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

"Cybersecurity and U.S. National Security"

Washington, D.C.
July 14, 2016

Good morning Chairman McCain, Ranking Member Reed, and members of the Senate Committee on Armed Services. On behalf of my Office and our partners in state and local law enforcement, I thank the Committee for its work and attention to what is not only a critically important issue of national security, but also an issue of public safety and justice for crime victims in thousands of local jurisdictions across the United States.

The decision by Apple and Google to engineer their mobile devices to be, in effect, "warrant-proof" has upended the balance that we have long enjoyed between privacy and public safety. Without federal legislation to restore that balance, we have delegated to businesses like Apple and Google the power to set it themselves.

The debate over encryption and public safety has matured significantly since 2014. The issue has crossed over into mainstream consciousness, owing in large part to Apple's public refusal to assist the FBI with unlocking a terrorist's iPhone in San Bernardino. The San Bernardino episode introduced many Americans for the first time to the problem posed by smartphone encryption in criminal investigations, and my Office and our partners have gone to

some lengths to demonstrate to the public and to policymakers the full scope of the challenge in each of our jurisdictions.

The basic facts underlying this debate are really not in dispute. First, as Tim Cook said himself in his open letter to customers dated February 16, 2016: "Smartphones, led by iPhone, have become an essential part of our lives."[1] As a citizen, I certainly appreciate the many benefits of the internet age.

But second, these devices are also essential to criminals. Our office investigates and prosecutes a wide range of cases – from homicide to sex crimes, from international financial crime to terrorism. In all those crimes and others, it is undisputed that criminals use smartphones to share digital information, and to plan and commit crimes, whether through iMessages, photos, or videos.

Third, criminals know iPhones now enable them to communicate with impunity about their crimes. The criminals are thrilled with this development. That is not hyperbole. In a real example from a case in my office, an incarcerated defendant on a pending sex crimes charge tells his friend on a lawfully recorded landline phone from jail, "Apple and Google came out with these softwares [sic] that I can no longer be [un]encrypted by the police… [i]f our phone[s are] running on iOS8 software, they can't open my phone. This may be [a]nother gift from God."

That is not a gift from God, but an unintended gift from two of the largest technology companies in the world.

Fourth, Apple and Google's decisions limit our access to critical information under a questionable claim of an increase in privacy. The encryption Apple provided on its mobile devices pre-iOS 8—that is, up until the end of September, 2014—was both secure for its

---

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

customers and amenable to court-authorized searches. We have good cause to believe that because Apple itself characterized its iOS 7 operating system as the ultimate in privacy, touting its proven encryption methods, and assuring users that iOS 7 could be used with confidence in any personal or corporate environment.[2] And yet, under iOS 7, Apple also maintained the ability to help—in Apple's 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."[3] Which is to say, Apple itself had already demonstrated that strong encryption and compliance with court orders were not incompatible.

Given Apple's own statements about the security of iOS 7, shortly after Apple's re-engineering of its phones to prevent search warrant access by law enforcement, I asked it in a letter dated March 2015, whether there was a *bona fide* security reason to make its new operating system, iOS 8, warrant-proof.[4] Apple chose not to answer me, but in March of this year, the House Judiciary Committee compelled Apple to answer the same question. That Committee asked Apple the following question, in writing, "Was the technology you possessed to decrypt these phones"—and the clear reference is iOS7 phones and their predecessors—"ever compromised?" Apple's written response was: "The process Apple used to extract data from locked iPhones running iOS 7 or earlier operating systems ***was not, to our knowledge, compromised***."[5] (Emphasis added.)

---

[2] *See* Apple, "iOS Security" (May 2012), at p. 2, https://web.archive.org/web/20121021133728/http:/images.apple.com/ipad/business/docs/iOS_Security_May12.pdf.

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

[4] Letter from Cyrus R. Vance, Jr. to Jane Horvath, Senior Director of Global Privacy for Apple, Inc. (March 31, 2015), attached as Appendix II to the 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.

[5] Bruce Sewell, Senior Vice President and General Counsel for Apple, Inc., Responses to Questions for the Record, "The Encryption Tightrope: Balancing Americans' Security and Privacy," at p. 2.

Apple's answer to this crucial question shows what we have long suspected: That Apple's method of data extraction under iOS 7 posed no documented security problems. That being so, then there should be no unreasonable security risk going forward if we return to the procedure where court-ordered warrants can be honored by extracting responsive data off of smartphones.

Let me give you the impact of this new encryption protocol introduced by Apple. In my Office alone, we now have more than 310 lawfully-seized iPhones running iOS 8 or 9 that are completely inaccessible, despite court-ordered search warrants having been issued for them. These devices represent hundreds of real crimes against New Yorkers that we cannot fully investigate, including cases of homicide, child sex abuse, human trafficking, assault, cybercrime, and identity theft.

The data from across the country tells a similar story. In California, the Los Angeles County Sheriff's Department has amassed more than 150 inaccessible devices, the Los Angeles Police Department has more than 300, and the Roseville Police Department has more than 200. Riverside County, California has 12 inaccessible devices connected to murder cases alone. The Charlotte-Mecklenburg Police Department in North Carolina has 160 inaccessible devices. In Texas, the Harris County District Attorney's Office collected more than 100 inaccessible devices in 2015 and have encountered 8 to 10 inaccessible devices per month so far this year. And in Massachusetts, the Suffolk County District Attorney's Office has 129 inaccessible devices.

My brief list shows the problem from the perspective of some members of state and local law enforcement. But even this small sampling represents more than one thousand cases in

---

http://docs.house.gov/meetings/JU/JU00/20160301/104573/HHRG-114-JU00-Wstate-SewellB-20160301-SD001.pdf.

which local prosecutors lack the evidence that we need—and that juries demand—to hold criminals accountable, exonerate the innocent, and deliver justice for victims and safety in our streets.

Some have argued that we now live in a "Golden Age of Surveillance," and therefore, prosecutors do not need smartphone evidence to effectively do our jobs. They frequently point to the availability of metadata, which is what we can obtain from a wireless carrier. Metadata typically consists of the time at which a call was placed or a message sent, and the phone numbers of the parties to that call or message. But metadata, while useful, is extremely limited because it does not include the substance of a call or message. With metadata, 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.

The same is often true for social media – it can be a good tool for figuring out whether people know each other, but in many cases, it does not provide the level of content that we need to make our case. For law enforcement to investigate, prosecute, and exonerate most effectively, we need access to substantive evidence when we have a court order.

The problems created by default device encryption manifest themselves differently in almost every criminal case. Without critical evidence on smartphones, prosecutors may not be able to secure the most serious charge, but instead can only seek a lesser offense. As an example, my Office recently handled a case where we had strong reason to believe that the defendant was running a human trafficking operation. But with evidence from that defendant's smartphone locked behind a passcode known only to him, and existing solely on his device, we could only charge a far less serious offense, Promoting Prostitution, which carries less stringent penalties than human trafficking.

In other cases, there may be co-conspirators to the criminal scheme, but without the substance of their communication with defendants, prosecutors cannot charge those co-conspirators at all. In other cases still, the defendant may have victimized additional people, but prosecutors cannot charge the defendant for those additional crimes without evidence contained on smartphones.

In my view, it is no answer to say, as some suggest, that "government" should develop the capacity to hack into devices. A technological arms race between the federal government and Silicon Valley is not in our collective interest. The enormous cost and energy of such a conflict are better directed against our common enemies, criminals.

Furthermore, local law enforcement agencies do not have the resources to access each lawfully-seized device. Many lack in-house forensics labs, and would be required to send each device to costly, third-party companies for analysis and data extraction. According to reports, the FBI paid upwards of a million dollars to bypass the terrorist's passcode in the San Bernardino case. That amount represents more than the budgets for all law enforcement agencies in many counties around the country.

And despite the large number of experts in the field of digital forensics and cryptology, such experts are still several iPhone models behind Apple. The method employed to open Syed Farook's iPhone in the San Bernardino case reportedly works only on that particular model iPhone and that particular operating system, and only until Apple finds and patches the flaw that the FBI was able to exploit.

The solution to the encryption problem is not a technological arms race. It is federal legislation. I appreciate that some are skeptical of federal regulation, but federal regulation of consumer products that impact public safety has been a part of our legal landscape for over 100

years, and numerous industries, especially in financial services, are required by federal regulation to retain data expressly for the purpose of helping to combat fraud and other wrongdoing. Many of these regulations initially faced resistance, and the affected industries argued that the regulations were imposing upon individuals' privacy interests. But over time, the regulations have been accepted, and it is clear that they play an important part in our society, especially in keeping people safe from criminal harm.

Federal regulation is already important in the communications industry. When telephone companies went from using copper wires to using fiber optics and digital signals, the police could no longer use their old techniques of executing wiretap orders, and so Congress passed the Communications Assistance for Law Enforcement Act (CALEA), mandating that telecom providers build into their systems mechanisms for law enforcement to install court-ordered wiretaps. CALEA has worked. It has saved lives, and it has withstood Constitutional challenge. It has not stifled innovation, as its opponents feared. It has not caused American consumers to migrate en masse to foreign competitors in search of greater privacy.

Also consider financial services, one of the most regulated industries in our country. As we learned more about how criminals were using banks to move money, Congress required firms to fight money laundering and to better know their customers – and specifically, to retain customers' data and make that data available to law enforcement with a court order. Over time, government and industry came together to work out compliance costs and procedures, and a broad consensus in favor of these rules emerged. The industry recognized that absolutism on customer privacy was not in its best interest. Banks and investment firms did not want to be conduits for crime and terror.

Here are a few other examples: DEA regulations require all U.S. pharmacies to maintain paper and electronic prescriptions bearing the name of the patient and prescriber, drugs dispensed, and dates filled. FTC regulations require any business that checks a customer's identification to maintain and provide victims and law enforcement with transaction records relating to identity theft. State regulations require private schools to maintain student data records, including records of attendance and suspected child abuse.

I could go on. The point is that companies in nearly every industry are required by law to maintain voluminous customer records and produce criminal evidence when they receive a court order. When your introduction of goods and services into the stream of commerce overlaps with public safety, this is the price of doing business in the United States. You cannot sell a car in this country unless it has dual air bags. But smartphone encryption, one of the great public safety challenges of our time, remains almost entirely self-regulated.

Apple and Google's position is that they must be exempt from these public safety obligations due to a cybersecurity risk unique to their sector. But if we are going to make such an exemption – if we are going to agree to live with the collateral consequence of a little bit more crime and terror – then the need for this exemption must be grounded in sound data analysis. We need quantitative data – not rhetoric – to substantiate the benefits of unregulated, default device encryption on smartphones. If we are going to authorize – for the first time in our society – evidence-free zones, we need to be sure there was a problem that needed to be solved in the first place. We need to know what we are getting in exchange for trading away a measure of our public safety.

My Office's proposed solution is to enact a federal statute providing that data on any smartphone made or sold in the United States must be accessible—not by law enforcement, but

by the maker of the smartphone's operating system—when the company is served with a valid search warrant. And if a person or entity such as Apple offers encryption software, it has to have the ability to provide data in response to a judicial order.

This solution – as spelled out in my Office's 2015 Report on Smartphone Encryption and Public Safety – requires no new technology, and no government backdoor. I want to make it clear that we do not want to ban encryption. There is probably no office in the country that deals with more cybercrime and identity theft cases than mine, so of course, we support strong encryption. Under our proposed solution, Apple would be able to comply with judicial warrants, and to offer the same strong encryption that it employed without a single documented breach before it adopted default device encryption in iOS 8.

This solution is limited to data at rest on smartphones. It would not affect encryption of data in motion. I cannot at this time offer a technical fix to address data in motion. I am confident, however, that engineers from industry and government, working together in good faith, can find one.

The focus of my Office's proposed legislation is appropriate because since September 2014, our primary obstacle in local law enforcement has involved getting access to data at rest on smartphones that we possess. That would be no small achievement because it is local law enforcement that prosecutes more than 95 percent of crimes committed in the United States.

As it stands today, Apple and Google—not a court, not Congress—decide who has access to key evidence in criminal investigations and trials. I cannot, and do not believe it is right, that two private companies should decide which victims can achieve justice.

There has been discussion about convening task forces to examine the science and policy implications of default device encryption. That may be a good step, but I urge Congress to act

quickly. Twelve months of taking testimony resulting in non-binding recommendations in a report will not adequately address the urgency of the problem that local law enforcement faces. Time is not a luxury that local law enforcement, crime victims, or communities can afford. Our laws require speedy trials. Victims require justice. And criminals must be held accountable before they can reoffend.

Centuries of jurisprudence hold that no item—not a home, not a file cabinet, and not a smartphone—is beyond the reach of a judicial order. Our access to data is grounded in and limited by the Fourth Amendment, which authorizes only reasonable searches, based on probable cause, supported by a particularized search warrant, issued by a neutral judge. That burden, not warrant-proof encryption, is the strongest safeguard we have in balancing privacy and public safety.

Thank you for the opportunity to testify today.