI. My last question, and I think perhaps it's not appropriate to an open session. So we had three so-called coincidences today: the fact that the technology has failed at United Airlines, the New York Stock Exchange, as well as the Wall Street Journal. I don't believe in coincidence. I believe a coincidence is an event that we don't have an explanation for. Is the FBI investigating these as breaches or have you not been called in, or you're not able to say?

Director COMEY. We—

Senator MIKULSKI. I was very troubled by these so-called coincidences.

Director COMEY. Yes, as was—obviously, that caught my attention. We're not big believers in coincidence, either. We want to dig into that. So we've been involved in—all three, in contact with all three companies to understand what's going on. And we do not see any indication of a cyber breach or cyber attack. Actually, I think the Wall Street Journal piece is connected to people flooding their website in response to the New York Stock Exchange to find out what's going on. But it looks—again, in my business you don't love

coincidences, but it does appear that there is not a cyber-intrusion involved.

Senator MIKULSKI. Thank you very much, Mr. Director.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Director, you've talked about the impact on terrorism cases and your counter-terrorism efforts. And you've said that it's very difficult to quantify what the impact is. But it's my understanding that this morning in testimony before the Judiciary Committee that the district attorney for Manhattan said that in the past six months alone there have been 74 cases where law enforcement had been stymied because they were unable to get information from lawfully seized cell phones. Is that accurate?

Director COMEY. I saw that in the written testimony of District Attorney Vance and so, knowing him, I believe it to be accurate.

Senator COLLINS. As I look at this problem, which obviously has ramifications, as some of my colleagues have pointed out, for criminal cases as well as for counter-terrorism investigations, would an option be to require the companies themselves to be able to access the information to comply with a lawful court order, not the government having the keys or a back door in, but the company itself. Might that be a solution to this problem?

Director COMEY. Yes. And that's something the deputy attorney general talked about this morning, that it's possible to imagine a world where the companies figure out how to comply in a way that maximizes security of their information and complies with the judge's order, and that every company does it in a slightly different way. Yes, that's a possible outcome.

Senator COLLINS. Now, there are some—most companies I suspect that are involved in developing this end-to-end encryption did so with the best of intentions. They were trying to increase the security of the data of their customers. But do you believe that there are some companies that have intentionally developed this kind of system in order to thwart their ability to respond to a lawful court order?

Director COMEY. I don't know, with respect to the intent question. I know there are companies that have, once they made the decision, advertised it as a solution that would be immune to a search warrant. Apple did that when they ruled out their new phone. But I don't know that the intention of the original change was to accomplish that result, if that distinction makes sense.

Senator COLLINS. Well, it doesn't to me, because when a company is advertising that the information would be safe from a search warrant that's very troubling to me, because that to me implies an intent to keep information away from law enforcement despite the issuance of a lawful court order. And I think most people involved in the encryption process in developing these products would not want to thwart law enforcement, whether it's for a criminal case or terrorism. But that kind of advertising does trouble me. And I won't ask you to respond to that.

I do want to switch to access to a different kind of information that suggests how much we need a computer—a cyber-security law. I just met with the CEO of a large bank. He relayed to me an inci-

dent where the FBI knew that his bank had been targeted for a cyber attack. Here's what he told me had to happen.

He said that the FBI under current law could not immediately go to this bank and convey the information. First, they had to go to the bank regulators, the OCC regional office. Then the information had to go from there to the OCC in Washington. From there, it had to go to the Department of Homeland Security. Then they had—the Department of Homeland Security approved the FBI contacting the bank to warn them of this imminent attack.

Well, obviously—and he said this all occurred over a weekend. So it was difficult to reach people, there were cell phones involved, et cetera. That's a terrible system. And we need to be able to empower the FBI in real time to be able to notify a financial services organization, the electric grid, the air traffic control system, critical infrastructure, of an impending attack. Would you agree with that?

Director COMEY. Very much. And what you've described surprises me because I think the way we operate is we call them. If there's a threat to an institution of any kind, we've developed relationships with their chief information security officers, so what—I'm going to go back and track—maybe you can privately give me the information.

Senator COLLINS. I will privately—

Director COMEY. Because it's not the way I understand it works or is supposed to work.

Senator COLLINS. Well, this incident really troubles me, because by the time the information got to the proper people at the bank, it is nothing short of a miracle that the cyber attack hadn't already occurred.

Thank you, Mr. Chairman.

Chairman BURR. Senator Warner.

Senator WARNER. Thank you, Mr. Chairman.

Director COMEY, good to see you again, and let me add my comments to my colleagues' about the good work that you and the people of the FBI do.

Building on Senator Collins' comment, I think again, even if this was a one-off, a notion that there's not clarity and a single point of contact is—speaks volumes about the need to at least take forward the legislation that this Committee passed in a bipartisan way and at least take a first step, it's not going to solve all the problems, but I think it would be a significant step forward.

I have some technology background. I've—I have had some conversations with companies in the IT space and the encryption space who once they've created this entity I think in a sense are starting to understand the potential problems that are being created. Can you speak to any of that in terms of a recognition that, under the guise of either privacy or business protections, of a growing recognition within particularly the IT community that this is very much a double-edged sword and may have created a monster that is not controllable?

Director COMEY. Thank you Senator. I meant what I said. I think they are good people, and I—look, it's not their job to worry about public safety. And so I don't think it's something that's front and center for them. I think what's happened is, particularly this ISIL threat and how real it is and everywhere has focused them. And

so they see it, and so we're having productive conversations. Again, they don't want people to die; they don't want kids to get kidnapped. These are regular folks. And so that's why I'm excited about the prospect of harnessing that innovation.

They are good people who want to have successful businesses and they want to protect their country. And so—again, I'm not a naysayer. I know here people write papers that say it's just too hard, and I'm not buying that, because I don't think the great people of Silicon Valley and other places have said: You know what, let's see what we can do in a way that protects that which we have built and the country in which we live.

Senator WARNER. And Mr. Chairman, I'd just say I've got a series of these companies in Virginia and when the hundred-plus military personnel and their families' names were publicized in an attempt to intimidate, I think it woke up in at least the Commonwealth of Virginia a lot of IT companies about the notion of how very real and how obscene some of the actions that this ISIL group does in terms of threatening people.

Let me move to—Senator Mikulski asked the question I was hoping to ask about the three events today and I hope you will get back to us. But I'm going to raise another issue that I think there has been a great deal of confusion around and concern about, and that's the OPM breach. We're literally months into this now and continue to get a series of different answers in terms of numbers. I've been very disappointed by OPM's reaction post-breach in terms of assuring those Federal employees current and past, both in terms of what actions the government's going to take to protect them going forward and some of the subcontractors they've been using and how ill-equipped they've been.

Not your topic, but if you can perhaps give a little more clarity about the overall scope of that attack within the confine or within the context of this public hearing? There's an awful lot of people listening for those kind of answers.

Director COMEY. It's something I have to approach carefully in an open hearing. And I know that the administration, OPM in particular, is working and is close to offering a more—a public and more detailed accounting of what we think was lost. But it is an enormous breach and a huge amount of data that is personal and sensitive to Federal employees, former Federal employees, people who applied for Federal employment was available to the adversary. And we have to—we have to assume that it was looked at and or ex-filled. So we—we're talking about millions and millions of people affected by this.

And the challenge of it is it's not just—I'm sure the adversary has my SF86 now. My SF86 lists every place I've ever lived since I was 18, every foreign travel I've ever taken, all of my family, their addresses. So it's not just my identity that's affected. It's, you know, I've got siblings, I've got five kids, I've got—all of that is in there. And so the numbers quickly grow far beyond the number of Federal employees, which is millions over the last 20 years. And so it is a very, very big number. It is a huge deal.

Senator WARNER. And I understand an active investigation. But I also know that we're now running on 60 plus days, actually, more than a year since the first breach. And the lack of a single answer

or even some sense of that answer overall from the administration is very troubling.

Thank you, Mr. Chairman.

Chairman BURR. Senator McCain. John, cut on that microphone, would you.

Senator MCCAIN. Is it true that you have stated on several occasions that ISIS poses over time a direct threat to the United States of America?

Director COMEY. Yes.

Senator MCCAIN. And that is the case today?

Director COMEY. Yes. Every day, they're trying to motivate people here to kill people on their behalf.

Senator MCCAIN. And every day that they take advantage of this use of the internet which you have described by going to unbreakable methods of communicating, the more people are recruited and motivated to—here in the United States and other countries, to attack the United States of America; is that true?

Director COMEY. Yes, sir.

Senator MCCAIN. So this is not a static situation. This is a growing problem as ISIS makes very effective use of the internet, is that correct?

Director COMEY. That's correct, sir.

Senator MCCAIN. So in all due respect to your opening comments, this is more than a conversation that's needed. It's action that's needed. And isn't it true that over time the ability of us to respond is diminished as the threat grows and we maintain the status quo?

Director COMEY. I think that's fair.

Senator MCCAIN. So we are now—and I've heard my colleagues, with all due respect, talking about attacks on privacy and our constitutional rights, et cetera. But it seems to me that our first obligation is the protection of our citizenry against attack which you agree is growing, is that a fact?

Director COMEY. With respect to the—I agree that our—that is our first responsibility. I also agree—

Senator MCCAIN. So the status quo is not acceptable if we support the—the assertion that our duty is to protect the lives and property of our fellow citizenry as our first priority, is that—do you agree with that?

Director COMEY. I agree that this is something we have to figure out what to do about.

Senator MCCAIN. So now we have a situation where the major corporations are not cooperating and saying that if we give the government access to their internet that somehow it will compromise their ability to do business, is that correct also?

Director COMEY. That's a fair summary of what some have said.

Senator MCCAIN. So we are discussing a situation in which the U.S. Government, i.e. law enforcement and the intelligence community, lack the capability to do that which they have the authority to do; is that correct?

Director COMEY. Certainly with respect to the interception of encrypted communications and accessing locked devices, yes.

Senator MCCAIN. So we're now in an interesting situation where your obligation is to defend the country and at the same time

you're unable to do so because these telecommunications—these organizations are saying that you can't and are devising methodology which prevents you from doing so if it's the single key only used by the user, is that correct?

Director COMEY. I wouldn't agree, Senator, that I'm unable to discharge my duty to protect the country. We're doing it every single day using all kinds of tools.

Senator MCCAIN. Are you able to have access to those systems that—which only have one key?

Director COMEY. No. We can't break strong encryption.

Senator MCCAIN. So you can't break it. And that is a mechanism which is installed by the manufacturer to prevent you from using the—that there's only one key that is available to them—to you.

Director COMEY. That's correct.

Senator MCCAIN. So suppose that we had legislation which required two keys, one for the user and one that, given a court order, requiring a court order, that you would be able to, with substantial reason and motivation for doing so, would want to go into that particular sight. What's the problem with that?

Director COMEY. Well, a lot of smart people, smarter than I certainly, say that would have a disastrous impact on broader security across the internet, which is also part of my responsibility to provide that.

Senator MCCAIN. Do you believe that?

Director COMEY. I'm skeptical that we can't find a solution that overcomes that harm. But a lot of—a lot of serious people say: Ah, you don't realize; you'll rush into something and it will be disaster for your country because it'll kill your innovation, it'll kill the internet. That causes me to at least pause and say, okay, well, let's talk about it.

Senator MCCAIN. Yes. But we've just established the fact that ISIS is rushing into trying—attempting to harm America and kill Americans, aren't we?

Director COMEY. They are.

Senator MCCAIN. So I say, with respect to my colleagues and their advocacy for our constitutional obligations and rights, that we are facing a determined enemy who is as we speak, according to you and the Director of Homeland Security, seeking to attack America, destroy America and kill Americans.

So it seems to me that the object should be here is to find a way not only to protect Americans' rights, but to protect American lives. And I hope that you will devote some of your efforts and I hope this Committee and I hope the Congress will understand the nature of this threat and to have—to say that we can't protect Americans' constitutional rights and at the same time protect America is something that I simply won't accept.

I thank you, Director Comey.

Chairman BARR. Senator Blunt.

Senator BLUNT. Thank you.

Director, thank you for being here and thank you for the work you do. Following up on the comments that Chairman McCain made, what are we really focused on here? A—the recruitment of somebody who's not already in a terror network? And the reason I'm asking this, it seems to me that if you want to use encrypted

equipment from some other country and two of you were committed to do that, you could do that.

I mean, when I'm out of the country, I can get on the internet, the wireless out of the country, the wireless network, use the equipment that I took with me, which is certainly not something I purchased there. So what I'm asking is if—even if we did something about encryption here, I'm no technical expert, but it seems to me that wouldn't stop two people who plan to communicate with each other on devices they got somewhere else from doing that.

Is there something here I don't understand about that? And then the other part of the question is, or is our real target here to monitor the recruiting efforts or the internal efforts of people who aren't in a terror network but are talking in the United States among themselves about doing terrorist things?

Director COMEY. Thank you, Senator. The recruitment tends to take place in a way that we with lawful process can see it either—usually on Twitter or Twitter Direct Messaging, which are not encrypted. And then if it looks productive to the ISIL recruiters, they move them to the end-to-end encrypted communication. And so a major concern is what are the guys in Syria telling these guys and what are they telling them back, and what are they saying to their buddies using encrypted platforms in the United States? So it's both the international, right, and the local within the network in the United States.

Senator BLUNT. I guess what I'm asking is, if the international encrypted equipment is still available, is there anything we can do that stops that from being a problem that you can't penetrate?

Director COMEY. I think the answer is—again, I'm not an expert—if the servers are located entirely outside the United States, that we would have a heck of a time enforcing a regime that would require them to give us access.

Now, I suppose an expert might say to you, well, but if it transits to United States, there's some way we can—we can impose our will on it. I just don't know well enough to evaluate that. So I do think one of the challenges that people have raised with us is to say, even if we fix our problem, you have to address it in some fashion internationally, because the really bad guys will move to infrastructure that is in Western Europe.

And so to solve your problem, people say, you've got—America has got to get its act together, and it's the big dog so you probably ought to do it first. Then your colleagues and allies in Western Europe have to get their act together to make sure there isn't a safe haven there. Now, that still leaves you with people who might want to move their infrastructure to some other less well governed part of the world. So you're always going to have a small part of that problem. But I think the main part of the problem could be dealt with with North America and Europe focusing on it.

Senator BLUNT. And is Europe focusing on it?

Director COMEY. Yes. As you—as I think I said earlier, the U.K. and France, they're a little bit ahead of us on this, the French in particular in the wake of Charlie Hebdo and the—and the Brits. Both—I know the British better—have legislation that requires access to communications. Their challenge is the reverse of what you're saying. The infrastructure is in the United States on which

they want to compel access. And so trying to figure out how to deal with that is a—is a challenge we're still working through.

Senator BLUNT. And so the infrastructure is really the target, as opposed to the device somebody might be using? Even if the device is encrypted, what infrastructure it goes through may or may not accept that encrypted message?

Director COMEY. Well, I think the reason I was talking about the infrastructure is that would give you the ability to compel some—to impose a requirement that that provider, the owner of that infrastructure that sits in your country, comply with American law to give judge—traditional orders to make them effective.

The challenge is, if the infrastructure is not in the United States, who are you compelling to give the judge's order effect?

Senator BLUNT. Mr. Chairman, I think I'm joining the group that's suggesting we have a more technical—does not—not to diminish either your ability in this area or mine. And probably in a closed session, so we could ask questions without being concerned about anybody telling us something that everybody in the world doesn't necessarily need to know so we'd understand this.

But I think we have a bigger problem than we can deal with on our own, and to fight a big fight here that is easily evaded by somebody who wants to evade it would be of concern to me. But in conjunction with others who are perhaps even ahead of us on this, I think the director makes a—makes a good point that we need to be sure we all understand.

Chairman BURR. I assure the Senator that Senator Feinstein and I were up conversing already about how we put together another hearing, if not a series of hearings, to try to get into this a little bit deeper and to better understand, along with the director, what our options might be as we proceed forward.

This is—this is something I would recommend to all the members that they become educated in on a periodic basis, because this is not the end of technological advances. Therefore it's not the—this is not the last challenge we're going to be faced with from a technology standpoint.

Senator Lankford.

Senator LANKFORD. Thank you Mr. Chairman. And you're right, this is not the last one we're going to deal with. This is the latest technological battle we're going to deal with.

Director COMEY, thank you for all your work and please pass on to the folks who worked some very long hours leading up to July the 4th our appreciation for what they did for the Nation and for the citizens of my State and people all over the country. We do appreciate their work very much and you have a terrific team.

The challenge that we face on this is not only the technology side in dealing with terrorism; it's also the benefit that is gained from this. I would tell you the folks at OPM would be glad to talk about encryption and the value of that right now. If they had kept their data in a more encrypted location and stored it better and had greater security on this, whether that be retailers around the country, whether that be banks, whether it be government agencies, we are benefiting from encryption and from the technology that has been invented.

The hard part of this is the other side of it. And so what I'd like to talk about is we've got to have some kind of balance in the conversation because we absolutely need encrypted technology because we are very exposed and we're finding out all the ways that our information is exposed and so we need that technology to continue to advance on one side as we deal with cyber security, but on basic law enforcement and on real threats for physical security, we've got to have a different ability, and I think that's the complicating factor of this.

With that in that conversation, talk to me a little bit about some legal frameworks here. If someone goes on social media and they have child pornography, that's a criminal issue. If someone goes on to social media and says, Here's a group of people to kill and we'd like you to kill them and here's some ideas to do that, talk to me about the legal frameworks between the two. Because there's a step before this when they move encryption that is the recruiting and that recruiting side is a group of individuals that are recruiting based on, we're looking for people who actively believe like we do, which is not the problem, but that will also act out and kill people. Help me understand some of the legal frameworks there?

Director COMEY. Well, the—if someone is on social media talking about the possibility or offering any kind of criminal activity, which includes terrorism because it's a criminal act as well, that that's obviously a predicate for an FBI investigation and for us using our lawful tools, including judicial orders, to find out what's going on there and who are these people.

Senator LANKFORD. Okay. So I'm really talking the step before that then, and that's where you're not talking about now, that social media side of that. What does that trigger at that point, or is that you begin the investigation, you begin the process obviously of trying to track this down because they're encouraging a criminal act on American soil.

But then you've got extra communication that's happening now on the encrypted level; is that what I'm picking up?

Director COMEY. Yes. Right. What's happening is they're broadcasting out this poison through Twitter. They have 21,000 followers now in English and they'll have Twitter-following communications so it tweets back and forth. Then they may have direct messaging through Twitter.

All of which again with lawful process we can get access to and evaluate. And if it looks like someone—and here's the way ISIL operates. If the person appears to be serious, they will then say: Okay, move to this mobile messaging app which is encrypted end-to-end. And that's when we lose them. And so—and we have—as I said earlier, we have no ability—If we intercept that mobile messaging app data traveling back and forth, we can intercept the data, but it's gobbledygook and we can't break that encryption.

Senator LANKFORD. Yes. Right. Yes, that part I understand. So the social media platforms, they still see no issue, once it's clearly known that this is an illegal activity that's happening on their platform? Is their response to say "You can't do that on our platform?" Or their response is, "Hey, we're just open for anything whether it's prostitution, child porn, or terrorism; you can use it?"

Director COMEY. Oh, I'm sorry. I misunderstood the question, Senator. They're being quite good about this, frankly, and it's gotten increasingly good over the last year.

Twitter does not want people engaging in, soliciting, advertising criminal activity of any sort on their social media platform. But they're being particularly aggressive at shutting down and trying to stop ISIL-related sites. I think it actually led ISIL to threaten to kill their CEO, which helped them understand the problem in a better way. And so it's a—they are being quite good about that.

Senator LANKFORD. Okay. And then you've alluded twice now to the U.K. and France are a little bit ahead of us on this, and then you said that they're discussing this. Can you give us greater detail to what they're discussing? When you say they're a little bit ahead of us on this, I think it's a rare moment for Europe to be ahead of us on anything, but that's a whole different issue. So help me understand what you mean by that?

Director COMEY. Right. I don't want to swell the Brits' heads. They're a little bit ahead of us, but then they're not. So let me explain what I mean by that. They have passed legislation that's called "DRIPA"—I don't remember what that stands for—that imposes data retention requirements on communications providers and then also imposes access requirements that the providers must comply with lawful orders for data that's moving on their network.

So they're ahead of us in that they've passed the legislative package that addresses in part what we're talking about here. Where they're not ahead of us is, they have to figure out, so how will that work when all the providers are in the United States? And so how will they enforce their legislation if they want data from someone who's located in California and all the infrastructure's in California? How will they actually make that a reality?

Senator LANKFORD. Okay, thank you.

I yield back.

Chairman BURR. Senator Risch.

Senator RISCH. Thank you, Mr. Chairman.

Director COMEY, those of us on this Committee meet regularly with heads of state and people like you from other countries. Interestingly enough, their top question to us always is and their top concern to us is similar to what we get from the American press and the American people. And that is that this whole thing has gotten to the point where the most serious problem is these lone wolf people who are either inspired or directed from out of their country to do something.

And of course, the most recent horrific example is what happened in Tunisia just last week. And without—obviously we are in an open session, I understand that. But I'd like to give you the opportunity to talk to the American people and tell them how—what a—what a concern this is for you, how this fits into your priorities, and what you're doing about this in matters that are unclassified. Could you do that for me please?

Director COMEY. Sure. Thank you, Senator. ISIL is reaching into the United States, to all 50 States, trying to motivate troubled souls and increasingly kids to either come to their caliphate or kill where you are. And social media, this investment in buzzing in your pocket all day long, actually works. It works to sell shoes, it

works to sell cars, it works to motivate troubled souls to do bad things. We are now reaping the results of a year-long effort by ISIL to invest in this social media push, which is why you see so many arrests by the FBI. These are our disruptions stopping people from going and shooting innocent people or trying to behead them.

And so this is going on all over the place. We're working very, very hard on it. I want the American people to know about it because it's an important thing, but we also need their help. In almost every case, someone saw something. Someone saw something weird that didn't seem right. We've got to get folks just to tell us. I mean, human nature is to write an innocent narrative over the hair standing up on the back of your neck and say: I must have misunderstood; he must be having a bad day. Okay, if it's just a bad day there won't be a problem. We investigate in secret so we don't smear innocent folks.

But we've got to get folks, when they see something that makes the hair stand up on the back of their neck, say, that guy doesn't seem right, and tell somebody, so that we can check it out, right? We need the help—because this spans all 50 States, we've got State and local law enforcement helping us all around the country. We need the good folks of America, if they see something that seems out of place just say something and we'll check it out. You can tell any police officer, any deputy sheriff in the entire United States. Since 9/11 we have gotten our act together and that information will get within minutes to the right people.

Senator RISCH. Director Comey, thank you for that, and I appreciate what you do and what your organization does. And we all know that you've got to be right every day 100 percent of the time. They've only got to be right once.

And so you're doing—you're a good job, and keep up the good work. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Thank you Senator.

Director, we're going to take just a few more questions and I'll just make this note for members. We've got a series of five stacked votes starting at 4:30.

I want to try to sort of wrap a lot of things that you talked about because people have asked individual pieces of this question on "Going Dark." Is your—is your greatest concern finding the balance between what we ask phone companies or service providers or manufacturers to do to their products or their system and where the breakpoint is before they become a foreign company versus a domestic company, where I would take from what your folks said to you, when you get to the point you've chased them out of the country you've just made your problem much worse versus better. Can you help us dissect that?

Director COMEY. Yes. The reason this is the hardest problem I've seen in my career in government is we have important public safety issues that we've talked about that I think everybody agrees are implicated by the universal strong encryption. And then we've got innovation, which is unbelievably important. It's the engine of our amazing country. And we've got security.

As a number of Senators have said, I care a lot about cyber security. I love strong encryption. So how do we take those all—those

things we care about, innovation and jobs, security on the internet and security for ordinary people from crime and terrorism, how do we maximize them all? How do we optimize them all? And as I said, some smart people say: Well, if you do anything, it will destroy the internet or it will chase all the business overseas.

And so I do think we have to engage on the technical solution with smart people and creative people and we need to think about is there an international aspect to this? And again, I'm making this up, but ought not the civilized rule of law countries agree upon a framework that makes sense? Sometimes people say to me: Well, if we do this for you, we've got to do it for China. And my response is: Well, if China wants you to do for me—for them what I want you to do, which is require me to go to an independent judge, show probable cause, get a written order, right, be subject to all this, that would be great for the Chinese people. I don't think China wants you to do what I want you to do. So I'm less worried about what we agree to being used against us in China.

But I am worried about this point that's raised about chasing business to other parts of the Western world, which is why I think we've got to be thoughtful about it.

Chairman BURR. Well, we certainly—we get that part and we're going to follow that up with some tech company questions at a hearing.

Now, before I turn to the Vice Chairman, I want to give you one opportunity. If there's something you want to share with the American people that you haven't already talked about as it relates to the Bureau, I want to give you the opportunity to do that about your folks at the Bureau and what the Bureau does and why the American people should care whether you're successful.

Director COMEY. Well as I said earlier, I—we work for the American people. We are the—I hope a lot of folks know folks in the Bureau. We're ordinary people who've chosen to do this with our lives. We use the tools you gave us. And I'm here not to scare the American people, but to say to the owners of the FBI: I've got a problem; I need help fixing it so that I can continue to do my job.

But make no mistake about it, the folks who work for me, we're going to stay at it every single day round the clock. And if this tool goes away, okay, we'll do our absolute best. But we think it would be irresponsible not to tell the shareholders, the people who own the FBI, the challenges we're facing so that we can figure out whether we can address it.

But my folks that—you know, on TV sometimes we look great, sometimes not. In movies sometimes good, sometimes not. In movies the director is often doing exciting things that I would rip an Achilles doing. But we are ordinary people who've chosen, not to make a good living but to make a different kind of life. We love this work. We love working for you, right? And we're simply here to tell you, sort of give you a status report on how's it going with the tools you've given us.

Chairman BURR. Vice Chair.

Vice Chairman FEINSTEIN. Thanks, Mr. Chairman.

We—this Committee passed out its intelligence authorization bill I think on June 24th. And in that bill we put a provision which would require technology companies to inform the appropriate au-

thority when they obtain knowledge of terrorist activity. Now, this is modeled after an existing law which requires technology companies to notify authorities about cases of child pornography, but it doesn't require companies to monitor any user, subscriber, or customer. It is really the beginning of saying: Look, Look, Mr. and Mrs. American Technology, you have a responsibility, too. What do you think of that?

Director COMEY. It's an interesting idea. I've heard about it. My folks have told me about it. I haven't read it or studied it and so I haven't—I frankly can't give you an intelligent answer. It's an interesting idea. I do find in practice that they are pretty good about telling us what they see so—that's a—I have to give you a non-answer.

Vice Chairman FEINSTEIN. Well, it's really simple. We do that for child pornography. Don't you think we should do it for possible terrorist acts?

Director COMEY. Maybe, but I haven't heard—I'd want to hear out the other side.

Vice Chairman FEINSTEIN. Oh, dear.

Director COMEY. I want to make sure I'm not missing something. Again, I haven't read it. I'm dumb enough when I know something. This is something I haven't studied enough to give you an intelligent answer.

Vice Chairman FEINSTEIN. Okay.

Thanks, Mr. Chairman.

Chairman BURR. Senator Wyden.

Senator WYDEN. Mr. Comey, one last question. If the United States were to require our companies doing business here to ensure government access to encrypted communications, would you expect that foreign governments would create the same requirement for companies operating there?

Director COMEY. I think they might or might try to.

Senator WYDEN. And I will tell you that in my view would clearly be the outcome. I think that would make American individuals and businesses more vulnerable to surveillance by foreign governments.

And I just want to leave you with one last thought. I've been on this Committee for 14 years, so I kind of get a sense where something is headed. And I think, Mr. Director, where this is headed is towards proposals for some kind of stockpile of encryption keys. I don't think we have it fleshed out where Senators are going to want to go, but I get the sense that's where this is going, that there should be some kind of stock pile of encryption keys for the government to access.

I just want you to know that I'm willing to work with you on ideas here but I think this proposal is a big time loser. It's a on ideas here, but I think this proposal is a big-time loser. It's a loser on security grounds for the reasons that I've mentioned. It is a retreat on privacy. And I think it will do great damage to our cutting-edge digital companies that have jobs and pay good wages.

So I hope we're not going to go there. I just want you to know my sense, having listened to a couple of hours of this and listening to this morning's testimony, where I think this is headed and I think it is the wrong way to proceed.

Thank you, Mr. Chairman.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Director Comey, you've heard this before, but I want to say it again. Please thank all of your personnel, not just for their efforts in recent weeks but their efforts that go unsung year in and year out.

I want to thank you in particular for the amount of humility that you've shown today. I think it's really helpful at wrapping our heads around how we should proceed on this because I think—I think the most dangerous thing is to jump to a solution that turns out to be the wrong solution.

I have some ideas that I won't share in open session, that I'll share with you and share with my colleagues here, about places we should be investing right now to address some of these concerns. And I'll just reiterate, I think we would be making a mistake if we immediately jump forward and say we passed a law tomorrow that prohibited strong end-to-end encryption with temporary expiring keys, and effectively what we did under that scenario, or at least what I would fear, is that a terrorist or a criminal would simply download an app from Pakistan or somewhere else that would allow them to get around this scenario. And it would put our Americans' data at risk, while protecting theirs effectively.

So I think we just need to think through all of that to make sure that at the end of the day, we're getting at the people who are causing the problem and we're not building in weakness into the protection of our country's data, be it the government or just individuals who expect their financial data, their healthcare data, all the things that we use online now, to remain—to remain private.

So with that, once again, I would ask you to share any final thoughts and thank you for realizing that there are going to be a lot of questions and realizing that we're not going to have all the answers immediately and we shouldn't jump to answers before we completely understand the problem.

Director COMEY. Well, thank you, Senator. I agree that something has to be approached carefully. As I said, I think it's the hardest problem I've seen in government. The stakes are very, very high on all sides of this.

I think we care about the same things whether we're from industry or government, and I think that's one of the great things about this country. We do hard stuff when we talk about it together and figure out together, especially when the whole effort is around shared values.

Senator HEINRICH. I'll leave you with one last thought. We've heard a lot about the amazing innovations of Silicon Valley and I would tend to agree that, especially on the business front, incredible stuff comes out of there all the time. I think as we seek a solution to some of these things, we should not forget the incredible innovations that come out of our national laboratories. And some of—some of those solutions may make even better sense in this scenario.

So thank you once again, Director.

Chairman BURR. Thank you, Senator Heinrich. I'd think less of you if you didn't get that plug in there on the lab before you left.

And I won't speak for the Vice Chairman but, you know, if anything I've been a little frustrated, frustrated that nobody in the ad-

ministration, no agency, is coming up and saying: Here's what we think we need. I mean, we've been talking about "Going Dark" for some time and I think you deserve a tremendous amount of credit for your restraint. Don't know that we know the answer yet, therefore we're not laying proposals on the table. We're not up saying: Here's a solution we think might work. We're—we'll come when we've got a solution we know will work, we know we can do.

So I commend you for that. I hadn't heard anybody talk about thousands of keys until today. I'm sure there's some that sit at home at night and are concerned that maybe that's the choice we'll make. If it were that easy, I think we'd already have a solution proposed to us and we'd be considering legislation and Dianne and I would be hashing it out with our members. The fact is that we know that that's not going to meet the test of getting legislation, one, through Congress; two, possibly signed into law. And I think we're just as challenged as you are, Director, about what the solution is. We want to—we want to be part of the solution. We want to work with you.

I think it's safe to say that we're probably going to have some hearings. They may be closed, they may be open. CEOs of tech companies, the privacy groups. We're going to try to reach out to some experts. Not with the belief that we're going to come up with a solution that you haven't come up with, but that we're going to be knowledgeable enough as we go down that road together to write legislation that both sides are confident of where we're going and we're fairly confident that it's going to be beneficial to the end goal, which is defending the American people.

So let me just add one note. When I left prior to the 4th after doing this now for 15 years since 2000, I was convinced that we were going to have an incident before I came back this Monday. It didn't happen. And I am convinced it did not happen because the Bureau and the intelligence community worked like it's designed to work, and you asked your folks all around the country to go on a different schedule and they did and they were on that tempo for weeks and may still be there.

And the fact is that we were able to thwart a lot of things early and maybe postpone some things that might have happened. Your folks deserve a tremendous amount of credit and the entire intelligence community does. We know this is not going away with the 4th of July. Ramadan stays vibrant for a few more weeks. There will be another national holiday and there'll be a target and we'll pick up on some things. But we also have to recognize the fact that we've got some areas that we're going to be making decisions without the information we've had in the past because of the communication tools that these folks are using.

We want to be able to address this as quickly as we can so that we can return to as robust of information sharing between intelligence and law enforcement, so that your folks feel confident they can do what they're asked to do versus just hoping that we're putting on a good enough face on Saturday that we're scaring the enemy or the opponent that well.

But you deserve a tremendous amount of credit for how over the last three or four weeks the Bureau has defended the American people. And for that, please give our regards to all at the Bureau.

And with that, Director, thank you for being here. Sorry that you had to pull a double-header today, but you're a strong guy. And hopefully your Achilles is still there. This hearing is adjourned.
[Whereupon, at 4:20 p.m., the hearing was adjourned.]

