HEARING BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

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

JULY 8, 2015

QUESTIONS FOR THE RECORD
FROM CHAIRMAN GRASSLEY TO
JAMES B. COMEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION:

1. <u>The 2014 Wiretap Report and the "Data-in-Motion" Problem</u>

The Administrative Office of the United States Courts releases an annual "Wiretap Report," concerning intercepted communications pursuant to Title III of the Omnibus Crime Control and Safe Streets Act. The most recent Wiretap Report for 2014 showed that law enforcement confronted encryption in a very small fraction of wiretap applications and was unable to decipher encrypted communications in only a few of those cases. Some commentators, including Professor Swire at the hearing, have asserted that this report contradicts law enforcement's claim that it is "Going Dark" and instead proves that encryption is not harming its ability to investigate crime by intercepting "data-in-motion." Regardless, there is no doubt that Congress would benefit from concrete statistical information about the scope of the "Going Dark" problem and how it is affecting law enforcement.

a. Does the Wiretap Report provide helpful data for evaluating the "Going Dark" problem faced by law enforcement, at least in the "data-in-motion" context? Or, as Deputy Attorney General Yates suggested in her testimony, does the Wiretap Report only reflect the number of applications that are sought and impacted by encryption, not the number of applications that are never sought because of encryption?

Response: Please see the response to Chairman Grassley's question 2 to Deputy Attorney General Yates, *infra*.

b. If the Wiretap Report is not a good benchmark for the "data-in-motion" problem, can the Federal Bureau of Investigation work to develop a better mechanism to keep track of the number of investigations that are negatively

impacted by strong encryption and share that information with Congress so that Congress can better evaluate the issue?

Response: Yes. The FBI is currently working on improving enterprise-wide quantitative data collection to better explain the "data-in-motion" problem. The objectives are to improve and streamline data collection metrics and ensure that the FBI has access to timely and accurate quantitative data to capture and convey the problem.

2. The Impact of Encryption and the "Data-at-Rest" Problem

Regarding the "data-at-rest" problem, District Attorney Vance stated in his written testimony to the Committee that "when smartphone encryption is fully deployed by Apple and Google, 71% of all mobile devices examined – at least by my Office's lab -- may be outside the reach of a search warrant."

a. Does the Federal Bureau of Investigation have similar information regarding the potential impact of encryption on the "data-at-rest" problem?

Response: Yes. The FBI encounters many of the same brands and models of electronic devices as the New York District Attorney's crime lab, and we utilize many of the same commercial forensic tools. The two companies that you reference share a large percentage of the smart phone operating system marketplace in the United States. As with the New York District Attorney's Office, the devices we encounter during investigations are generally representative of what is popular in the commercial marketplace. Some companies have advertised their intention to fully implement encryption methodologies that they are unable to bypass, even with lawful court order. As a consequence, the data on the vast majority of the devices seized in the United States may no longer be accessible to law enforcement even with a court order or search warrant.

b. For instance, does the FBI have any similar statistical information on how often it has obtained a judicially authorized search warrant for the digital contents of a device but was nonetheless unable to execute the warrant due to encryption? Similarly, does the FBI have any similar statistical information on how often it has obtained a judicially authorized search warrant to obtain the contents of an email account but was unable to execute the warrant due to encryption?

Response: No. As with the "data-in-motion" problem, the FBI is working on improving enterprise-wide quantitative data collection to better explain the "data-at rest" problem. Before the recent introduction of encrypted-by-default electronic devices into the marketplace, the challenges posed by encrypted "data at rest" were encountered intermittently in investigations. Prior to 2014, the FBI's Going Dark Initiative focused primarily on the data-in-motion

challenges. The technology industry's shift toward fully encrypted-by-default devices has been extremely rapid and the FBI has been working to shift our business practices to address these new challenges. Our ability to rely on commercial forensic tools has diminished, we can no longer reliably obtain critical information from certain manufacturers, and we have found ourselves relying on self-initiated efforts to solve these extremely complex challenges.

As noted above, the FBI is currently working on improving enterprise-wide quantitative data collection to better understand and explain the "data at rest" problem. This process includes adopting new business processes to help track when devices are encountered that cannot be decrypted, and when we believe leads have been lost or investigations impeded because of our inability to obtain data. As we adjust business practices to capture this information, one thing we know for certain is that, even with a court order or warrant, we increasingly cannot obtain the communications, transactions, documents, records, and contact lists of criminals that are contained within devices. We agree that the FBI must institute better methods to measure these challenges when they occur.

c. If the FBI does not have such information, can it develop a mechanism to keep track of the number of investigations that are negatively impacted by smartphone encryption and share that information with Congress so that Congress can better evaluate the issue?

Response: Yes. The FBI is working to identify new mechanisms to better capture and convey the challenges encountered with lawful access to both data-in-motion and data-at-rest.

3. CALEA

In prior testimony before Congress, the Federal Bureau of Investigation suggested that the "data-in-motion" problem was associated with limitations on the enforceability and scope of the Communications Assistance for Law Enforcement Act (CALEA).

a. How much of the "data-in-motion" side of the problem is attributable to problems with the enforceability of CALEA – i.e., providers or services that are covered by CALEA but that do not or are unable to comply with CALEA? Alternatively, how much is attributable to problems with the scope of CALEA – i.e., providers or services that are not covered by CALEA, either by statute or by FCC regulation?

Response: There are several constraints inherent to CALEA that limit certain provisions of the statute. Many of these constraints have become more pronounced over time as new communications services have been introduced. At the time of enactment, the portion of the

communications infrastructure covered by CALEA was significant – i.e., landline and cellular telecommunications carriers. In 2005, the scope was expanded through a decision from the Federal Communications Commission (FCC) to include interconnected Voice over Internet Protocol (VoIP) service providers and providers of broadband Internet access services. However, services and networks evolve very quickly and systems are frequently updated. Indeed, there have been instances where companies upgraded equipment or altered their architectures and they no longer have the capability to isolate the communications of the subject of a court order.

In some cases, law enforcement agencies may be able to install or provide equipment to facilitate the implementation of a court order. However the installation of law enforcement equipment tends to yield incomplete results, is resource intensive, and is not available to all of law enforcement – the very situation CALEA was intended to remedy.

As traditional telecommunications services become less popular, users have migrated to Internet-based communications services that are presently outside the scope of CALEA, and therefore are not subject to the CALEA requirement to have a lawful intercept capability. For example, pursuant to technical standards adopted under CALEA, telecommunications carriers maintain an interception capability for traditional text messages ("Short Message Service," or "SMS"). There are no analogous CALEA-based standards or requirements for Internet-based instant messages. This is true even though both types of messages are carried over connections made available by telecommunications carriers and seamlessly integrated within some popular Internet-based instant messaging applications.

b. How many providers or services have refused to comply with court orders on the basis that they are not subject to CALEA? Please identify each instance and each provider or service that has refused to comply with a court order in this area.

Response: Today's Internet-based service providers are generally not required to develop and maintain technical capabilities for intercepting communications. In many instances, providers that are not subject to the requirements imposed by CALEA are often unprepared to assist law enforcement when served with a court order. These providers may leverage internal systems not designed for interception purposes in an attempt to comply with lawful interception orders. As a result of this ad-hoc approach, court ordered compliance can be affected in a number of different ways, including: providing incomplete or unintelligible information that requires additional troubleshooting and support from both the provider and law enforcement; and delaying the delivery of the information as the provider manually retrieves data from its systems with a frequency that can vary between hours, days, and weeks. Ultimately, it has been the FBI's experience that none of the providers offering application-based communication services outside of CALEA are able to provide all of the information law enforcement is authorized by court order to collect.

For more information, please also see the response to Senator Whitehouse's question 1 to Director Comey, *infra*.

4. Spyware

In June, I wrote to you to ask for details about the FBI's use of spyware. According to press reports, some types of spyware programs can be remotely deployed to a targeted computer to surreptitiously activate the computer's camera and microphone; collect passwords; search the computer's hard drive, random-access memory, and other storage media; generate latitude and longitude coordinates for the computer's location; and intercept phone calls, texts, and social media messages. Some have argued that spyware is a potential solution to the Going Dark problem because it allows law enforcement to forgo trying to break strong encryption and instead lets law enforcement see the same decrypted version of the communication that the sender or receiver sees on his or her device. In fact, in 2013 the Wall Street Journal ran an article entitled: "FBI Taps Hacker Tactics to Spy on Suspects: Law-Enforcement Officials Expand Use of Tools Such as Spyware as People Under Investigation 'Go Dark,' Evading Wiretaps."

In your testimony, you stated: "what I'm confirming here is we cannot break strong encryption. We have not found that tool. I don't think it exists. But we look for other ways around the margins if a judge gives us permission to be able to get into a room or get into a device."

a. Does the FBI possess or deploy spyware that allows it to see decrypted versions of messages on a targeted device that were transmitted using strong encryption?

b. If so, has the FBI evaluated to what extent the use of such spyware could mitigate or resolve the problems of "Going Dark" without requiring companies to provide back doors or otherwise limit strong encryption? If so, what were the conclusions of that evaluation?

c. If current spyware technology does not have the capability to see decrypted versions of communications sent with strong encryption, has the FBI considered increasing its research and development of spyware tools in pursuit of this capability?

Response: The responses to these inquiries are classified and are, therefore, provided separately. In addition to the classified annex accompanying this document, we note that the Department of Justice has previously responded to the Committee's letters on this topic. Specifically, on July 14, 2015, the Department of Justice responded to the Committee's letter to the Deputy Attorney

General, dated April 27, 2015. The Committee submitted a follow-up letter to the FBI and the Drug Enforcement Administration (DEA) on July 15, 2015. On January 14, 2016, the FBI provided an unclassified response with a classified annex to the Committee in response to its letters of June 12, July 15, and December 16, 2015. Further, DEA responded to the July 15, 2015, letter on January 14, 2016.

QUESTIONS FROM CHAIRMAN GRASSLEY TO SALLY QUILLIAN YATES, DEPUTY ATTORNEY GENERAL

1. Legislative Proposals Timeline

At the hearing, I asked you whether the Obama Administration planned to come forward with a proposed legislative solution to the "Going Dark" problem, as well as the fate of its reported 2012 proposal. You told me that the Department of Justice is not seeking a legislative fix at this time, but wanted to work with the technology companies to find solutions that will work for each individual company. However, you acknowledged that the Department was "not ruling out a legislative solution" should one prove necessary. I also asked whether there was a process in place or a target timeline within the Administration to find solutions, but I didn't get an answer to that question.

a. **Does the Department of Justice have any formal process or any timeline in place to work with technology companies to find solutions to the "Going Dark" problem? If so, please provide as much detail about that process or timeline as possible. If not, why does the Department not have such a process or timeline?**

b. **Given the testimony at the hearing that "Going Dark" is a significant problem and is only getting worse, is there a date certain by which, if a solution to the problem has not been reached through dialogue with the technology companies, the Department of Justice will come forward with a legislative proposal?**

Response: The Department of Justice continues to work with companies and industry groups to address these issues, and those efforts have intensified in the last few months. In fact, the United States Government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. The Administration is not seeking legislation at this time. The United States Government is seeking voluntary cooperation from U.S. companies on a case-by-case basis, in order to address incidents or cases of concern. We will continue to pursue this cooperation, but note that solutions to particular issues may vary based on the technology

involved, the responsiveness of the company, and other factors. For this reason, we do not have a deadline in mind for any particular action.

2. The "Data-in-Motion" Problem and the Wiretap Report

The Administrative Office of the United States Courts releases an annual "Wiretap Report," concerning intercepted communications pursuant to Title III of the Omnibus Crime Control and Safe Streets Act. The most recent Wiretap Report for 2014 showed that law enforcement confronted encryption in a very small fraction of wiretap applications and was unable to decipher encrypted communications in only a few of those cases. Some commentators, including Professor Swire at the hearing, have asserted that this report contradicts law enforcement's claim that it is "Going Dark" and instead proves that encryption is not harming its ability to investigate crime by intercepting "data-in-motion." Regardless, there is no doubt that Congress would benefit from concrete statistical information about the scope of the "Going Dark" problem and how it is affecting law enforcement.

a. Does the Wiretap Report provide helpful data for evaluating the "Going Dark" problem faced by law enforcement, at least in the "data-in-motion" context? Or, as you suggested in your testimony, does the Wiretap Report only reflect the number of applications that are sought and impacted by encryption, not the number of applications that are never sought because of encryption?

b. If the Wiretap Report is not a good benchmark for the "data-in-motion" problem, can the Department of Justice work to develop a better mechanism to keep track of the number of investigations that are negatively impacted by strong encryption and share that information with Congress so that Congress can better evaluate the issue?

Response: Encryption presents a significant and growing challenge for law enforcement in the context of "data in motion." Billons of communications occur each day over services that, because of encryption, lack a meaningful interception capability. Unfortunately, the Wiretap Report cannot present a complete or accurate picture of this challenge. Pursuant to 18 U.S.C. § 2519, the Department of Justice, State prosecutors, and judges provide information to the Administrative Office of the United States Courts for inclusion in the Wiretap Report. The Wiretap Report only reflects the number of criminal applications that are sought, and not the many instances in which an investigator is dissuaded from pursuing a court order by the knowledge that the information obtained will be encrypted and unreadable. That is, the Wiretap Report does not include statistics on cases in which the investigator does not pursue an interception order because the provider has asserted that an intercept solution does not exist. Obtaining a wiretap order in criminal investigations is extremely resource-intensive as it requires

a huge investment in agent and attorney time, and the review process is extensive. It is not prudent for agents and prosecutors to devote resources to this task if they know in advance that the targeted communications cannot be intercepted. The Wiretap Report, which applies solely to approved wiretaps, records only those extremely rare instances where agents and prosecutors obtain a wiretap order and are surprised when encryption prevents the court-ordered interception. It is also important to note that the Wiretap Report does not include data for wiretaps authorized as part of national security investigations.

Because it does not capture the effect of the Going Dark problem on the choice of investigative tools, the Report is of limited utility in quantifying the challenges posed by encryption. Accordingly, the statistics in the Wiretap Report are not a reliable measure of the scope of the Going Dark problem. The Department of Justice is exploring ways to more accurately measure the impact of encryption in the context of "data in motion," and we look forward to sharing the results with the Committee.

3. The "Data-at-Rest" Problem and the Impact of Encryption

Regarding the "data-at-rest" problem, District Attorney Vance stated in his written testimony to the Committee that "when smartphone encryption is fully deployed by Apple and Google, 71% of all mobile devices examined – at least by my Office's lab – may be outside the reach of a search warrant."

a. Does the Department of Justice have similar information regarding the potential impact of encryption on the "data-at-rest" problem?

Response: Please see the response to Chairman Grassley's question 2(a) to FBI Director Comey, *supra*.

b. For instance, does the Department of Justice have any similar statistical information on how often it has obtained a judicially authorized search warrant for the digital contents of a device but was nonetheless unable to execute the warrant due to encryption? Similarly, does the Department of Justice have any similar statistical information on how often it has obtained a judicially authorized search warrant to obtain the contents of an email account but was unable to execute the warrant due to encryption?

Response: Please see the response to Chairman Grassley's question 2(b) to FBI Director Comey, *supra*.

c. If the Department of Justice does not have such information, can it develop a mechanism to keep track of the number of investigations that are negatively impacted by smartphone encryption and share that information with Congress so that Congress can better evaluate the issue?

Response: Please see the response to Chairman Grassley's question 2(c) to FBI Director Comey, *supra*.

4. CALEA

In prior testimony before Congress, the Federal Bureau of Investigation suggested that the "data-in-motion" problem was associated with limitations on the enforceability and scope of the Communications Assistance for Law Enforcement Act (CALEA).

a. How much of the "data-in-motion" side of the problem is attributable to problems with the enforceability of CALEA – i.e., providers or services that are covered by CALEA but that do not or are unable to comply with CALEA? Alternatively, how much is attributable to problems with the scope of CALEA – i.e., providers or services that are not covered by CALEA, either by statute or by FCC regulation?

Response: Please see the response to Chairman Grassley's question 3(a) to FBI Director Comey, *supra*.

b. How many providers or services have refused to comply with court orders on the basis that they are not subject to CALEA? Please identify each instance and each provider or service that has refused to comply with a court order in this area.

Response: Please see the response to Chairman Grassley's question 3(a) to FBI Director Comey, *supra*.

5. Department of Justice's Discussions with Technology and Communication Companies

You testified that the Department of Justice is working with technology and communications companies to try to find solutions to the "Going Dark" problem.

a. Please provide as much information as possible about the Department of Justice's engagement with these companies, including the specific companies

that are part of the discussions, when the discussions on this topic began, and whether the discussions with each company remain ongoing.

b. Have any companies refused to productively engage with the Department of Justice on this issue? If so, please identify them.

c. Will you commit to providing the Committee with quarterly updates about the status of the Department's engagement with these companies to find solutions to this problem?

Response: The Department of Justice regularly works with companies in connection with the need for lawful access to customer data to protect public safety and national security. This often occurs in connection with specific court orders or search warrants, but also involves broader engagement about a company's technical capabilities concerning compliance with legal process. We use this broader engagement, which also extends to industry groups and organizations, to exchange information regarding Going Dark challenges and to hear the companies' perspectives. Most are willing to engage on the Going Dark problem, though some prefer that this engagement take place in one-on-one discussions regarding their capabilities. These discussions occur frequently with a variety of companies, groups, and organizations. We would welcome the opportunity to offer the Committee regular updates about our continuing efforts to attain individualized solutions.

6. Contempt as a Solution

Some critics of the "Going Dark" problem argue that law enforcement has other options available to them, such as the use of contempt to force a defendant to provide law enforcement with access to his or her encrypted information. Is this a viable option in most investigations? Why or why not?

Response: This is not a viable option in most investigations. Courts thus far have held that the compelled production of a password violates the defendant's Fifth Amendment privilege against self-incrimination in most circumstances. Moreover, even if courts were to hold otherwise on the Fifth Amendment question, many offenders would choose to accept a punishment for contempt rather than risk a lengthy sentence for the underlying crime. In addition, in some cases, especially those involving real-time interception pursuant to a court order, it is not feasible to compel an individual because doing so would alert them to the surveillance. And, finally, regardless of the legal landscape, compelling disclosure of passwords is not a useful solution in many national security surveillance contexts, such as those involving spies and terrorists.

QUESTION FROM SENATOR WHITEHOUSE TO
JAMES B. COMEY, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION:

1. During your testimony, you mentioned that there are companies that have the technical capability to comply with requests issued by law enforcement but have declined to do so. Please provide all available information about these declinations, including the name and address of the company and the type of request issued by law enforcement.

Response: In the current legal and technological environment, there are several circumstances in which companies may decline to comply with requests issued by law enforcement authorities. In some instances, a company may have the technical capability to comply but it declines to do so based on a legal argument that applies in that narrow case (these arguments may relate to jurisdiction, the form of the request, or other factors). As a separate matter, some companies may decide not to fully develop the capability to comply because there is no legal mandate to do so. Companies may also decide not to comply because they assert that doing so would cause reputational harm. *See, e.g.*, Response Brief of Apple, Inc., *In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued By this Court*, No. 15 MISC 1902 (JO) (E.D.N.Y. Oct. 19, 2015). Although the FBI does not retain information regarding these various circumstances, we would be pleased to provide anecdotal information to the Committee regarding our efforts and results in an appropriate setting.

QUESTION FROM SENATOR WHITEHOUSE TO
SALLY QUILLIAN YATES, DEPUTY ATTORNEY GENERAL:

2. Has the Department of Justice explored whether there is any potential civil liability for companies that choose to encrypt customer data in a manner that they cannot decrypt, even when presented with a valid search warrant? If the Department has not explored this issue, would it be willing to do so?

Response: The Department of Justice has not undertaken a detailed analysis of that issue, but we would be willing to work with you and your staff to understand the exact scope and contours of any such analysis.

Our efforts have focused on preventing the type of harm that might give rise to civil liability by ensuring that companies retain the ability to comply with lawful court orders. Indeed, many companies maintain that ability while simultaneously guarding individual security and privacy through the use of strong encryption. We look forward to working with the industry to find other ways to implement strong data protection while preserving the ability to protect public safety and national security.