U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

April 15, 2016

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing on “Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives”

On Tuesday, April 19, 2016, at 10:00 a.m. in 2123 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled “Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives.” This hearing will examine the balance between the benefits of strong encryption and its effect on the law enforcement and intelligence communities. Recent debate has focused heavily on a February 2016 court order that sought to compel Apple, Inc. (Apple) to assist the Federal Bureau of Investigations (FBI) in unlocking an iPhone used by one of the San Bernardino attackers. However, the issues surrounding the growing prevalence of default encryption are much broader. As such, this hearing will feature testimony from a diverse set of stakeholders, including representatives from federal and state law enforcement, as well as representatives from the device and enterprise information technology industries, and academia.

I. WITNESSES

First Panel

- Amy Hess, Executive Assistant Director for Science and Technology, Federal Bureau of Investigations;

- Thomas Galati, Chief, Intelligence Bureau, New York Police Department;

- Ron Hickman, Sheriff, Harris County Sheriff’s Office, on behalf of the National Sheriff’s Association; and

- Charles Cohen, Commander, Indiana Internet Crimes Against Children Task Force.

Second Panel

- Bruce Sewell, General Counsel, Apple, Inc.;

- Amit Yoran, President, RSA Security LLC;

- Daniel Weitzner, Director and Principal Research Scientist, Computer Science and Artificial Intelligence Laboratory (CSAIL) Decentralized Information Group (DIG), Massachusetts Institute of Technology; and

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

II. BACKGROUND

While concerns surrounding encryption and its effect on law enforcement has gained prominence in recent years, the debate regarding government access to encrypted data – commonly referred to as the "Crypto Wars" – has existed for decades. For example, in the mid-1990's, intense debate over encryption prompted proposals to install a government-mandated method to permit lawful "exceptional access" capabilities into computing technologies. This so-called "Clipper Chip" was a "backdoor" that would, in theory, preserve the government's ability to access encrypted information with legal authorization. The technology community resisted this proposal, arguing that such a system would create a vulnerability that could be exploited by actors outside of the government.[1] These concerns were ultimately validated when a critical flaw was discovered in the chip's design.[2]

The growth in recent years of digital communications platforms and the spread of default encryption have rejuvenated the debate. Previously, encryption technologies – though highly effective if implemented properly – were complex, cumbersome, and hard to use. Most users, including criminals, did not possess the technical proficiency or patience to deploy strong encryption. However, mounting concerns regarding the security and privacy of digital data in recent years has incentivized companies to develop products and platforms that incorporate strong encryption by default, thus facilitating the widespread adoption of encryption technologies.

As a result, the law enforcement and intelligence communities, led primarily by the FBI, have reiterated their claims that they are losing the ability to monitor, obtain, and otherwise use the digital evidence associated with suspected terrorists, child predators, and other criminals. It is true that the deployment of strong encryption by companies like Apple and Google, and messaging apps like WhatsApp and Signal, create situations where neither the company nor the authorities can easily gain access to decrypted data – a situation commonly referred to as "going dark."

However, technology companies have strongly rejected any calls that would force them to weaken encryption or to otherwise create backdoors in their products. They claim that doing so would significantly undermine the security of their products and the wider internet, and would leave huge swaths of data vulnerable to hacking and theft. Recent discoveries of exploitable vulnerabilities in internet products, most notably the unauthorized backdoor discovered in

[1] Steven Levy, *Battle of the Clipper Chip*, N. Y. TIMES, June 12, 1994, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all.
[2] John Markoff, *Flaw Discovered in Federal Plan for Wiretapping*, N. Y. TIMES, June 2, 1994, http://www.nytimes.com/1994/06/02/us/flaw-discovered-in-federal-plan-for-wiretapping.html.

networking equipment provider Juniper's products,[3] support the technology community's claims.[4]

The majority of the recent public debate has centered on the February 2016 court order to compel Apple to assist the FBI in unlocking a specific iPhone that was used by one of the San Bernardino attackers. In that case, the FBI eventually withdrew its request after an unidentified third-party provided an undisclosed method for gaining access into the iPhone in question.[5] There are, however, other pending cases – including in New York where a federal magistrate judge initially ruled in Apple's favor and the government has appealed – and there will inevitably be more in the future.[6]

While these investigations provide valuable case studies, the issues implicated in the Crypto Wars debate encompass many stakeholders beyond Apple and the FBI, and many technologies beyond iPhones. For example, the messaging platform WhatsApp recently announced that it had completed its planned roll-out of strong, "end-to-end" encryption across the entirety of its products.[7] In completing this roll-out, WhatsApp has extended the number of individuals protected by strong encryption by nearly a billion.[8]

These examples – the iPhones in each court case, and WhatsApp – represent the two primary types of data that encryption may be used to protect; data-at-rest and data-in-transit. In the recent cases involving iPhones, law enforcement is interested in obtaining access to data-at-rest in the device itself. In the case of WhatsApp's encrypted messaging, law enforcement and others are concerned about having access to communications, or data-in-transit. Data-at-rest refers to information that is statically stored, most commonly on devices such as smartphones or in the cloud. Data-in-transit, on the other hand, refers to information as it moves throughout the internet. This can refer to data that is being sent from a desktop browser to a company's server, for example, or – as in WhatsApp's case – from a smartphone to another smartphone. While the encryption technologies used to protect data-at-rest and data-in-transit are, at their core, similar,

[3] *2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756),* JUNIPER NETWORKS, Dec. 20, 2015, https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST.

[4] Several cryptographic experts and government agencies, including the United States Computer Emergency Readiness Team (US-CERT), have indicated that the Juniper vulnerability could allow unauthorized actors to intercept and decrypt otherwise protected communications on a commercial scale. See: *Vulnerability Note VU#640184 Juniper ScreenOS contains multiple vulnerabilities*, COMPUTER EMERGENCY READINESS TEAM | SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY, Dec. 21, 2015, https://www.kb.cert.org/vuls/id/640184.

[5] Ellen Nakashima, *FBI paid professional hackers one-time fee to crack San Bernardino iPhone*, WASH. POST, Apr. 12, 2016, https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

[6] Ellen Nakashima, *Judge rules in favor of Apple in key case involving a locked iPhone*, WASH. POST, Feb. 29, 2016, https://www.washingtonpost.com/world/national-security/judge-rules-in-favor-of-apple-in-key-case-involving-a-locked-iphone/2016/02/29/fa76783e-db3d-11e5-925f-1d10062cc82d_story.html.

[7] Previously, their strongest implementation applied only to smartphones running the Android mobile operating system, and did not cover group, photo, or video messages. See: moxie0, *WhatsApp's Signal Protocol integration is now complete*, OPEN WHISPER SYSTEMS, Apr. 5, 2016, https://whispersystems.org/blog/whatsapp-complete/.

[8] Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED, Apr. 5, 2016, http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

the distinction between the two forms of data is important to the technical and policy discussion of this challenge.

There are three primary types of technologies that create data-in-motion and data-at-rest, each of which affects “going dark” differently:

- **Cloud Services** – Apple’s iCloud, Google’s Gmail and associated programs (Docs, Sheets, etc.), and Dropbox are some of the most well-known examples of cloud services. These services allow users to access data such as email, documents, and media over the internet through, for example, web browsers or apps.
    - **Effect on “going dark”: Low** – The majority of cloud services are hosted on hardware owned and operated by private companies that may analyze the associated data. While the data may be transported and stored in an encrypted format, the entity hosting the data likely possesses the ability to decrypt it.
- **Electronic Communications** – Messaging programs like WhatsApp, iMessage, and Google Hangouts, video and voice chat programs like Skype, FaceTime, and WebEx, along with more traditional methods like email, are just a few examples of the types of electronic communications that exist today. Regardless of specific features, “electronic communications” use the internet to send data between two or more users.
    - **Effect on “going dark”: Varies** – Different types of electronic communications vary greatly in terms of their use of encryption. Some programs like iMessage and WhatsApp are specifically designed to prevent anyone other than the message recipients from decrypting message data. Others, like Skype and Google Hangouts, encrypt data in transit, but have access to decrypted data at some point in the data’s lifetime.
- **Devices** – This category includes smartphones (like Apple’s iPhone and those running Google’s Android operating system), tablets, and laptops. As a general rule, devices tend to contain a significant amount of data pertaining to the device’s owner, including chat logs, emails, personally-identifiable information and much more.
    - **Effect on “going dark”: High** – Most modern devices now use operating systems that automatically employ some level of encryption. While traditional devices like laptops usually require that users manually enable higher levels of encryption, modern smartphone and tablet operating systems (including iOS and Android) are fully encrypted by default. Further, these operating systems are often designed in such a way as to make brute-forcing the encryption mathematically impossible, both for the associated companies and any interested third-parties such as law enforcement.

The growth of new technologies such as the Internet of Things (e.g. smart TVs, thermostats, baby bottles, etc.) and cyber-physical systems (smart grid, connected automobiles, medical devices, etc.) add new layers of complexity to this debate that must also be considered.

On the one hand, the growth of connected technologies opens new opportunities for investigation and surveillance by the law enforcement and the intelligence communities. On the other hand, many of these technologies – especially cyber-physical systems – will depend on strong encryption to ensure the security of products that could result in catastrophic or physical harm if compromised.

The unintended consequences of weakening or otherwise undermining strong encryption may range from the reduced economic competitiveness of U.S. companies, to an increased threat to the safety of products, the security of information, and the privacy of U.S. citizens. However, widespread default encryption could provide safe havens for terrorists, child predators, and other bad actors. This hearing presents an opportunity for representatives from law enforcement and the technology community to educate Congress and the public on the critical equities faced by both stakeholders, and to discuss how society may balance the law enforcement's need for access to encrypted data and the critical importance of safe, secure systems.

III. ISSUES

The following issues may be examined at the hearing:

- How has the evolution of encryption impacted law enforcement and intelligence capabilities, and how is it expected to impact those capabilities in the future?

- What are the concerns for data-in-transit and data-at-rest?

- Is a primary factor in the "going dark" phenomenon strong encryption, or is it the default application of strong encryption?

- How useful is metadata to investigations and prosecutions as compared to content data (i.e. text messages, pictures, etc.)?

- Is "legal hacking" by the government a viable option, and if so, what factors must be considered?

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact John Ohly or Jessica Wilkerson of the Committee staff at (202) 225-2927.