FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

April 15, 2016

To: Subcommittee on Oversight and Investigations Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives"

On **Tuesday, April 19, 2016, at 10:00 am in room 2123 of the Rayburn House Office Building**, the Subcommittee on Oversight and Investigations will hold a hearing titled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives." The hearing will focus on the debate surrounding increased use of strong encryption and law enforcement's concerns regarding access to encrypted information.

I. BACKGROUND

Encryption is a technique used to secure electronic communications from unwanted access. Encryption transforms a message from a format where it can be read (plaintext) to a format where it cannot be read (ciphertext), while decryption then changes a message from ciphertext back to plaintext.[1] Data can be encrypted while it is "in transit" between users, or while it is "at rest" in storage on a device, drive, or server.[2] When a user views or otherwise processes the data, it is in plaintext.

"End-to-end encryption" is used to secure electronic communications by allowing only the individuals who send and receive a message to access it—not anyone in between.[3] End-to-end encryption prevents hackers and even the messaging service itself from decrypting the

[1] Congressional Research Service, *Encryption: Selected Legal Issues* (Mar. 3, 2016) (R44407).

[2] *Id.*

[3] Andy Greenburg, *Hacker Lexicon: What is End-to-End Encryption*, Wired (Nov. 25, 2014).

message. End-to-end encryption is becoming increasingly widespread on computer and smartphone devices and applications.

In September 2014, for example, Apple released an update to its mobile operating system (iOS 8) that automatically implements end-to-end encryption by creating a device-specific encryption key, for which Apple does not retain a copy.[4] In prior versions of its operating system, Apple maintained a key that could allow the company to unlock any device without the passcode. This practice further enabled Apple to unlock devices for law enforcement and for users who had locked themselves out. By no longer holding such a key, Apple claims it no longer has the ability to unlock devices for anyone under any circumstance. Operating systems for Android devices and the Facebook-owned WhatsApp, now also offer end-to-end encryption services.[5]

Encryption provides many important benefits, such as consumer privacy protections for activities like online banking or internet purchases, and in securing communications or important data from cybercriminals. Intelligence and law enforcement communities, however, have expressed concerns that the trend towards stronger forms of encryption has potential downsides affecting law enforcement's ability to access certain encrypted information.

II. THE DEBATE OVER ENCRYPTION AND LAW ENFORCEMENT'S ACCESS TO INFORMATION

A. History

Encryption of electronic communications has been around for decades, as has the debate about technological advances limiting law enforcement's access to data. In the 1990s, new digital and wireless communications raised concerns regarding law enforcement's ability to intercept communications for lawfully authorized surveillance.[6] In response, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994.[7] CALEA requires telecommunications carriers to assist law enforcement in executing authorized electronic surveillance; however, CALEA does not apply to or cover e-mail or data stored on smartphones or similar devices. Telecommunications carriers are not required or responsible under CALEA or any other laws 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."[8]

---

[4] Congressional Research Service, *Encryption: Selected Legal Issues* (Mar. 3, 2016) (R44407).

[5] *Id.*; *WhatsApp Introduces End-to-End Encryption*, New York Times (Apr. 5, 2016).

[6] Congressional Research Service, *Encryption: Selected Legal Issues* (Mar. 3, 2016) (R44407).

[7] 47 U.S.C. §1002(b)(3).

[8] *Id.*

Also in the 1990s, controversy around the use and export of data encryption, labeled the "Crypto Wars," saw the government attempt to limit the use and proliferation of strong cryptography.[9]

B. Renewed Concerns

Recent developments in technology products and services and the security policies of some technology companies — in particular the growth of end-to-end encryption — have led to increased concerns from law enforcement. In the course of investigations, encryption has limited the government's ability to obtain access to some electronic communications, even in circumstances that satisfy constitutional warrant requirements.[10] Justice Department officials have compared these situations to "a house that can't be searched, or a car trunk that could never be opened."[11]

As explained by one group of experts who assessed the encryption debate:

> The U.S. intelligence and law enforcement communities view this trend with varying degrees of alarm, alleging that their interception capabilities are "going dark." As they describe it, companies are increasingly adopting technological architectures that inhibit the government's ability to obtain access to communications, even in circumstances that satisfy the Fourth Amendment's warrant requirements. Encryption is the hallmark of these architectures. Government officials are concerned because, without access to communications, they fear they may not be able to prevent terrorist attacks and investigate and prosecute criminal activity.[12]

Law enforcement officials have increasingly referenced this "Going Dark" concern as affecting investigations of possible criminal or terrorist activity. For example, in recent testimony before the House Judiciary Committee, FBI Director James Comey stated, "We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders."[13] He went on to say that the "Going Dark problem is, at base, one of technological choices and capability," explaining that the FBI is

---

[9] Congressional Research Service, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations* (Feb. 18, 2016) (R44187).

[10] The Berkman Center for Internet & Society at Harvard University, *Don't Panic – Making Progress on the "Going Dark" Debate* (Feb. 1, 2016).

[11] Devlin Barrett and Danny Yadron, *New Level of Smartphone Encryption Alarms Law Enforcement*, Wall Street Journal (Sept. 22, 2014).

[12] The Berkman Center for Internet & Society at Harvard University, *Don't Panic – Making Progress on the "Going Dark" Debate* (Feb. 1, 2016).

[13] *Id.*

seeking to "ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe."[14]

State and local law enforcement have echoed the FBI's concerns. For example, New York County's District Attorney stated in recent Congressional testimony that due to the centrality of smartphones to many people's lives, "default device encryption cripples even the most basic steps of a criminal investigation."[15] He cited 175 Apple devices his office is unable to access as of March 2016, due to Apple's encryption system.[16]

Tech companies, privacy advocates, and others have argued that requiring companies to weaken encryption to provide special access for law enforcement would introduce vulnerabilities that could compromise device security.[17] They call such special access a "backdoor." They also argue that due to the ready availability of encryption software around the world, a system that allows law enforcement access in the United States would not prevent terrorists and criminals from communicating in an inaccessible, encrypted manner.[18] U.S. government-mandated special access or tech company assistance could lead to similar requests by oppressive regimes around the world to access devices for their own purposes. The tech community's concerns also reflect the heightened privacy concerns of consumers and companies following the disclosures of government surveillance by Edward Snowden in 2013.[19]

Apple CEO Tim Cook has been particularly vocal in criticizing government efforts to require special access to encrypted devices for law enforcement. For example, in a letter to customers, he stated, "we have used encryption to protect our customers' personal data because we believe it's the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."[20] He argued that government efforts to compel Apple to assist in unlocking an encrypted iPhone would "hurt only the well-meaning and law-abiding citizens," as bad actors would still have access to encryption.

---

[14] *Id.*

[15] House Judiciary Committee, Testimony of Cyrus Vance, Jr., District Attorney, New York County, *Hearing on The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong. (Mar. 1, 2016).

[16] *Id.*

[17] Apple, *A Message to Our Customers* (Feb. 16, 2016) (online at www.apple.com/customer-letter/); The Berkman Center for Internet & Society at Harvard University, *Don't Panic – Making Progress on the "Going Dark" Debate* (Feb. 1, 2016).

[18] Open Technology Institute, *The Crypto Cat is Out of the Bag: An Illustrative Inventory of Widely-Available Encryption Applications* (Dec. 8, 2015).

[19] *Jeh Johnson Warns of Post-Snowden Encryption Frenzy*, Politico (May 15, 2015).

[20] Apple, *A Message to Our Customers* (Feb. 16, 2016) (online at www.apple.com/customer-letter/).

Some in the tech community have also disputed that law enforcement is "Going Dark," arguing instead that we are now in a "golden age of surveillance."[21] They argue that the growth of technology has resulted in an expansion of surveillance capabilities. A recent report from Harvard's Berkman Center for Internet and Society examined this debate over surveillance and its limits.[22] The report found that end-to-end encryption is unlikely to be fully adopted by many companies or platforms, because businesses that provide communications services require access to their customer's data for revenue and product functionality. They also argue that metadata, like location data, telephone calling records, and header information in e-mails, must remain unencrypted for systems to operate. The report also noted that the projected growth of various connected devices and appliances of everyday life—the so-called "Internet of Things"—has the potential to drastically change surveillance and expose a wealth of information to law enforcement.[23] The report thus concludes, "communications in the future will neither be eclipsed into darkness nor illuminated without shadow."[24]

This encryption debate raises novel questions about the legal balance between individual privacy and national security.[25] There is limited case law regarding access to smartphones and the issue of compelling decryption. The debate further raises legal issues related to compelling an individual user to provide his or her password to decrypt data or compelling a device or software manufacturer to assist in providing access or breaking encryption.[26]

C. Recent Developments in the FBI – Apple Dispute

The December 2, 2015, terrorist attack in San Bernardino, California and the subsequent investigation have pushed the encryption and "Going Dark" debate to greater national prominence. Following the attack, investigators recovered an iPhone belonging to one of the suspected shooters, but two months later were still unable to unlock the device.[27]

On February 16, 2016, a federal magistrate judge, at the Justice Department's request, ordered Apple to provide "reasonable technical assistance to assist law enforcement agents in

[21] Center for Democracy & Technology, *Going Dark Versus a Golden Age for Surveillance* (Nov. 28, 2011).

[22] The Berkman Center for Internet & Society at Harvard University, *Don't Panic – Making Progress on the "Going Dark" Debate* (Feb. 1, 2016).

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] Congressional Research Service, *Encryption: Selected Legal Issues* (Mar. 3, 2016) (R44407).

[27] Congressional Research Service, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations* (Feb. 18, 2016) (R44187).

obtaining access to the data" on the smartphone.[28] Apple appealed the ruling, arguing that the software required to access the phone does not exist and creating such software would weaken privacy protections.[29] On March 21, 2016, one day before a scheduled hearing, the FBI asked for a delay of the proceedings and announced that a third party had approached them with a method to access the iPhone in question.[30] On March 28, the FBI confirmed that it had successfully accessed the data stored on the shooter's phone and that it was requesting the court to vacate the order compelling Apple to assist it in accessing the phone.[31]

Several congressional committees have thus far held hearings on this issue.[32] On March 21, 2016, the House Energy and Commerce and Judiciary Committees announced the creation of an encryption working group to examine the complicated legal and policy issues surrounding encryption.[33]

III. WITNESSES

Panel 1

Amy Hess
Executive Assistant Director
Science and Technology Branch
Federal Bureau of Investigation

Chief Thomas Galati

---

[28] United States District Court for the Central District of California, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, Order Compelling Apple, Inc. to Assist Agents in Search (Feb. 16, 2016).

[29] *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, New York Times (Feb. 17, 2016).

[30] United States District Court for the Central District of California, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451M, Government's Ex Parte Application For a Continuance (Mar. 21, 2016).

[31] United States District Court for the Central District of California, *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, CM 16-10, Government's Status Report (Mar. 28, 2016).

[32] Committee on Judiciary, *Hearing on The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong. (Mar. 1, 2016); Committee on Oversight and Government Reform, *Hearing on Encryption Technology and Potential U.S. Policy Responses*, 114th Cong. (April 29, 2015).

[33] Committee on Energy and Commerce, *Upton, Pallone, Goodlatte, Conyers Announce Bipartisan Encryption Working Group* (Mar. 21, 2016).

Intelligence Bureau
New York Police Department

Sheriff Ron Hickman
Harris County, Texas
Representing the National Sheriffs Association

Captain Charles Cohen
Commander
Office of Intelligence and Investigative Technologies
Indiana State Police

Panel 2

Bruce Sewell
Senior Vice President and General Counsel
Apple Inc.

Amit Yoran
President
RSA

Dr. Matthew Blaze
Associate Professor, Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

Daniel Weitzner
Director, MIT Internet Policy Research Initiative
Principal Research Scientist, MIT Computer Science and Artificial Intelligence Lab
Massachusetts Institute of Technology