Written Testimony of New York County District Attorney Cyrus R. Vance, Jr.
Before the United States Senate Committee on the Judiciary

"Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy"

Washington, D.C.
July 8, 2015

Good morning Chairman Grassley, Ranking Member Leahy, and Members of the Senate Judiciary Committee. Thank you for your leadership on these issues, and for the opportunity to testify today.

Encryption and government access to data stored on electronic devices have largely been discussed as a federal and national security issue. In truth, the implications of this discussion are equally, or even more importantly, of significant concern to state and local law enforcement. That is because more than 90 percent of all criminal cases filed annually are filed and adjudicated in state courts around the country.[1]

To use the New York County District Attorney's Office as a point of reference, my Office handles more than 100,000 criminal cases each year, which is more than all of the cases handled by the Department of Justice nationwide. And the range of those cases is broad – from murder, rape, and robbery, to identity theft, financial fraud, and terrorism.

[1] *See* http://www.ncsc.org/Sitecore/Content/Microsites/PopUp/Home/CSP/CSP_Intro; http://www.bjs.gov/content/pub/pdf/fjs12st.pdf.

People live their lives today on their smartphones, which they use for, among others things, emailing, texting, taking pictures, posting pictures, shopping, conducting business, and searching the web. To investigate these 100,000 cases without smartphone data is to fight crime with one hand tied behind our backs.

Therefore, I want to focus my testimony on an issue deeply troubling for law enforcement at all levels: the encryption of smartphone data by Apple and Google. I believe that by having an open discussion among lawmakers, law enforcement, and the private sector, we can reach a solution that strikes the right balance between privacy and public safety.

I. The Use of Smartphone Evidence Pursuant to Judicial Warrants

As you know, the Fourth Amendment of the United States Constitution authorizes reasonable searches and seizures, providing law enforcement agencies access to places where criminals hide evidence of their crimes – from car trunks, to storage facilities, to computers, mobile devices, and digital networks. In order to safeguard Fourth Amendment rights, these searches are conducted pursuant to judicial warrants, issued upon a neutral judge's finding of probable cause. The probable cause standard represents a balance between privacy and public safety carefully calibrated by centuries of jurisprudence, and it guides individuals and companies in developing their expectations of privacy.

Through this judicial process, my Office obtains smartphone evidence to support all types of cases – homicides, sex crimes, child abuse, fraud, assaults, robberies, cybercrime, and identity theft. Many perpetrators, particularly those who commit sexual offenses, take photos and videos of their acts, and store them on computers and smartphones.

Between October 2014 and June 2015, 35 percent of the data extracted from all phones by my Office was collected from Apple devices; 36 percent was collected from Android devices.[2] That means that when smartphone encryption is fully deployed by Apple and Google, 71 percent of all mobile devices examined—at least by my Office's lab—may be outside the reach of a search warrant.

I want to emphasize I am testifying from a state and local perspective. I am not advocating bulk data collection or unauthorized surveillance. Instead, I am concerned about protecting local law enforcement's ability to conduct targeted requests for information, scrutinized by an impartial judge for his or her evaluation as to whether probable cause has been established. Importantly, and *by Apple's own admission*, governmental request for information have affected only .00571 percent of Apple's customers.[3]

II. Apple and Google's New Encryption[4] Policies

Last fall, Apple and Google, whose operating systems run 96 percent of smartphones worldwide, announced with some fanfare, but without notice to my Office or other law enforcement offices I have spoken to, that they had engineered their new mobile operating systems such that they can no longer assist law enforcement with search warrants written for passcode-protected smartphones. According to Apple's website:

> On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. . . . Apple *will not perform iOS data*

[2] The remaining 29 percent of data was extracted from other types of phones, such as flip phones and burner phones.

[3] https://www.apple.com/privacy/government-information-requests/.

[4] Data transmitted between phones, computers, and other digital devices can be encrypted (i) while in transit between those devices and (ii) on the devices themselves. This latter type of encryption is referred to as full-disc encryption, and that is the type of encryption that I am concerned with here.

extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess. [Emphasis added.][5]

Apple's announcement led to an immediate response by law enforcement officials who pointed out that allowing a phone or tablet to be locked such that it would be beyond the reach of lawful searches and seizures was unprecedented and posed a threat to law enforcement efforts – in effect, a boon to criminals. Unless law enforcement officials can obtain the passcode from the user, which will be difficult or impossible in many cases, or can use "brute force" to obtain the passcode (again, difficult or impossible, and attempts to do this would likely lead to the destruction of evidence on the iPhone), the search warrant would be of no consequence, because no one will be able to unlock the phone, notwithstanding the court order.

Law enforcement's warnings are hardly idle. Recently, a father of six was murdered in Evanston, Illinois. City of Evanston Police believe that prior to his murder, the victim was robbed of a large sum of money. There were no eyewitnesses to or surveillance footage of the killing. Found alongside the body of the deceased were an iPhone 6 and a Samsung Galaxy S6 Edge running Google Android. Cook County prosecutors served Apple and Google with judicial warrants to unlock the phones, believing that relevant evidence might be stored on them. Apple and Google replied, in substance, that they could not, because they did not know the user's passcode. Information that might be crucial to solving the murder, therefore, had effectively died with the victim. His homicide remains unsolved. His killer remains at large.

It is not hyperbole to say that beginning in September 2014, Americans conceded a measure of their protection against everyday crimes to Apple and Google's new encryption policies. Yet, I

---

[5] https://www.apple.com/privacy/government-information-requests/.

would note that, before the changes, neither company, to our knowledge, ever suggested that their encryption keys, held by the companies, were vulnerable to hacking or theft.

Fully one-quarter of our felony cases now involve cybercrime or identity theft, so I am keenly aware of the dangers and impact of these crimes on our community (which happens to be situated in a world financial center and is the number one target for terrorism in the world). Because of this, my Office has invested heavily in becoming highly proficient and active in the prosecution of these crimes, and in the promotion of best cybersecurity practices for New York consumers and companies. From my vantage point, and in my opinion, for reasons set forth later in my testimony, Apple and Google's new encryption policies seem to increase protection for consumers from hackers only minimally, if at all. But those policies create serious new risks for my constituents and the millions of visitors and workers passing through Manhattan every day.

III. The Problem Created by Apple and Google's New Encryption Policy

Some commentators have argued that the effective unsearchability of smartphones will not be significant because law enforcement has other avenues for investigation.[6] These arguments are flawed, for the reasons set forth below. While Apple is not the only company to have announced a similar program, for ease of presentation, and because Apple has been the most vocal company on the relevant issues, I address here only Apple's program, devices, and statements. I believe that the arguments and reasoning here would apply as well to Google's program and any similar program.

A. The Search of an iCloud Account is Not a Substitute for the Search of an iPhone

Apple's new encryption policy currently does not affect law enforcement officials' ability to obtain user data from an iCloud account. Law enforcement officials who obtain a search warrant

[6] *See, e.g.*, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html?_r=0.

for a person's iCloud account can serve that warrant on Apple, and thus obtain the contents of the account, regardless of whether the person's iPhone uses iOS 8.

But searching a person's iCloud account is not the same as searching the person's iDevice.[7] The ability of law enforcement officials to obtain a search warrant for an iCloud account does not mean that those officials will obtain the same content as they would if they could search the user's device. In many cases, law enforcement officials cannot obtain the entirety of an iPhone's data by obtaining the contents of the associated iCloud account.

First, and most fundamentally, users of iDevices are not required to set up iCloud accounts or to back-up to iCloud accounts. Therefore, not all users of iDevices will have data stored to iCloud. It is clear that even minimally sophisticated wrongdoers who use their iDevices to perpetrate crimes will take the relatively simple steps necessary to avoid backing up those devices to iCloud.

Second, even when a user chooses to back up his or her data to iCloud routinely, some data may not be backed up and would, therefore, be unattainable through a search warrant for an iCloud account. Data that is saved on an iPhone will not be backed up to the cloud until the iPhone is connected to WiFi. So, if evidence is stored on an iPhone when the phone is disconnected from Wi-Fi, and the iPhone is recovered by law enforcement officials before it is reconnected to Wi-Fi, then the evidence would exist only on the iPhone itself.

iPhone users are given only five gigabytes of free storage space on iCloud, whereas iPhone 6s come with either 16, 64, or 128 gigabytes of storage space on the device itself. Thus, unless a user pays for additional iCloud storage space, the vast majority of their storage space will be on the iPhone itself.

---

[7] Mobile devices manufactured by Apple are called iDevices, and include phones (iPhones), tablets (iPads), and MP3 players that play audio and video files (iPods).

Third, it may be possible to recover at least some deleted data from an iDevice. Once data has been deleted from an iCloud account, however, it is not recoverable.[8] Thus, the iPhone is the only route to evidence that has been deleted – which may, of course, be among the most probative evidence.

Fourth, it will often be more difficult for a prosecutor to prove who uses the data on a particular iCloud account than it would be to prove who owns a particular iDevice. iDevices are often recovered from a person, which supports the inference that the person controls the device. To establish the person's ownership of the device, a prosecutor may simply have to call one witness – the officer who recovered the device. By contrast, the identity of the user of an iCloud account may be more difficult to establish. A prosecutor may need to present testimony or records from Apple relating to the subscriber information, IP login history,[9] and/or content of the account, testimony or records from internet service providers regarding the subscriber information of certain IP addresses, and/or testimony of forensic analysts, among other witnesses.

B. The Difficulty of Getting Passcodes from Defendants

In many cases, the iPhone that may contain evidence about a criminal case belongs to the defendant, and thus it is her or his passcode that prevents the government from gathering the

[8] Apple Legal Process Guidelines, https://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf, page 9.

[9] An IP address is a series of numbers separated by three periods (i.e. 192.168.10.12) that uniquely identifies a particular connection to the internet at a specific date and time. Apple maintains a record of the IP addresses used to log in to iCloud accounts within a recent time period. Pursuant to appropriate legal process, law enforcement officials can obtain the IP login history for a particular iCloud account, that is, a list of IP addresses that the user of the iCloud account used to connect to the internet prior to signing in to his or her iCloud account, as well as the dates and times of those log-ins. After law enforcement obtains this information from Apple, law enforcement officials can send a subpoena to the internet service provider that owns each IP address listed requesting the subscriber information for each IP address. Examples of internet service providers include Time Warner Cable or Comcast. The subscriber information for the IP address will be the name and contact information provided by the user of the particular internet service account when they signed up for that account.

evidence. In most cases, it will be almost impossible to compel a defendant to provide her or his passcode to the government.

Case law holds almost universally that a defendant cannot be compelled (by, for example, 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.[10] 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 iPhone *using* the passcode. There have been no cases of which we are aware that consider 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 password, it might also determine that the situations are somewhat different.[11]

Second, if the existence of particular evidence on the iPhone is a foregone conclusion, then the defendant may have no Fifth Amendment privilege with respect to those contents of the iPhone, and thus may be compelled to provide the government with the passcode.[12] It would be very

---

[10] 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 password 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); *United States v. Kirschner*, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010).

[11] Professor Oren Kerr has suggested that because it is (or may, in many cases be) a "foregone conclusion" that a person knows the password to her or his own smartphone, it would not violate the Fifth Amendment to compel a phone owner to use her or his password to open the phone. *See* Kerr, Apple's Dangerous Game, on *The Volokh Conspiracy* (September 19, 2014) (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 password may not implicate the Fifth Amendment; it does not say that a person's knowledge of her or his password would satisfy the foregone conclusion requirement.)

[12] *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 (D. Vt. Feb. 19, 2009) at *3; *In re Fricosu*, 841 F. Supp.2d 1232, 1237 (D. Colo. 2012).

difficult in most circumstances, however, for the government to establish with the requisite degree of certainty the existence of evidence in the contents of an iPhone that would clear the "foregone conclusion" hurdle.

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 likelihood that any defendant who faces potentially serious criminal charges would simply refuse to comply with the subpoena or order, and go into contempt.[13]

The consequence of the foregoing is that 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 iPhone, and that, 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. And, of course, whatever powers law enforcement might have to compel a defendant to cooperate in opening her or his phone, those powers are irrelevant to the situation in which the phone that law enforcement needs to open belongs to an unavailable victim (for example, the deceased, in a murder case) or to a witness or potential defendant who fled the scene of the crime.

IV. Apple's Stated Reasons for Its New Encryption Policy

Apple, to our knowledge, has given four principal justifications for its new policy.

First, it has suggested that the new policy is a response to public concerns expressed in light of the revelations by Edward Snowden about data collection by the National Security Agency.[14]

---

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

[14] http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html?_r=0.

Second, Apple has suggested that unless it makes its iDevices impregnable to lawful governmental access, Apple will lose customers, who will seek to purchase substitute, impregnable devices.[15]

Third, Apple has suggested that if it were to build its devices such that it could respond to lawful governmental requests for information in them, then the iDevices would be less secure than if Apple built them (as it has) to be impregnable to such requests.[16]

Fourth, Apple has also suggested that if it were to build its devices such that it could respond to lawful domestic governmental requests for information in them, then foreign governments would also request access to the information contained in the devices, or hack into the devices to gain access;[17] if those government were repressive, commentators have suggested, then it would, in effect, be helping repressive governments to limit their citizens' liberty.

Each of these proposed justifications will be addressed in turn.

A. American Customer Privacy Concerns Based on NSA's Actions

Apple's encryption efforts – and, more particularly, its announcement of those efforts – appear to be partially in response to concerns expressed by the public in the wake of revelations about incursions of privacy by the NSA, many of which were brought to light by Edward Snowden and others working with him.[18] The encryption efforts are not a reasonable response to the Snowden-NSA issue for at least two reasons.

---

15 Id.

16 http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.a3spud:Ugxb.

17 http://www.fastcompany.com/3046469/fast-feed/major-tech-companies-but-not-amazon-sign-letter-to-obama-against-security-backdoor; http://www.pcworld.com/article/2933397/tech-industry-redoubles-efforts-to-fight-us-govt-encryption-backdoors.html.

18 http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2; http://www.bbc.com/news/world-us-canada-23123964.

First, the effect of Apple's encryption is that it prevents (i) the necessity of Apple responding to lawful government requests and (ii) the government from examining the contents of iDevices, even when an independent judge has authorized such disclosure by issuing a search warrant. Of course, a search warrant cannot be issued absent a showing of probable cause to believe that a crime has been committed and that evidence or proceeds of the crime might be found on the iDevice to be searched.[19]

The warrant requirement has been described by the Supreme Court as "[t]he bulwark of Fourth Amendment protection,"[20] and there is no reason to believe that it cannot continue to serve in that role, whether the object to be searched is an iPhone or a home. In fact, what makes Apple's proposal remarkable is that it would provide greater protection to one's iPhone than one has in one's home, which, of course, has always been afforded the highest level of privacy protection.[21] Every home can be entered with a search warrant. I cannot think of another device that has been knowingly designed in a way to prevent *lawful* government inspection. Thus, even if Apple's new encryption policy would have prevented the NSA's actions, or will be able to prevent similar conduct, it comes at a very high and unjustified cost.

Second, Apple's new encryption policy would not have prevented the NSA's gathering of data, which, at least according to press coverage, was not sanctioned by a court or covered by a

---

[19] *See* U.S. Const., amend. IV (". . . . no Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (defining probable cause as "a fair probability that contraband or evidence of a crime will be found in a particular place").

[20] *Franks v. Delaware*, 438 U.S. 154, 164 (1978). *See also, e.g., Gonzales v. Beto*, 425 F.2d 963, 967 (5th Cir. 1970) ("The requirement of a search warrant is unquestionably a strong bulwark against the evils at which the fourth amendment is directed.").

[21] *See* U.S. Const., amend. IV ("The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated . . ."); *Minnesota v. Carter*, 525 U.S. 83, 94 (1998) ("The people's protection against unreasonable search and seizure in their "houses" was drawn from the English common-law maxim, "A man's home is his castle.") (Scalia, J., concurring).

search warrant.[22] That press coverage indicates that the NSA collected phone call data (including numbers called and the duration of phone calls), and the content of at least some phone conversations, often involving people for whom there was no reasonable suspicion of criminal activity, without judicial approval.[23] Of course, that is nothing like what we are suggesting, and, in any event, the encryption of iDevices would not have prevented the mass collection of phone call data, which is obtained from phone service providers rather than from phones themselves. And default full-disc encryption would not have prevented the NSA from intercepting communications in transit.

B. Security Concerns if Apple Can Decrypt

Apple has asserted that full-disc encryption maximizes the security of their users' devices and data. One should question that assertion for several reasons.

First, even before Apple enacted its new policy, a person who somehow obtained Apple's encryption key would still need the iPhone itself to obtain information on the device. It is highly unlikely that someone who snatches an iPhone from a subway commuter would also be a master hacker capable of breaching Apple's own security systems to obtain the encryption key. As best I can tell, Apple and Google's new encryption policies prevent lawful access by state and local law enforcement, and do nothing to address serious challenges like institutional data breaches or invasion by malware.

Second, if a user's phone were to be stolen, the user could use the Find My iPhone app in order to wipe the phone's data and prevent the thief from accessing that data. Users who have an

---

[22] I am not opining on the legality of the NSA's activity, but merely relying on the news coverage about that activity. *See, e.g.*, http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/07/second-circuit-rules-mostly-symbolically-that-current-text-of-section-215-doesnt-authorize-bulk-surveillance/; http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?_r=0**;** *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015).

[23] *See, e.g.*, ZDNET, NSA Planned Google Play Hack to Target Android Smartphones, May 21, 2015.

iCloud account can use the Find My iPhone app remotely to lock their phones or erase their data if their phones are lost or stolen. This app can effectively prevent thief-hackers from obtaining a phone's data.[24]

Third, according to Apple, most data stored on the iCloud is encrypted.[25] As noted above, law enforcement officials are able to obtain some iCloud data through the service of a search warrant on Apple. The fair inference is that Apple retains the ability to decrypt this iCloud data. But if Apple's ability to decrypt data on the iCloud does not render that data insecure – and Apple touts the security of its iCloud data[26] – then presumably neither would Apple's retaining the ability to decrypt data on an iPhone.

C. Concern About Foreign Governments' Access to Customer Information

Apple has suggested that if it maintains an encryption key to iOS 8, then repressive governments would seek access to information contained on devices, including those belonging to dissidents. If Apple were to comply, this would impede those dissidents' civil liberties. This contradicts commentators' arguments, referenced above, that iOS 8 will not be a significant burden on law enforcement, which can still request data from a user's iCloud account. Apple cannot have it both ways: Either iOS 8 does deter investigations or it does not.

But even more fundamentally, Apple's desire not to cooperate with requests from repressive governments does not justify its refusal to cooperate with *bona fide* requests from local law enforcement, approved by independent state or federal courts, in the United States. As I said before, the warrant requirement of the United States Constitution has been the fundamental

---

24 A similar app is also available for Apple tablets and computers.

25 https://support.apple.com/en-us/HT202303.

26 *See, e.g.*, id.

protection for people's privacy and liberty in this country. It can and should apply to iOS 8, as it does to any other home or device.

V. The Cost of Evidence Made Inaccessible Through Apple's Encryption

Although encryption has been often discussed in the context of international terrorism, the NSA, and the CIA, the greatest cost of these new encryption policies may well be borne by local law enforcement. Smartphones are ubiquitous, and there is almost no kind of case in which prosecutors have not used evidence from smartphones. My Office (and, I expect, every other local prosecutor's office) has used evidence from cellphones in homicides, rape cases, human trafficking, assaults, domestic violence cases, narcotics cases, kidnappings, larcenies, frauds, identity theft, cybercrime, and robberies. Indeed, it is the rare case in which information from a smartphone is *not* useful. The following list of recent cases is representative:

- **Homicide:** *People v. Hayes*, Indictment Number 4451/12: The victim was filming a video using his iPhone when he was shot and killed by the defendant. The video captured the shooting. Because the iPhone was not locked, the video was recovered and admitted into evidence at trial. The video corroborated eyewitness testimony. The defendant was convicted of murder and sentenced to 35 years to life.
- **Sex Trafficking:** *People v. Brown*, Indictment Numbers 865/12, 3908/12, and 3338/13: The defendant directed a sex trafficking operation involving at least four women, using physical violence, threats of force, and psychological manipulation to coerce the women to engage in prostitution. Evidence recovered from electronic devices lawfully seized from the defendant's home proved crucial to his conviction at trial. In particular, the defendant's cellular phones contained photographs showing him posing his victims for online prostitution advertisements, and showing that he had "branded" multiple women, with his

nickname tattooed onto their bodies; text messages between him and several victims confirmed that he had engaged in acts of violence against the testifying witness and others. The defendant was convicted of multiple counts of sex trafficking and promoting prostitution and was sentenced to 10-20 years in prison.

- **Cybercrime and Identity Theft:** *People v. Jacas et al.,* Indictment Number 42/12 and *People v. Brahms et al.*, Indictment Number 5151/11: This case involved the successful prosecution of a 29-member identity theft ring, which was able to be investigated and prosecuted, in large part, because of evidence obtained early in the investigation from an iPhone, pursuant to a search warrant. An iPhone was recovered from a waiter who was arrested for stealing more than 20 customers' credit card numbers by surreptitiously swiping those credit cards through a card reader that stored the credit card number and other data. When the phone was lawfully searched, law enforcement officials discovered text messages between members of the group regarding the ring's crimes. Investigators were able to obtain an eavesdropping warrant, and ultimately arrested 29 people, including employees of high-end restaurants who stole credit card numbers, shoppers who made purchases using counterfeit credit cards containing the stolen credit card numbers, and managers who oversaw the operation. The group compromised over 100 American Express credit card numbers and stole property worth over $1,000,000. All of the defendants pleaded guilty, and more than $1,000,000 in cash and merchandise were seized and forfeited.
- **Sex Offenses:** *United States v. Juarez*, Case No. 12-CR-59: The defendant was arrested for unlawful surveillance by an NYPD officer after the officer observed the defendant using a cell phone to film up women's skirts. My Office obtained a search warrant for the phone.

During the subsequent search of the phone's micro SD card, forensic analysts discovered a series of images, taken by the defendant, showing a seven-year-old girl lying down on a bed and an adult man pushing aside her underwear, revealing her genitals. The case was referred to the United States Attorney's Office for the Eastern District of New York, which charged the defendant with producing child pornography.

- **Physical and Sexual Abuse of a Child:** *U.S. v. Patricia and Matthew Ayers*, Case No. 5:14 CR 0117 LSC SGC: In case after case, law enforcement has been able to discover and prosecute child abuse by using video or photographic evidence taken by the abuser. This case is illustrative: From 2010 to 2013, the defendants abused and exploited a young child in their care who, during that period, was six to nine years old. The couple took photographs of the child in lewd poses, as well as of each other engaged in sexual acts with the child. The defendants recorded the abuse with their smartphones and downloaded the images to a computer. In at least one instance, one of the defendants transmitted images to another individual, indicating that she would travel interstate with the child to the individual's home so the individual could also have sexual relations with the child. The federal judge overseeing the case described it as the worst case he has personally dealt with, including murders, in his 16 years on the bench. The defendants were ultimately convicted of producing child pornography, in violation of 18 U.S.C. § 2251(a), and were sentenced to 1,590 and 750 years, respectively, in federal prison.

There are many other cases—almost too many to count—that I might have selected, but the point is clear: We would risk losing crucial evidence in all of these cases if the contents of passcode-protected smartphones were unavailable to us, even with a warrant.

The enormity of the loss is fully appreciated by wrongdoers who use smartphones. Recently, a defendant in a serious felony case told another individual on recorded jailhouse call that "Apple and Google came out with these softwares that can no longer be encrypted [sic: *de*crypted] by the police. . . . If our phones is running on the i0[S]8 software, they can't open my phone. That might be another gift from God."

This defendant's appreciation of the safety that the iOS 8 operating system afforded him, is surely shared by criminal defendants in every jurisdiction in America charged with all manner of crimes, including rape, kidnapping, robbery, promotion of child pornography, larceny, and presumably by those interested in committing acts of terrorism. Criminal defendants across the nation are the principal beneficiaries of iOS 8, and the safety of all American communities is imperiled by it.

VI. Proposed Solution: Return to a Balanced Approach – Requiring Phones To Be Manufactured So That They Would Be Accessible To Law Enforcement When Law Enforcement Has Obtained a Search Warrant

Apple has done something truly extraordinary. I am aware of no products other than those running iOS 8 and Google's analogous Android devices that have been designed specifically to be impervious to lawful governmental processes. While Apple pursues an extraordinary path, I am proposing here a perfectly conventional one – a return to the balanced approach in place prior to the introduction of iOS 8. Apple's products should be configured such that data on its iDevices can be accessed by law enforcement when it has judicial authorization to do so.

I believe that the only way Apple could be compelled to configure its products along the lines that I have suggested is through legislation. It is important to proceed with great caution, and any legislation must be carefully drafted to avoid stifling innovation or causing material harm to the United States technology sector, which is so vital to our national economy. But, in the fast-

changing field of technology, legislation is the right tool – far better than litigation – to effect change and balance social objectives.

Legislation can be changed, revised, amended, and tweaked, to accommodate valid social goals in the face of a shifting technological landscape. As Justice Alito has observed, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[27] Furthermore, legislation allows the public, rather than Apple or any other company, to set the balance between privacy and security. The trade-off is borne by the public, and it should be decided by the public as well.

Informed legislation, however, requires debate and open discussion. I have attempted to discuss with Apple many of the items that I have discussed here. In March of this year, I travelled to Apple's headquarters and expressed my concerns directly to members of Apple's management team as to how Apple's encryption policy adversely affected law enforcement's ability to protect the public safety. I followed up my visit with a letter, summarizing my questions about iOS 8. To date, I have not received a response. (A copy of my letter to Apple, and a copy of a similar letter that I wrote to Google, are attached to this written testimony.)

I would encourage this Committee to seek answers from Apple. The time has come for *someone* to determine the proper balance between the marginal benefits of full-disc encryption, and the need for state and local law enforcement to prosecute and prevent crime, and for victims to obtain justice. That someone should not be Apple or Google. It should be you, the Congress.

Thank you for the opportunity to testify today.

---

[27] *U.S. v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (citing Owen Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805-06 (2004)).

DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N.Y. 10013
(212) 335-9000

CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

March 31, 2015

Jane Horvath, Senior Director of Global Privacy
Apple Headquarters
1 Infinite Loop
Cupertino, CA 95014

Re: Follow-up from our meeting of March 19, 2015

Dear Jane,

Thank you for the time you spent on March 19th with me and my colleagues, as well as representatives from the Secret Service and the National Computer Forensics Institute, discussing smartphone encryption and its impact on law enforcement. We found the discussion helpful.

For us better to understand some of the concerns that you expressed at our meeting, we have some additional questions which we hope that you can answer the following questions:

1. There was much discussion at our meeting about mobile phone data being "backed up" in the Cloud. Therefore, could you please advise us:

    a. What percentage of Apple mobile device users have associated iOS backups stored on Apple's iCloud servers?

    b. What percentage of current Apple mobile device users have the iCloud backup option turned on?

    c. What percentage of current Apple mobile device users have utilized iCloud backup to produce at least one backup stored with Apple?

    d. What is the retention period of an iCloud backup if the user decides to turn off iCloud backup?

    e. Are the iOS8 backups stored on the iCloud encrypted?

2. As we explained, our view is that the judicially-issued search warrant is the bulwark for the protection of people's privacy. I understood that Apple believes that if Apple kept a "key" so that it was able to open locked iPhones, some foreign authorities might compel Apple to open iPhones and thus use them against their own citizens. That leads to the following questions:

    a. Is it accurate that, after the iOS8 upgrade, Apple no longer maintains the ability to unlock iPhones running on iOS8 anywhere in the world market? For example, does Apple no longer maintain the ability to unlock iPhones running iOS8 that it sells in China, India, or other world markets outside of the United States? Even if Apple does not maintain the ability to unlock devices running on iOS8, does Apple provide any foreign agency or entity the right or ability to unlock iOS8 devices?

    b. In the past five (5) years, how many demands have there been from foreign jurisdictions to unlock iPhones, and has phone content been provided to those jurisdictions in response?

    c. For the instances identified in 2(b) above, were those demands from foreign jurisdictions made directly to Apple, or through letters rogatory, or in some other fashion?

3. If Apple kept a "key" so that it was able to unlock iPhones, would the iPhones be more vulnerable to hackers than if Apple had no such "key"? Is there any "key" or similar device that Apple might keep without sacrificing the security of iPhones from hackers? Is there a way to measure or quantify the vulnerability to hackers of iPhones (a) if Apple kept a key, as compared to (b) if it did not keep a key?

We appreciate your time, and we look forward to further conversations. Thank you also for being gracious hosts; it was terrific to be on the Apple campus and see a true state of the art workplace.

Sincerely,

Cyrus Vance

Cyrus R. Vance, Jr.

DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N.Y. 10013
(212) 335-9000

CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

April 1, 2015

Kent Walker, Senior Vice President and General Counsel
Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Re: Follow-up from our meeting of March 19, 2015

Dear Kent,

Thank you for the time you spent on March 19th with me and my colleagues, as well as representatives from the Secret Service and the National Computer Forensics Institute, discussing smartphone encryption and its impact on law enforcement. We found the discussion helpful.

I was pleased and grateful to learn that Google intends to install a law enforcement portal to make interactions between law enforcement and Google, and responses to grand jury subpoenas and search warrants, as efficient and timely as possible.

It is my understanding that Google will continue its encryption initiative and that you expect more original equipment manufacturers to create more devices that support encryption over the next few months. As we made very clear, while we understand your position we feel that encryption that cannot be reached even by lawful process poses a significant problem for law enforcement, and a public safety threat.

To better understand some of the encryption-related matters that we discussed during our meeting, we have some questions that we hope you can answer:

1. In response to our concern about our inability to extract data from cellular phones with full device encryption, it was suggested to us that an alternative means to obtain some of the data from the device would be to obtain date "backed up" to the cloud. Therefore, could you please advise us:

    a. What percentage of Android mobile device users have associated backups stored on servers?

    b. What percentage of current Android mobile device users have the backup option turned on?

c. What percentage of current Android mobile device users have utilized cloud backup to produce at least one stored backup?

d. What is the retention period of a cloud backup if the user decides to turn off the backup?

e. Are the backups stored on the cloud currently encrypted? If it is not currently encrypted, are their plans to encrypt the cloud content and what is the timeline for such implementation?

2. If Google kept a "key" so that it was able to unlock phones, would the phones be more vulnerable to hackers than if Google had no such key? Is there any key or similar device that Google might keep without sacrificing the security of Android devices from hackers? Is there a way to measure or quantify the vulnerability to hackers of Android phones (a) if Google kept a key, as compared to (b) if it did not keep a key?

You expressed frustration at the fact that your employees are required to appear before the grand jury to authenticate Google's business records. I share your frustration, and have drafted proposed legislation that would allow business records to be authenticated by affidavit. A copy of our proposed legislation is enclosed herewith. Google supported an earlier, almost identical, version of this proposed legislation, and I presume that Google would support this as well.

Thank you also for being gracious hosts, and for showing us your state–of-the-art workplace.

Sincerely,

Cyrus R. Vance, Jr.

w/attachment