House Judiciary Committee
Response to Questions for the Record from Chairman Goodlatte
Washington, D.C.

Cyrus R. Vance, Jr., District Attorney, New York County, New York

---

Question 1:

Now that the FBI has found a solution to unlocking the San Bernardino terrorist's iPhone, have you asked the FBI to share their solution with your office?

Response to Question 1:

Yes.

Question 2:

Are you aware whether the solution FBI has found would assist in your own investigations and backlog of phones to search?

Response to Question 2:

The lawful method employed by the FBI to open Syed Farook's iPhone reportedly works on only the particular model and operating system on that phone. Moreover, Apple could alter the operating system so that the FBI's solution would no longer work. Finally, tools of the kind used to open that phone cost far more than most local agencies can afford.

Most local police and prosecutors offices do not have in-house forensics labs. Many state and local law enforcement agencies would be required to send each device to an outside company for forensic analysis and decryption.

Question 3:

Are you also seeking outside assistance in unlocking the phones without Apple's help?

Response to Question 3:

Yes.

Question 4:

How many cases on average do you experience per year where encryption or locked phones prevent your office from accessing necessary investigative information that is likely to yield evidentiary value in solving a crime? What is your oldest case that is now being blocked due to an inability to access content on locked iPhones?

Response to Question 4:

We have been working on this issue since September of 2014 when Apple and Google adopted default device encryption for smartphones. We released a report on Smartphone Encryption and Public Safety in November of last year. As of that paper's release, we had 111 Apple devices that were completely inaccessible. The number of inaccessible phones has risen to approximately 250 devices, out of a total of 853 phones seized by my Office's Cyber Lab between October 2014 and April 2016. Note that these 250 devices are only those obtained by my Office's Cyber Lab in Manhattan; it does not include the number of inaccessible devices seized by the New York City Police Department, or by the District Attorney's Offices of the four other boroughs in New York City.

These 250 devices arise from a wide variety of cases, including murder, sex crimes, child abuse, and complex financial crimes.

Question 5:

What is the effect if Congress were to make a determination that under no circumstances can the government require access or even the mere option to use its own technology to decrypt devices that are previously secured with a passcode or encryption?

Response to Question 5:

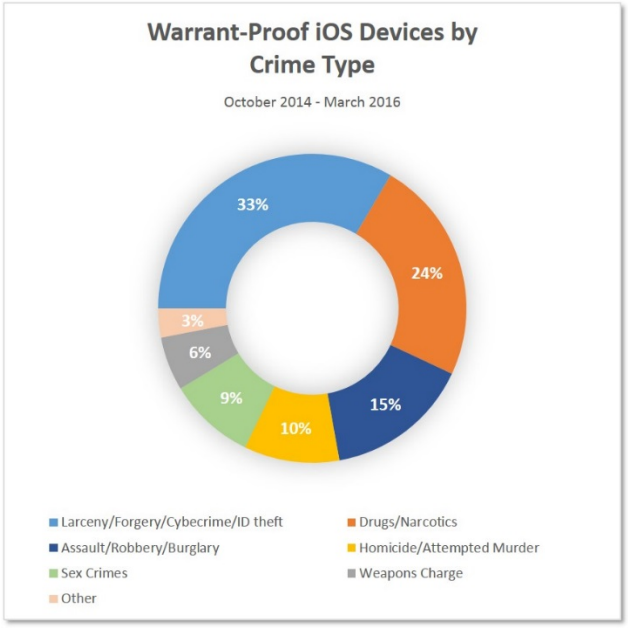
The impact would be felt largely at the state and local level, where 95 percent of criminal prosecutions are handled every year. Because many individuals – including criminals – now live a large part of their lives on smartphones, much critical evidence of crime resides on smartphones, including messages, photos, videos, calendars, and address books. Without smartphone evidence, certain cases will have to be dismissed because prosecutors will not be able to proceed to trial due to a lack of sufficient evidence. In some cases, victims will be waiting for a measure of closure that may never come, and defendants will be free to reoffend. In other cases, prosecutors may be able to obtain a plea to a lesser charge than the top count charged, because without the smartphone evidence, prosecutors will not be able to make the case for the top charge. It is not our position that default device encryption makes it impossible to bring *any* charges against *any* defendants. It does pose a substantial impediment to investigating thoroughly and completely. Plainly said, it affects the process of investigation, exoneration, and prosecution.

Question 6:

In your discussions with other DAs around the country concerning their challenges faced by encryption, have you noticed whether there is any particular crime that seems to be hindered more by encryption than others? For instance, are you noticing gangs using encryption over those exploiting children, or vice-versa?

Response to Question 6:

Affected cases run the gamut from violent crimes such as homicide, to cybercrime and identity theft. This is a breakdown of crime categories corresponding to inaccessible Apple devices received by the Manhattan District Attorney's Office's Cyber Lab from October 2014 to March 2016.



In a series of op-eds and in congressional testimony, we have told a number of stories from across the country – like that of Brittney Mills in Baton Rouge, and Ray Owens in Evanston – whose killers remain on the loose.

Question 7:

Apple has argued publicly that it does not have capability to assist the government with iOS 8 encryption. However, in the Eastern District of New York, Apple is currently contesting an order issued under the "All Writs Act" to assist law enforcement with a cell phone that has iOS 7 encryption, which Apple has the capability to do. If Apple is no longer willing to assist law enforcement when it has the capability to do so, how cooperative can they possibly be when discussing iOS 8, iOS 9, or future operating systems?

Response to Question 7:

This is why our office supports legislative action to require their cooperation when compelled by a court to do so.

Question 8:

You have pointed out that Apple and Google software runs nearly 97 percent of the world's smartphones. These are American-based companies. Have you encountered phones with software other than that of Apple and Google that happened to be encrypted, and if so, do you have any recourse to unlocking or decrypting those phones?

Response to Question 8:

No, all phones in cases currently being prosecuted by my Office are running on either the iOS or Android operating systems.

Question 9:

Are you participating in the FBI-run National Domestic Communications Assistance Center (NDCAC)? Is the NDCAC reviewing any technological solutions to assist law enforcement in gaining access to encrypted communications?

Response to Question 9:

Yes to both questions.

Question 10:

Is it realistic for state and locals to stay in front of technological solutions developed by companies such as Apple in order to remain able to lawfully access necessary communications?

Response to Question 10:

No, we simply do not have the resources. There is a deeply worrisome, inversely proportional relationship: The volume of encrypted devices are at the highest level for state and local enforcement agencies, where resources are at the lowest level.

Question 11:

Do you ever obtain technical assistance from the FBI in accessing communications on phones or computers that you have seized? Are there ever any legal or resource restrictions in preventing you from receiving the necessary technical assistance from

the FBI, particularly any that Congress might be able to solve with legislation or additional funding for the Bureau?

Response to Question 11:

The Manhattan District Attorney's Office has its own High Technical Assistance Unit and performs a wide variety of forensics across multiple device types for our investigations and cases. We have received and continue to receive technical assistance from the Federal Bureau of Investigation. We are not aware of any restrictions imposed by New York law that would prevent the FBI from sharing data with us, although there may be such restrictions imposed by federal law, and the costs of such sharing may, depending on the circumstances, be substantial. Furthermore, if the FBI were to provide technical assistance to us, and we were to rely on that assistance in a proceeding, FBI agents might be called upon to testify about the techniques or methods. This might be costly to the FBI and law enforcement generally.

Question 12:

In your law enforcement career, how would you rank this issue of encryption in terms of complicating investigations?

Response to Question 12:

Apple's introduction of a product that is beyond the reach of a search warrant into the stream of commerce – and marketing that product as warrant-proof – is entirely unprecedented. One of the largest companies in the world intentionally and explicitly frustrating its own ability to comply with court orders is entirely unprecedented.

Question 13:

What are some of the solutions that you are proposing, and do you foresee challenges in implementing them?

Response to Question 13:

We believe federal legislation is the only viable solution. State and local law enforcement does not have the resources of the FBI, and cannot afford to litigate these case by case, and rely on expensive lawful hacking solutions.

My Office — in consultation with cryptologists, technologists and law enforcement partners — has proposed a solution that we believe is both technologically and politically feasible: Keep the operating systems of smartphones encrypted, but still answerable to locally issued search warrants – just as they were until very recently. This can be achieved by a federal statute providing that any smartphone made or sold in the United States must be able to be unlocked — not by the government, but by the designer of the phone's operating system — when the company is served with a valid search warrant.

Our solution, as set forth in our November 2015 Report, is that these companies make their smartphones amenable to search warrants. We want Apple to offer the same strong encryption that it employed without any documented security problems before iOS 8. Previous mobile operating systems allowed the company to access data on a seized device with a valid court order. Apple has never explained why the prior systems lacked security or were vulnerable to hackers, and thus, needed to be changed.

Question 14:

When considering strong encryption without a "key" versus strong encryption with a "key," is it really an either/or proposition?

Response to Question 14:

Neither our proposed solution, nor any pending legislation we support, proposes a government-held key.

Question 15:

Director Comey has said that the FBI is engaging the private sector in discussions about how to best deal with the "going dark" problem. Are you having similar discussions with tech companies? How are those discussions going? Which major service providers are constructively working with you on this issue? Which ones are not?

Response to Question 15:

Neither our Office, nor any state or local law enforcement agency of which we are aware, received any prior warning about Apple's policy change. We read it on the company's website, which stated: "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."

On March 19, 2015, I, along with two members of my Office, two representatives from the United States Secret Service, and two representatives from the Alabama Office of Prosecution Services, participated in separate meetings with senior Apple and Google executives at their respective headquarters in California to discuss this more.

On March 31, 2015, and April 1, 2015, I sent letters to Apple and Google, respectively, setting forth questions that arose from our meetings with them. I have attached a copy of both my letters. (Copies of the letters were also attached as exhibits to my written testimony before your Committee.) I had hoped that the letters would foster a dialogue, but neither company has responded.

Question 16:

Are you aware of providers acquiescing to requests for access from the governments of other countries as a condition of doing business there?

Response to Question 16:

No. However, Apple's Reports on Government Information Requests - which are released every six months – show that it has complied with orders from foreign governments and law enforcement agencies.

It is our understanding that if a foreign nation's government wanted information from an American company, it also would have to go through lawful processes in the U.S., either pursuant to a Mutual Legal Assistance Treaty or a letter rogatory. If the foreign government used the MLAT process, the executive branch of the federal government would decide whether, in its discretion, the foreign government's request was proper. If the foreign government used a letter rogatory, a federal court would make that determination. In either case, the request could be refused if the information was sought for use in a proceeding that would violate human rights.

Question 17:

Don't your investigators use encryption? How do you reconcile the need for your investigators to have access to the strongest of encryption with the need for the general public to have access to the same strong encryption?

Response to Question 17:

We want Apple to offer the same strong encryption that it employed without any documented security problems before iOS 8. Previous mobile operating systems allowed the company to access data on a seized device with a valid court order. Apple has never explained why the prior systems lacked security or were vulnerable to hackers, and thus, needed to be changed.

Question 18:

Under what circumstances can the government compel a person to provide access to their cell phone? Is there a difference between whether a person uses a passcode (such as a four digit number) or biometrics (such as a fingerprint) to "lock" their cell phone?

Response to Question 18:

Case law holds almost universally that a defendant cannot be compelled (by, *e.g.*, a grand jury subpoena or order of the court) to provide the government with her or his passcode,

because such compulsion would violate the defendant's Fifth Amendment right against self-incrimination.[1] There are two potential exceptions to this rule.

First, it is an open question whether, instead of being compelled to provide the government with a passcode, the defendant might be compelled to unlock her or his phone *using* the passcode. There have been no cases considering this precise question, and although a court might conclude that it is no different from the situation in which a defendant is compelled to provide the government with the passcode, it might also determine that the situations are somewhat different.[2]

Second, if the existence of evidence on the phone is a foregone conclusion, then the defendant may have no Fifth Amendment privilege with respect to the contents of the phone, and thus may be compelled to provide the government with the passcode.[3] It would be difficult in most circumstances, however, for the government to establish with the requisite degree of certainty the existence of evidence in a phone that would clear the "foregone conclusion" hurdle.[4]

In any event, even if the government could lawfully compel a defendant to disclose her or his passcode – or to open her or his phone using the passcode – there is a substantial

---

[1] The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const., amend. V. The amendment's prohibition against self-incrimination has been "incorporated" so that it applies to state criminal proceedings, as well as federal. *See Malloy v. Hogan*, 378 U.S. 1, 6 (1964); *Griffin v. California*, 380 U.S. 609, 615 (1965). The cases addressing the question whether a defendant may be compelled to provide her or his passcode to the government, and holding that such compulsion would violate the Fifth Amendment include: *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *U.S. v. Kirschner*, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010); *SEC v. Huang*, No. 15-269 (E.D.Pa.) (Sept. 23, 2015) (slip op. at 4-5); *Commonwealth v. Baust*, 89 Va. Cir. 267, 270-71 (Circuit Ct. of the City of Virginia Beach) (Oct. 28, 2014).

[2] Professor Orin Kerr has suggested that because it is (or may, in many cases be) a "foregone conclusion" that a person knows the passcode to her or his own smartphone, it would not violate the Fifth Amendment to compel a phone owner to use her or his passcode to open the phone. *See* Kerr, "Apple's Dangerous Game," *The Washington Post*, September 19, 2014 (https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/) (citing *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009)). This may be correct, although it has not been tested in any case. *Boucher* suggests that if the *content* of the smart phone is known (a "foregone conclusion"), then requiring the passcode may not implicate the Fifth Amendment; it does not say that a person's knowledge of her or his passcode would satisfy the foregone conclusion requirement.

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

[4] Professor Kerr has also explored the argument that compelling a person to provide her or his password may not violate the Fifth Amendment because the provision of the password may not be incriminating, as that term is by the Supreme Court in cases such as *Hoffman v. U.S.*, 341 U.S. 479 (1951), and *Fischer v. U.S.*, 425 U.S. 391 (1976). *See* Kerr, "A Revised Approach to the Fifth Amendment and Obtaining Passcodes," *The Washington Post*, September 25, 2015 (https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/25/a-revised-approach-to-the-fifth-amendment-and-obtaining-passcodes/). Professor Kerr's analysis may be right, although it does not appear that any courts have adopted it, and therefore there are still questions about the application of the Fifth Amendment to efforts to compel persons to provide their passcodes to the government.

likelihood that any defendant who faces potentially serious criminal charges would simply refuse to comply with the subpoena or order, and go into contempt.[5]

In sum: In almost all cases, it will be legally impossible to compel a defendant to provide his or her passcode or to use the passcode to open her or his phone. In those few cases in which it might be legally possible to compel the defendant to provide the information, it would be impossible as a practical matter to compel a recalcitrant defendant facing serious charges to do so.

Question 19:

When the government takes possession of an iPhone as evidence, what can the government do to get into the phone for evidentiary purposes? What are the limitations? What about an Android phone?

Response to Question 19:

The applicable law enforcement agency may search the device pursuant to a judicially-authorized warrant after establishing probable cause, and subject to the encryption on the device. This applies to all types of devices.

Question 20:

After a serious criminal incident, how does law enforcement access a device (or app) to determine a suspect's contacts with other suspected criminals or co-conspirators? Or determine if another crime is imminent? What privacy or security interests exist in that situation?

Response to Question 20:

As in response to Question 19, in order to examine such evidence, the applicable law enforcement agency may search the device pursuant to a judicially-authorized warrant after establishing probable cause, and subject to the encryption on the device. This probable cause standard has long been recognized by our courts and legislature as the striking the correct balance between privacy and security.

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