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

"The Encryption Tightrope: Balancing Americans' Security and Privacy"

Washington, D.C.
March 1, 2016

Good afternoon Chairman Goodlatte, Ranking Member Conyers, and Members of the House Judiciary Committee. Thank you for your attention to this issue, and for the opportunity to testify today. This Committee had invited the National District Attorney's Association to participate in today's hearing, and my colleagues at the NDAA, in turn, asked me to serve as the organization's representative. I am grateful for this opportunity to speak with you on a topic of such importance and urgency to state and local law enforcement.

In recent weeks, the encryption debate has focused on the federal government's investigation into the heinous terrorist acts committed in San Bernardino, California on December 2, 2015. I applaud our federal colleagues for their commitment to justice for the 14 people killed, the 21 people injured, and all of their families. Law enforcement agencies at all levels, as well as crime victims' advocates and other concerned community leaders, are watching this case with great interest.

While the San Bernardino case is a federal case, it is important to recognize that 95 percent of all criminal prosecutions in this country are handled at the state and local level, and that Apple's switch to default device encryption in the fall of 2014 severely harms many of these prosecutions.

And that is why I am here today as a representative of the thousands of local and state prosecutors around the country: Smartphone encryption has real-life consequences for public safety, for crime victims and their families, and for your constituents and mine. In the absence of a uniform policy, our nation will effectively delegate the crafting of national security and law enforcement policy to boardrooms in Silicon Valley. That is, important responsibilities of our government will be carried out by Apple, Google,[1] and other technology companies, who will advance the best interests of their shareholders, not necessarily the best interests of our nation.

For the reasons set forth below, the line between personal privacy and public safety should be drawn by Congress, not Silicon Valley.

I. Smartphone Encryption's Impact on Law Enforcement and Crime Victims[2]

The United States Constitution provides that local law enforcement agents may obtain access to places where criminals hide evidence – including their homes, car trunks,

---

[1] Google, through its parent company Alphabet, has also announced that it will require default full disk encryption on its Android devices. As Apple has been the public leader among technology companies in the question of default full disk encryption, I shall focus on it in these remarks, even though many of the points may be applicable to Google and other technology companies.

[2] For background information on smartphone device encryption, *see* Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety (Nov. 2015), http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf. *See also* Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the U.S. Senate Judiciary Committee (July 8, 2015), http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf; and

storage facilities, computers, and digital networks – so long as the agents have a search warrant issued by a judge. Carved into the bedrock of the Fourth Amendment is a balance between the privacy rights of individuals and the public safety rights of their communities.

iPhones are now the first consumer products in American history that are beyond the reach of Fourth Amendment warrants. Like everyone else, I value my privacy. And I understand there is a fear arising out of mass security breaches, collection of bulk data, and warrantless surveillance. But that is not the access state and local law enforcement seek or expect. Police and prosecutors' access to electronic data is grounded in and limited by the Fourth Amendment, which (a) authorizes only "reasonable" searches, (b) based on probable cause, (c) supported by a particularized search warrant, and (d) approved by a neutral judge. I believe the high burden imposed by the Fourth Amendment – not warrant-proof encryption – is our best protection from abuse.[3]

Critics of law enforcement's position often point out that for centuries, we have successfully conducted investigations without evidence obtained from smartphones, and therefore, we should be able to continue to investigate crime without such evidence. But Apple itself explained why accessing evidence on smartphones is now so critical. In an open letter to customers dated February 16, 2016, Apple CEO Tim Cook stated that, "Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to

---

Response of Cyrus R. Vance, Jr. to the Berkman Center's Report, "Don't Panic: Making Progress in the 'Going Dark' Debate" (Feb. 5, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Letter_CyrusVance_Re_DontPanic.pdf.

[3] Apple itself states that "less than .00673% of customers have been affected by government information requests." http://www.apple.com/privacy/government-information-requests/.

our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going."[4]

This is precisely why default device encryption cripples even the most basic steps of a criminal investigation. In the past, criminals kept evidence of their crimes in safes, file cabinets, and closets. Today, criminals, like the rest of us, live their lives on smartphones and store evidence of their crimes on smartphones. And when you consider that Apple's iOS, together with Android, run 96.7 percent of smartphones worldwide, it should be clear why investigating a case without access to this evidence is doing so with one hand tied behind our backs.

Opponents of our position also ask why law enforcement agencies cannot simply rely on data stored in the cloud. First, not all data on devices are backed up to the cloud. Even data that can be backed up may not be because smartphone users are not required to set up a cloud account or back up to the cloud. Even minimally sophisticated users who use their phones to perpetrate crimes know to avoid backing up their data to the cloud. And even if a user chooses to use the cloud, data on a device will not be backed up unless the device is connected to Wi-Fi,[5] or for Android phones, a cellular connection. Additionally, although it may be possible to recover at least some deleted data from an Apple device, Apple states that once data has been deleted from an iCloud account, Apple cannot provide it in response to a search warrant.

---

[4] Tim Cook, "A Message to Our Customers" (Feb. 16, 2016), http://www.apple.com/customer-letter/.

[5] *See* Apple, "iOS Security: iOS 9.0 or later" (Sept., 2015), http://images.apple.com/business/docs/iOS_Security_Guide.pdf at p. 42.

Other opponents point to the availability of metadata, which often can be obtained through service of a search warrant on a telecommunications carrier. Metadata typically consists of (a) the time at which a call was placed or a message sent, (b) the phone number of the caller or message-sender, as well as the phone number of the recipient of the call or message, and (c) in the case of a phone call, the duration of the call. But metadata does *not* include the substance of a call or message. Thus metadata, while useful, is extremely limited. With it, I can show that two people spoke before a criminal incident, but I cannot show what they said, and that information, of course, will be critical for proving their intent and the scope of their agreement. For law enforcement to investigate, prosecute, and exonerate effectively, the most substantive evidence should be reviewed and utilized.

Likewise, iMessages – the default messaging platform between Apple devices – are transferred over Apple's servers rather than across telecommunications channels. Thus, telecommunications carriers are not privy to iMessages, their content, or their metadata. Additionally, Apple is not required by any regulation to retain that information. Indeed, Apple states that it does not retain the content of iMessages, and does not provide decrypted iMessage data in response to court orders.[6]

The real-world effect of all of this is that Apple's encryption policy frustrates the ability of law enforcement to prevent, investigate, and prosecute criminals, including the very hackers that Apple claims it wants to protect users against. It also impacts law enforcement's ability to exonerate those suspected of, but not responsible for crimes.

---

[6] *See* Apple, "iOS Security: iOS 9.0 or later" (Sept. 2015), http://images.apple.com/business/docs/iOS_Security_Guide.pdf, at p. 39: "Apple does not log messages or attachments, and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple cannot decrypt the data."

When Apple made the overnight switch to default device encryption in September 2014, my Office began tracking the number of cases in which we recovered iPhones that we could not unlock and that we reasonably believed contained data pertinent to the case that we were investigating. As of the November 2015 release of our Report on Smartphone Encryption and Public Safety, we were locked out of 111 Apple devices running iOS 8 or higher. That number is now 175 – comprising one quarter of the approximately 670 Apple devices received by our in-house Cyber Lab during that same period. As Apple users continue to migrate to the newer operating systems, the percentage of iOS devices that we are unable to access has increased significantly; in fact, in recent months, approximately one out of every two Apple devices collected by my Office's Cyber Lab is inaccessible. These numbers do not include Android devices or any devices that may have been processed by other district attorneys in New York City, or by the New York City Police Department.

The 175 Apple devices from which my Office is locked out represent investigations into the attempted murder of three individuals, the sexual abuse of a child, sex trafficking, child pornography, assault, robbery, identity theft, and all manner of other crimes. My colleagues from jurisdictions around the country have been running into the same road blocks in their efforts to investigate and prosecute serious crimes. For example, last year in Texas, Harris County District Attorney Devon Anderson's Office encountered more than 100 encrypted Apple devices from a variety of cases, including human trafficking, violent street crimes, and sexual assaults. In 2016, the problem continues with investigators unable to access eight to ten Apple devices every month. Similarly, in just the past two months in the Chicago area, Cook County State Attorney Anita Alvarez's Cyber Lab has received 30

encrypted devices that they are unable to access. The Connecticut Division of Scientific Services has encountered 46 encrypted Apple devices across a variety of criminal cases, including several matters involving child pornography.

As prosecutors, we have the extraordinarily difficult task of explaining to crime victims, or their surviving family members, that we have hit an investigative road block or dead end in their case, simply because Apple states that it will not comply with search warrants. In this debate among law enforcement leaders, intelligence officials, civil liberties proponents, and technology companies, one important voice has largely been left out – that of crime victims and their loved ones. Safe Horizon, the nation's leading victim assistance organization, recently explained how significantly encryption will hurt crime victims:

> It is important to note the devastating impact that smartphone encryption can have on victims of crime and abuse…. As a result [of default device encryption], perpetrators of child abuse and sexual assault are far less likely to be held accountable for these and other crimes. We recognize and respect a phone user's right to privacy. However, it is imperative that all evidence pertaining to criminal activity be available to law enforcement agencies with duly authorized search warrants. We owe no less to survivors of child abuse, human trafficking, domestic violence, and other violent crimes.[7]

II. Achieving a Balance Between Privacy and Security

My Office's Report — drafted in consultation with cryptologists, technologists, and law enforcement partners — proposed a solution that we believe is both technologically and politically feasible: *Keep the operating systems of smartphones encrypted, but still answerable to search warrants issued by neutral judges*. We do not want a backdoor for

[7] Safe Horizon, "Safe Horizon on Apple's Opposition to FBI Accessing Smartphones" (Feb. 18, 2016), http://www.safehorizon.org/page/in-the-news-125/news/safe-horizon-on-apples-opposition-to-fbi-accessing-smartphones-356.html.

the government to access users' information, and we do not want a key held by the government. We want Apple, Google, and other technology companies to maintain *their* ability to access data at rest on phones pursuant to a neutral judge's court order.

My Office has drafted, and provided to members of Congress, proposed federal legislation that requires designers of operating systems used on devices manufactured, leased, or sold in the United States to ensure that data on those devices, pursuant to a search warrant, are capable of being accessed in unencrypted form. Designers would not be responsible for decrypting, or ensuring the government's ability to decrypt, any data encrypted by a user, unless the encryption used was part of the operating system's design. This solution represents the reasonable, achievable, middle ground in this debate.

Throughout our history, the government has enacted statutory schemes to balance business concerns with law enforcement compliance, particularly when those businesses' products become an integral part of our lives. Those businesses recognize that they have a corporate responsibility to help protect victims from crime being perpetrated through the use of their products. One example is banks and financial institutions. As we learned more about how criminals were using banks to move money, Congress enacted statutes related to money laundering, fraud, and document preservation. Similarly, when it became clear that criminals were using phone lines to perpetrate crimes, Congress passed the Communications Assistance for Law Enforcement Act, requiring telephone companies to provide an access point for wiretaps.

Indeed, companies from every sector – finance, health care, transportation, energy, manufacturing, and telecommunications, to name a few – recognize and comply with the

obligation to respond to signed court orders arising out of criminal cases. For example, in 2014, Verizon received 287,559 United States law enforcement requests for data; they received 149,810 requests in the first half of 2015.[8] Facebook received 29,707 United States law enforcement requests for data in 2014; for the first half of 2015, they received 17,577 requests.[9] Now that smartphones have become as ubiquitous as landlines, it is time for Congress to enact legislation ensuring that law enforcement can access evidence of crime stored on smartphones with a judicial order.

Rather than accepting its corporate responsibility, Apple touted in its marketing of iOS 8 that "Apple will not perform iOS data 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."[10] In refusing to assist law enforcement, Apple contends that doing so would leave their customers' information open to hackers, foreign dictatorships,[11] and other bad actors. Before I address that argument, I want to emphasize that there is probably no local law enforcement office in the country

---

[8] Verizon, "United States Report," https://www.verizon.com/about/portal/transparency-report/us-report/.

[9] Facebook, "United States Law Enforcement Requests for Data," https://govtrequests.facebook.com/country/United%20States/2015-H1/.

[10] This language was previously found at https://www.apple.com/privacy/government-information-requests/.

[11] Many in the technology industry claim that if the U.S. government seeks access to smartphone evidence, the government will "have little room to object" to requests from repressive regimes. *See* Open letter to Pres. Barack Obama (May 19, 2015), https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf. This assertion ignores the fact that local law enforcement in the U.S. seeks access to information only through a lawful judicial process. If a foreign nation's government, repressive or not, 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 (MLAT) 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.

that deals with more cybercrime and identity theft than mine, so of course we understand the importance of encryption. We want smartphone makers to offer the same strong encryption that Apple employed before iOS 8. Those previous mobile operating systems allowed data to be accessed on a seized device with a valid court order, and I am not aware of any documented security problems with those operating systems. Apple has never explained why its prior systems lacked security or were vulnerable to hackers and thus needed to be changed.

Indeed, Apple characterized its prior encryption as the ultimate in privacy. Apple's May 2012 guide to "iOS Security" – published before its switch to default device encryption – notes that "Apple is committed to incorporating proven encryption methods and creating modern mobile-centric privacy and security technologies to ensure that iOS devices can be used with confidence in any personal or corporate environment."[12] According to Apple, iOS 7 "provides solid protection against viruses, malware and other exploits that compromise the security of other platforms."

And yet, under iOS 7, Apple maintained the ability to help – in their own words – "police investigating robberies and other crimes, searching for missing children, trying to locate a patient with Alzheimer's disease, or hoping to prevent a suicide."[13] Apple itself has demonstrated that strong encryption and compliance with court orders are not incompatible.

---

[12] Apple, "iOS Security" (May 2012), https://web.archive.org/web/20121021133728/http:/images.apple.com/ipad/business/docs/iOS_Security_May12.pdf.

[13] Apple, "Apple's Commitment to Customer Privacy" (June 16, 2013), http://www.apple.com/apples-commitment-to-customer-privacy/.

Furthermore, it is not entirely clear what cybersecurity problem Apple's new encryption is intended to solve. Individuals' phones were not being stolen *and* hacked into. Prior to iOS 8, to bypass the lock on a passcode-protected phone, Apple required both (i) possession of the phone[14] and (ii) its custom method to bypass the device encryption. We never held the key, we have never wanted to hold the key, and we have never heard about a key held by Apple being stolen. Even if a hacker were able to learn Apple's decryption process — which Apple guards closely — that hacker would also need to have the actual device to steal its data. Likewise, a thief who steals a person's locked smartphone would also need to know either the victim's passcode or Apple's highly guarded decryption process to obtain the device's data.

There has been much discussion and concern about large-scale, institutional data breaches involving Home Depot, Target, and other large companies. These breaches are deeply disturbing, of course, but they have nothing to do with the level of encryption on iPhones. These two issues – large-scale data breaches from servers, and smartphone encryption – should not be conflated. Apple's default device encryption would do nothing to protect against large-scale institutional data breaches or the use of malware.

Apple and other proponents of device encryption have portrayed the new policy as a response to the concerns raised by Edward Snowden about data collection by the National Security Agency. But, once again, data collection has nothing to do with smartphone encryption. Smartphone encryption would not have prevented the NSA's mass collection of phone-call data or the interception of telecommunications, as revealed by Mr. Snowden.

---

[14] Mr. Cook stated in his February 16, 2016 letter to customers that in the wrong hands, any software it creates for the government "would have the potential to unlock any iPhone in someone's *physical* possession." (Emphasis added.) http://www.apple.com/customer-letter/.

Likewise, Apple has not explained how any software it may create for purposes of responding to search warrants – software which Apple keeps in its sole possession – would fall into "the wrong hands." In its refusal to assist the government, Apple has not addressed the fact that it already can, and frequently does, bypass iPhone users' passcodes. For example, Apple has the ability to access an Apple device remotely, such as when it tracks the location of a device and erases its contents remotely ("Find My iPhone"), or when it sends iOS software updates to the customer's iPhone. Apple is able to do these things without knowing the particular device's passcode. But Apple has never contended that the existing means for tracking and wiping devices remotely or pushing software updates may be exploited by bad actors. Rather, Apple maintains that its customers' data is secure.

Furthermore, Apple allows corporate administrators and other employers, through mobile device management ("MDM") solutions, to access organization-owned and employee-owned devices remotely, and to modify the device's iOS software, settings, and data. According to Apple, "an MDM server can perform a wide variety of administrative commands, including changing configuration settings automatically without user interaction, locking or wiping a device remotely, or clearing the passcode lock so users can reset forgotten passwords."[15] Apple has never explained why MDMs – tools that Apple enables and promotes, and which allow third parties to access a user's iPhone without a passcode – do not compromise an iPhone user's security, while any software Apple develops in order to comply with a search warrant may fall into "the wrong hands."

I previously sought answers to a few of the questions raised in this testimony in letters sent to Apple and Google in April 2015. To date, I have not received a response

[15] *See* Apple, "iOS Deployment Overview for Enterprise," http://images.apple.com/business/docs/iOS_Enterprise_Deployment_Overview.pdf.

from either company. Those letters are annexed to my Office's Report on Smartphone Encryption and Public Safety.

III. Conclusion

Apple's influence can be felt in every corner of the globe. In its fiscal quarter ended December 26, 2015 alone, Apple reported record profits of $18.4 billion.[16] But Apple is not above the law,[17] and its bottom line is not more important than the safety of Americans.

In Mr. Cook's February 16, 2016 letter, he argues that the FBI's request for assistance in the San Bernardino case "threatens the security of our customers." Mr. Cook and his colleagues at Apple have effectively decided that they know better than our elected representatives and professionals in law enforcement how best to keep Americans safe. In the absence of laws that keep pace with technology, we have enabled Apple and other technology companies to upset the balance between privacy and public safety established by centuries of jurisprudence.

Technology companies should not be able to dictate who can access key evidence in criminal investigations. No device or company, no matter how popular, should be able to exempt itself from court obligations unilaterally. And they should not be able to write their own laws. I do not believe Americans would want to cede this vast authority to private enterprise. That authority should rest with the people's elected officials. I urge Congress to enact a national solution.

Thank you for the opportunity to participate in this critically important discussion.

---

[16] Apple, "Apple Reports Record First Quarter Results" (Jan. 26, 2016), http://www.apple.com/pr/library/2016/01/26Apple-Reports-Record-First-Quarter-Results.html.

[17] Notably, in testimony before the U.S. Senate Judiciary Committee in 2013, Mr. Cook told lawmakers: "We not only comply with the laws, but we comply with the spirit of the laws." https://www.apple.com/pr/pdf/timcookopeningstatement.pdf.