REPORT OF THE
MANHATTAN DISTRICT ATTORNEY'S
OFFICE ON

SMARTPHONE ENCRYPTION AND PUBLIC SAFETY

An update to the November 2015 Report

November 2016

Contents

Introduction

In September 2014, Apple Inc. announced that its new mobile operating system, iOS 8, would differ from all of Apple's previous operating systems in that it would be designed and built so that Apple would no longer have the ability to extract data from any mobile device, even if presented with a properly executed and judicially authorized search warrant directing it to do so. As Apple explained on its website, "[u]nlike 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."[1]

The reaction to Apple's announcement was swift. Google followed suit, and announced that it, too, would create operating systems that it could no longer access.[2] At the same time, representatives of law enforcement expressed deep concern that making emails, iMessages, photos, and other forms of data stored on devices impossible to extract, and thus beyond the reach of law enforcement, would pose a significant risk to public safety, because it would allow law breakers, be they international terrorists or domestic criminals (*e.g.,* thieves, fraudsters, drug traffickers, identity scammers) to plot, coordinate, arrange, recruit and conspire, without fear of law enforcement discovering their tracks.[3]

---

[1] *See* Apple.com Privacy page, September 19, 2014, available at https://web.archive.org/web/20140919170856/http://www.apple.com/privacy/government-information-requests/. As of the date of this report, Apple has a similar statement on its website: "For all devices running iOS 8 and later versions, 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." Apple.com Government Information Requests, September 29, 2016, available at http://www.apple.com/privacy/government-information-requests/.

[2] *See, e.g.,* Craig Timberg, "Newest Androids will join iPhones in offering default encryption, blocking police," *Washington Post*, September 18, 2014, available at https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

[3] *See, e.g.,* testimonies by District Attorney Cyrus R. Vance Jr., which include the following: "Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the United States Senate Committee on the Judiciary," July 8, 2015, available at http://manhattanda.org/sites/default/files/7.8.15%20DA%20Vance%20Written%20Testimony%20re%20Encryption.pdf; "Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the United States House of Representatives Committee on the Judiciary," March 1, 2016, available at http://manhattanda.org/sites/default/files/3.1.16%20DA%20Vance%20House%20Judiciary%20Encryption%20Written%20Testimony_0.pdf; "Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the United States Senate Committee on Armed Services," July 14, 2016, available at http://manhattanda.org/sites/default/files/7.14.16%20DA%20Vance%20Written%20Testimony%20for%20Senate%20Armed%20Services%20Committee.pdf.

See also op-eds by District Attorney Cyrus R. Vance Jr., which include the following: "Apple and Google Threaten Public Safety with Default Smartphone Encryption," *Washington Post*, September 25, 2014, available at https://www.washingtonpost.com/opinions/apple-and-google-threaten-public-

In November 2015, approximately one year after Apple's announcement, this Office issued a white paper, Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety (the "Report").[4] The Report attempted to explain and illustrate some of the legal and practical problems for law enforcement posed by default device decryption,[5] and to report on the efforts that foreign countries have made with regard to such devices.[6] The Report also noted that the actual benefits of iOS 8's default device encryption had not been demonstrated by Apple, and it therefore presented a set of questions for Apple and others to answer about the anticipated practical benefits.[7] Finally, the Report included proposed legislation, for both state and federal governments, that would effectively end the sale and distribution of impenetrable mobile devices.[8]

This paper is intended to update readers on developments since this Office issued the Report. As will be seen below, the risks posed by default device encryption have been illustrated again and again since the Report was issued, and while there have been vigorous efforts by law enforcement officials to address those risks and dangers, there has been precious little progress.

---

safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html?utm_term=.f4b099de00f4; co-authored with François Molins, Adrian Leppard, and Javier Zaragoza, "When Phone Encryption Blocks Justice," *New York Times*, August 11, 2015, available at http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html; "5 ways tech companies distort the encryption debate," *Washington Post*, December 15, 2015, available at https://www.washingtonpost.com/news/in-theory/wp/2015/12/15/5-things-tech-companies-dont-understand-about-encryption/?utm_term=.9d72beee67c6; co-authored with Jackie Lacey and Bonnie Dumanis, "Congress can put iPhones back within reach of law enforcement," *L.A. Times*, May 11, 2016, available at http://www.latimes.com/opinion/op-ed/la-oe-vance-congress-act-on-iphones-20160511-story.html.

See also testimonies by Hon. James B. Comey, which include the following: "Joint Statement with Deputy Attorney General Sally Quillian Yates before the Senate Judiciary Committee," July 8, 2015, available at https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy; "Statement Before the House Judiciary Committee," March 1, 2016, available at https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy.

See also James Comey, "We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead," *Lawfare*, February 21, 2016, available at https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead; David Sanger and Brian X. Chen, "Signaling Post-Snowden Era, New iPhone Locks Out NSA," *New York Times*, September 26, 2014, available at http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html.

4 Available at http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

5 *See* Report at 4 - 12.

6 *See id.* at 16 - 17.

7 *See id.* at 20 - 22.

8 *See id.* at 13.

-- As illustrated by the San Bernardino domestic terrorist attack in December 2015, as well as by the ever-increasing number of smartphones lawfully seized by law enforcement that cannot be accessed by law enforcement or by Apple, the threat to public safety ***is increasing rapidly***. *See infra* Point I.

-- Default device encryption ***does not meaningfully increase*** smartphone users' protection from unauthorized hackers, and requiring the smartphone manufacturer or software supplier to maintain a key to the smartphones would not imperil those users. *See infra* Point II.

-- ***There is no comprehensive lawful and effective way*** to compel smartphone users to provide their passcodes to law enforcement or to unlock their devices. *See infra* Point III.

-- Although there have been efforts on the federal level and in at least three states to address the public safety concerns raised by impenetrable smartphones, ***the legislative efforts have stalled.*** *See infra* Point IV.

-- Several foreign nations, often spurred by the fear of terrorism, have addressed the question of whether manufacturers and software providers can be compelled to extract data from smartphones that they manufacture or for which they provide software. ***These nations' efforts in this endeavor have been halting***. *See infra* Point V.

-- Federal legislation is required to address the problem of smartphones whose contents are impervious to search warrants. Two proposed bills, the Compliance with Court Orders Act, drafted by Senators Richard Burr and Dianne Feinstein, and a bill drafted by our Office, would adequately ***address the problem***. *See infra* Point VI.

It is important to be clear at the outset about the scope of the issue addressed in this report. The public is bombarded with stories of large-scale, institutional cyberattacks and data breaches including, for example, the hack of the Democratic National Committee (DNC) in 2016, the breach at the Office of Personnel Management (OPM) in 2015, the Target attack in 2014, and other compromises of personal identifying information from banks and governmental agencies.[9] Regrettably, it has become commonplace for individuals and institutions to be victimized by cybercriminals, both domestic and international.

These unwarranted and enormous invasions of privacy must be distinguished from the extremely limited, lawful infringement on privacy that takes place when Apple unlocks devices in a secure facility following its receipt of a judicially authorized order; the latter scenario is the subject of this report. In most cases, the large-scale breaches were caused by

---

[9] *See e.g.* Jonathan Stempel, "Home Depot settles consumer lawsuit over big 2014 data breach," *Reuters*, March 8, 2016, available at http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z; Brendan Koerner, "Inside the Cyberattack that Shocked the U.S. Government," *Wired,* October 23, 2016, available at https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/; Kassia Halcli, "Does the U.S. government really know who hacked Democrats' emails?," *PBS*, October 26, 2016, available at http://www.pbs.org/newshour/rundown/does-government-know-hacked-emails/.

phishing, malware, and improperly protected security systems. Device encryption does not defend against these categories of cyberattacks and hacks, nor does it protect users against phishing scams.[10] If anything, it thwarts law enforcement's ability to identify and apprehend the perpetrators. Likewise, device encryption would not have protected users from the NSA's bulk collection of communications metadata,[11] and Apple's implementation of default device encryption does not prevent Apple from collecting and using certain personal and non-personal information of its users, and often sharing this information with third parties.[12]

I. The Risks Remain, and Are Growing

In the more than two years since Apple and Google announced that their operating systems would be inaccessible to the companies themselves, law enforcement's inability to access critical evidence has hindered criminal investigations and prosecutions throughout the world.

During this time, Apple has released three new generations of iPhone models, as well as two new iterations of its iOS operating system. With iOS 9, Apple increased the default passcode requirement from four digits to six digits, significantly increasing the number of possible passcode combinations and making "brute force" efforts to get information more difficult. With iOS 10, Apple introduced "differential privacy," which increases the amount of data being collected by Apple (and third-party app developers), but strips user-identifying information from the data. Apple explained that differential privacy technology is being used

---

10 In many of its public statements on this topic, Apple has failed to distinguish between, on the one hand, wide-scale security breaches, and, on the other hand, security issues that default device encryption purportedly addresses. *See, e.g.,* Nancy Gibbs and Lev Grossman, "Here's the Full Transcript of TIME's Interview with Apple CEO Tim Cook," *Time Magazine,* March 17, 2016, available at http://time.com/4261796/tim-cook-transcript/. In this interview Cook argues, *inter alia*, that the order to unlock the iPhone in the San Bernardino case somehow sought to do away with end-to-end encryption of communications, making "millions of people more vulnerable." This was not the case.

11 In fact, leaked NSA documents note that Apple was a participant in the NSA's PRISM program in 2012. To our knowledge, Apple has never confirmed their participation in this program. *See* Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *Washington Post*, June 7, 2013, available at https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian,* June 7, 2013, available at https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1.

12 Apple discloses a number of scenarios in which personal and non-personal information is accessed and shared in their Privacy Policy and Terms of Service. *See* Apple's Privacy Policy, September 12, 2016, available at http://www.apple.com/privacy/privacy-policy/; Apple Media Services Terms and Conditions, September 13, 2016, available at http://www.apple.com/legal/internet-services/itunes/us/terms.html.

"to help discover the usage patterns of a large number of users without compromising individual privacy."[13]

Apple's position in regards to law enforcement requests for information has thus remained unchanged: it remains unable – because it has intentionally rendered itself unable – to respond to law enforcement requests, or court issued search warrants, for encrypted data stored on users' smartphones.

A. San Bernardino

The threat to public safety posed by impenetrable mobile devices was illustrated in connection with the events of December 2, 2015 in San Bernardino, when Syed Rizwan Farook and his wife Tashfeen Malik attacked the Inland Regional Center using five firearms, killing 14 individuals and injuring over 22, and attempted to unleash more carnage by leaving three pipe bombs at the scene. The FBI's efforts to investigate the attack (Was anyone else involved or aware of it? Who had supplied the weapons to Farook and Malik? Had they been aided or abetted by anyone else? Were they part of a larger conspiracy?) and to investigate the likelihood of future attacks were stymied because Apple was unable to access data stored on Farook's iPhone 5C, which was running iOS 9, due to the company's adoption of default device encryption. Although Farook's phone belonged to his employer, who consented to a search of the phone by the FBI, FBI officials were unable to access the device without the passcode set by Farook, which they did not have.[14]

The FBI thus could not access the contents of Farook's phone to review his iMessages, text messages, photos, or videos. It is difficult to overstate the value of such information in a criminal investigation. In Farook's case, it might have shown how and when the couple was radicalized, if there were other associates who provided assistance, how they were able to plan and execute the attack, and to determine whether potential future attacks by others in their network were on the horizon.

---

13 *See* Apple's email explanation to Gizmodo, William Turton, "Is Apple's New Privacy Feature Safe?" *Gizmodo*, June 13, 2016, available at http://gizmodo.com/is-apples-new-privacy-feature-safe-1781910821.

14 According to Apple executives, and later confirmed by the FBI, San Bernardino County officials were asked to, and did, reset the password of the Apple ID associated with Farook's iPhone and the device's iCloud account. Apple claims that if this reset had not occurred, the government may have been able to obtain a backup copy of the information stored on the phone from the device's iCloud account. The Apple ID password reset did not, however, affect any data that may have been stored on the device itself – that is, had the password not been reset, the data on the phone would not have been any more easily accessed by the FBI than it was following the reset. *See, e.g.,* Ellen Nakashima and Mark Berman, "FBI asked San Bernardino to reset the password for shooter's phone backup," *Washington Post*, February 20, 2016, available at https://www.washingtonpost.com/world/national-security/fbi-asked-san-bernardino-to-reset-the-password-for-shooters-phone-backup/2016/02/20/21fe9684-d800-11e5-be55-2cc3c1e4b76b_story.html; "FBI Admits It Urged Change Of Apple ID Password For Terrorist's iPhone," *Buzzfeed*, February 21, 2016, available at https://www.buzzfeed.com/johnpaczkowski/apple-terrorists-appleid-passcode-changed-in-government-cust?utm_term=.myLDP1BJx#.stMkqD5Rj.

As was widely publicized, the FBI was, eventually, able to access Farook's smartphone,[15] and some have argued that its eventual success in doing so demonstrates that Apple's efforts to make mobile devices impenetrable to law enforcement should not be of concern.[16] These commentators envision a technological "arms race" between private industry and law enforcement, in which private industry makes devices that are more and more inaccessible, and the government chases after industry, straining to find more and more sophisticated ways to hack lawfully into the devices.[17] Such an arms race would ill-serve the public.

First, it would be prohibitively expensive for law enforcement. Reports estimate that third-party data extraction on the single iPhone in the San Bernardino case cost close to one million dollars.[18] Such an expenditure is simply not an option for the thousands of state and local law enforcement agencies throughout the United States.

Second, it would take too much time, and victims would suffer in the interim. The FBI's efforts to access Farook's smartphone took months, which is too long for many cases in which time is of the essence to bring criminal charges, ensure a speedy trial, locate missing persons, or determine if another attack is imminent.

Third, the hacking work is not easily replicable, so the FBI could not simply issue guidance to law enforcement agencies explaining how to hack into iPhone 5Cs, nor could it

---

15 *See, e.g.* Edvard Petterson, Alex Webb, and Chris Strohm, "U.S. Drops Apple Case After Getting Into Terrorist's iPhone," *Bloomberg,* March 28, 2016, available at https://www.bloomberg.com/news/articles/2016-03-28/u-s-drops-apple-case-after-successfully-accessing-iphone-data-imcj88xu; Katie Benner and Eric Lichtblau, "U.S. Says It Has Unlocked iPhone Without Apple," *New York Times,* March 28, 2016, available at http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0; Joel Rubin, James Queally, and Paresh Dave, "FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now," *L.A. Times,* March 28, 2016, available at http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.

16 *Id.; see also* Alex Webb, "IPhone Security Is the Casualty in Apple's Victory Over the FBI," *Bloomberg,* March 28, 2016, available at https://www.bloomberg.com/news/articles/2016-03-29/iphone-security-is-the-casualty-in-apple-s-victory-over-the-fbi.

17 *See, e.g.* Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report, "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," available at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8; Susan Landau, "Testimony for House Judiciary Committee Hearing on 'The Encryption Tightrope: Balancing Americans' Security and Privacy'," March 1, 2016, available at https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf; Berkman Center for Internet & Society at Harvard University, "Don't Panic: Making Progress on the "Going Dark" Debate," February 1, 2016, available at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

18 *See* Mark Hosenball, "FBI paid under $1 million to unlock San Bernardino iPhone: sources," *Reuters,* May 4, 2016, available at http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032.

easily open any iPhone 5Cs that come into its possession.[19] The method employed to access data on Syed Farook's iPhone in the San Bernardino case reportedly works only on Farook's particular model iPhone (5C) and the iOS version that was running on the device.[20]

Fourth, even if the FBI's work were easily replicable, it would have a relatively short "shelf life," for Apple has stated that whenever it finds a "fault" in its security it attempts to patch it to achieve the goal of impregnability.[21] Thus, the FBI's solution will work only until Apple finds and patches the flaw that allowed the FBI to view the phone's contents.

Fifth, it would be difficult to introduce "hacked" evidence at trial. Introducing into evidence data that has been obtained through hacking or other means not provided by the operating system manufacturer may be more difficult than introducing into evidence data that is obtained through a process that was designed by the smartphone manufacturer or operating system supplier, because there may be significant questions about the authenticity, integrity and completeness of the information that has been obtained through hacking. And, there may be lengthy and expensive discovery battles about the hacking method that would be avoided if the data could be extracted through a means provided by the operating system manufacturer.

B. Cases Across the Country

While terrorism cases naturally generate the lion's share of the media coverage, the impact of default device encryption is felt most profoundly on the local level, in the investigation of domestic crimes occurring every day across the U.S. The harm is experienced every day across the country, in literally over a thousand instances.

In the Manhattan District Attorney's Office alone, 423 Apple iPhones and iPads lawfully seized since October 2014 remain inaccessible due to default device encryption.[22] These devices relate to cases involving various types of crimes investigated throughout the office, ranging from cybercrime, to narcotics, to violent offenses.

---

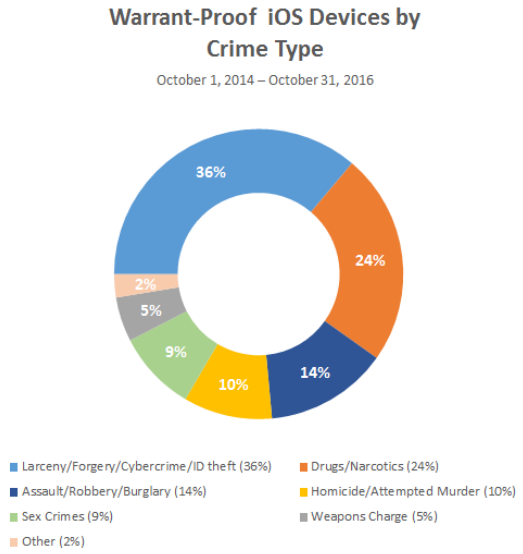
19 Many private companies that provide advanced technical services for government agencies insist on non-disclosure orders that protect the companies' intellectual property by limiting the government agency's ability to share the information or techniques developed by the private company. It is not clear whether there was such a non-disclosure agreement in place in connection with the San Bernardino matter.

20 *See e.g.* "FBI director says its hack is for iPhone 5C only; feds debate sharing method with Apple," *Associated Press,* April 7, 2016, available at http://www.latimes.com/business/technology/la-fi-tn-fbi-apple-iphone-5c-20160407-story.html; Katie Bo Williams, "FBI chief: Hack won't work on newer iPhones," *The Hill,* April 7, 2016, available at http://thehill.com/policy/cybersecurity/275483-fbi-director-iphone-hack-wont-work-on-newer-iphones.

21 *See* Testimony of Bruce Sewell for the House Judiciary Committee Hearing on 'The Encryption Tightrope: Balancing Americans' Security and Privacy'," March 1, 2016, available at https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/.

22 Manhattan District Attorney's Office statistics pertain to devices for which law enforcement obtained a search warrant and that were delivered to its High Technology Analysis Unit for processing.

SMARTPHONE ENCRYPTION STATISTICS
October 1, 2014 – October 31, 2016



Device Type	Count
iPhone 4S	1
iPhone 5	9
iPhone 5C	5
iPhone 5S	51
iPhone 6	166
iPhone 6+	66
iPhone 6S	63
iPhone 6S+	30
iPhone SE	2
iPads (various)	30
Total	**423**

Notably, approximately 10% of the impenetrable devices pertain to homicide or attempted murder cases and 9% to sex crimes. While the Manhattan District Attorney's Office has been locked out of approximately 34% of all Apple devices lawfully recovered since October 2014, that number jumped to approximately 42% of those recovered in the past three months.[23] With over 96% of all smartphones worldwide operated by either Apple or Google,[24] and as devices compatible with operating systems that predate default device encryption are becoming outdated, this trend is poised to continue.

Since the release of the Report in November 2015, law enforcement officials around the world have continued to grapple with default device encryption that inhibits or precludes their ability to perform complete and thorough investigations. Although complete statistics are not available, anecdotal evidence establishes the point:

-- The Harris County District Attorney's Office in Texas encounters between eight and ten encrypted devices every month in its criminal investigations, a significant percentage of which are associated with homicides.

-- The Suffolk County District Attorney's Office in Massachusetts has encountered 151 encrypted devices linked to a variety of criminal cases, including sex crimes, homicides, and larcenies.

---

23 For the period from August 1, 2016 through October 31, 2016.

24 *See* http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

-- Law enforcement officials in Los Angeles, California were unable to search over 300 encrypted devices linked to their criminal investigations.

-- The Wisconsin Department of Justice has 68 encrypted devices linked to criminal investigations.

These figures are almost certainly artificially low, because law enforcement agents who encounter a locked device in the field often do not have the time to make note of the device before moving on to the next investigative step.

The Manhattan District Attorney's Office, in partnership with several state and local law enforcement organizations and the National Domestic Communications Assistance Center (NDCAC), have sought to collect data from across the country about the number of impenetrable mobile devices seized by law enforcement. To that end, the partners have developed and launched an online portal, managed by NDCAC, through which law enforcement organizations can submit case-related information. In the two months since its launch, more than 30 agencies from 23 states have used the portal. As more agencies use it, a fuller understanding of the impact of smartphone encryption on state and local law enforcement will be developed.

The portal has already collected information about cases stymied or investigations curtailed by devices that cannot be unlocked, despite a court's finding of probable cause to believe the device contains evidence of a crime. For example:

-- **Louisiana:** A woman was asleep in her home when two men wearing masks and gloves and armed with hand guns climbed into a bathroom window in the home. The woman's four teenage children were also present. The suspects kicked in the woman's bedroom door, and hit her with a gun; they also duct-taped the hands and feet of two of the teenagers and assaulted them. One of the suspects was apprehended in the neighborhood a short time later, and his iPhone 6 was located nearby.

Detectives determined that the suspect had been communicating with the same three cell phone numbers immediately before and after the robbery and they believed the communications and contact list stored on the iPhone would materially advance the investigation, as the devices were likely used to plan and execute the robbery. The phone was passcode-locked, however, and the suspect was released because of insufficient evidence.

-- **Massachusetts:** A 30-year-old man was found shot to death inside his home. His locked iPhone was recovered near his body. A canvas of the area did not develop video evidence or useful witness statements. Evidence at the scene suggested that the victim may have allowed the assailant entry into his residence, and investigators believe that communications sent from the victim's iPhone leading up to the murder could shed light on the identity of his killer.

-- **Minnesota:** As part of a long-term investigation into a violent street gang, police executed multiple search warrants on gang members' residences, stash houses, and hangouts, recovering numerous iPhones, firearms and contraband. The suspects have

refused to provide officers with their passcodes and have told officers that they know law enforcement cannot get into iPhones.

-- **Missouri (Homicide):** A twenty-year-old man was shot and killed on a street while communicating from his iPhone 6. Family members have offered to sign any consent form required to allow for access to the device, but the device remains inaccessible.

-- **Missouri (Identity Theft/Fraud):** A group of suspects used compromised personal identifying information belonging to Sprint customers (account numbers, usernames and passwords, social security numbers, etc.) to go into Sprint stores and add phone lines and additional phones to the victims' accounts. One individual was arrested, and revealed that the co-conspirators he was working for would text him victims' information before he went into a store. His iPhone 6 was recovered, and one victim's information was visible on the screen. The contents of the device would almost certainly assist in identifying the co-conspirators. A warrant was issued to search the rest of the phone, but the phone's encryption prevented investigators from accessing it.

-- **New Jersey:** A victim was shot dead in his car, and a suspect was identified. The suspect's iPhone was used to send numerous messages around the time of the homicide, but police cannot read those messages, because they cannot get into the phone.

-- **Tennessee:** A victim's mother reported an aggravated sexual assault of her child by an adult suspect. The suspect had directed the victim to download the KIK messaging app so that communications between him and victim could not be traced. The victim's smartphone contained messages from the suspect, but the suspect's iPhone 5 was locked and encrypted. Based in part on the fact that defendants who engage in child exploitation are often repeat offenders, investigators believe the suspect's device would provide additional evidence of his assaults on the victim, as well as identities of additional victims.

In these cases and countless others, evidence on the locked devices can be accessed only via a search of the devices themselves. In some instances, the devices were recovered shortly after the crimes, and so communications made at or around the time of the crime would not have been backed up to cloud storage. In other cases, the use of encrypted messaging apps makes obtaining messages from the provider impossible. Only by searching the device itself can law enforcement access this critical information.

C. Alternatives to Collecting Evidence from Mobile Devices

It has been argued that impenetrable mobile device encryption does not pose a significant harm to law enforcement because we live in a "golden age of surveillance," in which there are numerous other sources of information about criminal activity.[25] The Report

[25] *See, e.g.,* Testimony of Peter Swire for the Senate Judiciary Committee Hearing on "'Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," July 8, 2015,

explained the weakness in that argument: The other sources of information may be incomplete, or unavailable to law enforcement.[26] They generally do not give as complete a picture of criminal liability, or as complete access to evidence relevant to a criminal investigation or prosecution, as would a mobile device.[27]

Furthermore, the alternatives available to law enforcement have become significantly more limited in light of the recent announcement by Facebook that it would provide an "opt-in" feature (not by default) that would permit users to encrypt messages on its platform.[28] Facebook has approximately 900 million Messenger users,[29] and its messages have frequently been useful in criminal prosecutions.[30] They may no longer be available. Facebook is thus following in the steps of app developers, including, most prominently WhatsApp, which makes end-to-end encryption available to those who download its product. WhatsApp is currently owned by Facebook[31] and has more than 1 billion users.

These developments, with doubtless more to come, show that far from it being a "golden age" for law enforcement, today's criminals have means of communication that are more secure from law enforcement's scrutiny than criminals had ever dared hope.

To the extent that there are other investigative techniques available, the "exhaustion" requirement discussed in Sections VI.D and VI.E, *infra*, would impose on law enforcement an obligation to attempt to obtain evidence from all other sources before applying for an order to extract data from a device. In other words, an extraction order would only issue after alternative methods to get the evidence proved unsuccessful.

---

available at https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.

26 *See* Report at 6 - 8.

27 *Id.*

28 *See, e.g.,* Facebook Newsroom, "Messenger Starts Testing End-to-End Encryption with Secret Conversations," July 8, 2016, available at http://newsroom.fb.com/news/2016/07/messenger-starts-testing-end-to-end-encryption-with-secret-conversations/.

29 *See* Andy Greenberg, "You Can All Finally Encrypt Facebook Messenger, So Do It," *Wired,* October 4, 2016, available at https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/.

30 *See, e.g., United States v. Browne*, 834 F.3d 403, (3d Cir. 2016); *United States v. Barnes,* 803 F.3d 209, 217-18 (5th Cir. 2015); *United States v. Brinson,* 772 F.3d 1314, 1320-21 (10th Cir. 2014).

31 Facebook Newsroom, "Facebook to Acquire WhatsApp," February 19, 2014, available at http://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp/.

II. Requiring Manufacturers or Software Designers to Retain the Ability to Extract Data Stored on Smartphones Will Not Materially Increase Users' Risks of Being Hacked

A. Apple's Method of Data Extraction Before iOS 8 Was Never Compromised

Before it adopted default device encryption in iOS 8, Apple characterized the encryption methods it employed in iOS 7 as offering the ultimate in privacy and security. Apple's May 2012 guide to "iOS Security" notes that Apple had incorporated "proven encryption methods" and "mobile-centric privacy and security technologies to ensure that iOS devices can be used with confidence in any personal or corporate environment."[32] Apple proudly stated that iOS 7 "provides solid protection against viruses, malware and other exploits that compromise the security of other platforms."[33] Before iOS 8, Apple also maintained the ability to help "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."[34]

To understand Apple's security-related reasons for adopting default device encryption – to lock itself and the government out, effectively – this Office sent Apple a letter in March 2015, that set forth a series of questions, including the following (emphasis added):

> 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?**[35]

Apple never responded to the letter.[36]

The Report, which was issued in November 2015, set forth six questions for Apple and Google, two of which were as follows (emphases added):

> Question 1
>
> In iOS 7 and prior operating systems, and in Android systems prior to Lollipop 5.0, if an attacker learned Apple's or Google's decryption process, **could [the**

---

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

33 *Id.*

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

35 *See* Report at Appendix II.

36 An almost identical letter was sent at the same time to Google, which also declined to answer.

attacker] use it to remotely attack devices or would he need possession of the device?[37]

Question 2

What technical problem does the full-disk encryption of iOS 8 and Lollipop 5.0 solve?

a. **Quantify the problem to the extent possible.** For example, if the largest security threat posed by prior systems was a hacker hacking Apple's or Google's systems to gain access to the decryption process, what are the chances of this? Has it happened before? If the largest security threat posed by prior systems was an insider improperly sharing Apple's or Google's decryption process, has this happened before? What security protocols are in place to make sure this doesn't happen? What are the chances of them being breached?

Once again, neither Apple nor Google responded.

In March 2016, Chairman of the U.S. House of Representatives Judiciary Committee Robert Goodlatte (R-Va.) provided a list of questions to an Apple representative, who testified about encryption before Rep. Goodlatte's committee.[38] Two of Representative Goodlatte's questions, and Apple's answers, were particularly important. They are as follows (emphases added):

Representative Goodlatte's Question

Why did Apple change its operating system with the iOS8 version in such a way? Presumably, it was to ensure that the phones cannot be hacked? **How many phones operating on iOS 7 or an earlier operating system were hacked?**[39]

Apple's Response

Apple **does not have data** tracking that type of information.

Representative Goodlatte's Question

[W]as the technology you possessed to decrypt these phones ever compromised?

---

37 *See* Report at Appendix II.

38 *See* Responses to Questions for the Record "The Encryption Tightrope: Balancing Americans' Security and Privacy" Bruce Sewell, Senior Vice President and General Counsel Apple, Inc., available at http://manhattanda.org/sites/default/files/Apple%20responses%20to%20QFR%203.1.16%20House%20Judiciary%20Committee%20hearing.pdf.

39 *Id.*

Apple's Response

> The process Apple used to extract data from locked iPhones running iOS 7 or earlier operating systems **was not, to our knowledge, compromised.**

The upshot of these questions, and of Apple's belated answers, is clear: There was no lack of security associated with data extraction in iOS 7. And, consequently, Apple has not demonstrated that default device encryption materially enhances users' security.

B. Smartphone Manufacturers Can Facilitate or Perform Lawful Data Extractions Without Compromising Security

As set forth below, this Office advocates enactment of a federal law that would require smartphone manufacturers and software designers whose software is used in smartphones to retain the ability to extract the information on the smartphones, if and when the manufacturer or designer receives a search warrant for that information. The proposed legislation would restore the *status quo* before Apple's iOS 8, and would be no different conceptually than legislation that requires products to be safe, buildings to be constructed with exits and egresses that satisfy specific requirements, and roads to have maximum speed limits.

Some have argued that requiring manufacturers and designers to retain the ability to extract the information on the smartphones upon receipt of a search warrant would render all users' smartphones vulnerable to hackers,[40] and it is important to see why that is not correct. To obtain the information from a person's smartphone, a hacker would need both Apple's secret means to bypass a phone's passcode *and the phone itself*. The legislation that this Office advocates would require manufacturers and designers to keep a "key" to the device encryption on smartphones. Presumably, Apple would hold the key as closely as they do any other trade secret. (That is precisely what Apple did until it introduced iOS 8.) But even if the secret means for data extraction were stolen, it is unlikely that the same sophisticated hackers would also snatch individual smartphones from unsuspecting users. As Apple's experience through iOS 7 indicates, it has not happened yet.[41]

One technologist has proposed a method that would provide secure, lawful access to phones' contents by placing the filesystem key that can decrypt data on the phone in a series of *cryptographic envelopes* that, like Russian dolls, are "nested," one envelope inside the other.[42]

---

[40] *See, e.g.,* Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report, "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," available at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8; Craig Federighi, "The FBI wants to roll back safeguards that keep us a step ahead of criminals," *Washington Post,* March 6, 2016, available at https://www.washingtonpost.com/opinions/apple-vp-the-fbi-wants-to-roll-back-safeguards-that-keep-us-a-step-ahead-of-criminals/2016/03/06/cceb0622-e3d1-11e5-a6f3-21ccdbc5f74e_story.html?utm_term=.8df63e42350f.

[41] The fact that enterprises often require access to their employees' smartphones without any suggestion that such access unacceptably degrades security shows that authorized access does not render otherwise secure systems vulnerable.

[42] *See* Matt Tait, "An Approach to Jim Comey's Technical Challenge," *Lawfare*, April 27, 2016, available at https://www.lawfareblog.com/approach-james-comeys-technical-challenge.

Different private keys would open each envelope, and therefore the filesystem key could be obtained only if each of the respective key holders for each layer in the stack unlocked "its" envelope.[43]

> Suppose, for example, we put the filesystem key in an envelope sealed with the FBI's public key, and then put that sealed envelope inside another envelope, this time sealed with the manufacturer's public key.
>
> To start with, the drive can no longer be decrypted unilaterally by the FBI. The FBI doesn't have the manufacturer's private key, it can't open the outer envelope. The drive also can't be unilaterally decrypted by the manufacturer. Although the manufacturer can open the outer envelope, only the FBI can open the inner one to retrieve the filesystem key. Decryption of the drive (at least, without knowledge of the user's password) now cryptographically requires both organizations to work with each other—all but eliminating the possibility of criminal misuse by insiders, or institutional misuse.[44]

As this proposal demonstrates, there are technological solutions at hand that would thoroughly protect people's privacy, while still allowing appropriate and authorized access in criminal investigations.[45]

III. This Problem Cannot Be Solved by the Courts

In their efforts to investigate and prosecute crime both before and after the introduction of iOS 8, federal, state, and local agencies have looked to the courts to compel the extraction of information from locked devices. In some situations, the government has attempted to order the user of a device to unlock it by entering his or her own passcode. In other cases, orders have been directed to Apple, mandating that it provide assistance to law enforcement. The resulting decisions, some of which are described below, have created a complex landscape in which judicial authority to compel decryption assistance is unclear.

A. Compelling Assistance from Users

Apple's CEO has suggested that when law enforcement officers have a court-ordered warrant to search a phone, they should be able to compel the user to unlock the phone.[46] As the Report noted, the Fifth Amendment prevents the government from ordering users to give

---

43 *Id.*

44 *Id.*

45 If Apple, for commercial or other reasons would want to prevent itself from unilaterally accessing data, then an envelope approach, of the sort described, appears technically feasible.

46 Nancy Gibbs and Lev Grossman, "Here's the Full Transcript of TIME's Interview with Apple CEO Tim Cook," *Time Magazine,* March 17, 2016, available at http://time.com/4261796/tim-cook-transcript/. ("Let's say they have a problem with you. They can come to you and say, open your phone. And one way is for it to be between the government and you. Then you can, I don't know, they could pass a law that says you have to do it, or you have to do it or there's some penalty, or something. That's for somebody else to decide. But it does seem like it should be between you and them").

up the passcodes to their own devices,[47] and Congress cannot simply "pass a law that says you have to do it."[48] It is less clear whether there is a Fifth Amendment prohibition against ordering defendants to unlock their phones for law enforcement to review (in other words, to enter the passcodes themselves), or to provide readable copies of the contents of their devices.

The constitutionality of ordering a person to unlock his device, or to provide a plaintext copy of its contents, is the subject of much debate. Even though the users are not required to give "testimony" in these scenarios, which would be prohibited by the Fifth Amendment, users may still enjoy a Fifth Amendment privilege to refuse to unlock their phones. That is because by complying with the order, a user effectively confirms the existence and authenticity of the records sought.[49] Assuming there is a Fifth Amendment privilege, the government might still be able to obtain these types of decryption orders,[50] if it can demonstrate that the evidence sought is a "foregone conclusion."[51]

But the law is unclear as to what, exactly, must be a "foregone conclusion" in order for the Fifth Amendment privilege to be overcome. Is it the existence of the *passcode*, or of *particular records* on the device? Courts have been inconsistent in their answers to this question. In one line of cases, courts have held that the government need only show that the existence of the passcode, and the user's ownership and control over it, are foregone conclusions in order to defeat the privilege.[52] On the other hand, different courts have held that to satisfy the foregone conclusion doctrine the government must demonstrate to a reasonable degree of certainty that the particular evidence it is looking for on the device exists, and is authentic.[53]

Under the latter approach, the government faces a daunting task. After all, in most cases where law enforcement officers have probable cause to believe evidence of a crime is on

---

47 *See, e.g., SEC v. Huang*, 2015 U.S. Dist. LEXIS 127853 at *3 (E.D. Pa. Sept. 23, 2015). (finding "the personal thought process defining a smartphone passcode not shared with an employer is testimonial").

48 Nancy Gibbs and Lev Grossman, "Here's the Full Transcript of TIME's Interview with Apple CEO Tim Cook," *Time Magazine,* March 17, 2016, available at http://time.com/4261796/tim-cook-transcript/.

49 *Fisher v. United States*, 425 U.S. 391, 401 (1976); *United States v. Doe*, 465 U.S. 605 (1984); *Doe v. United States*, 487 U.S. 201 (1988); *Unites States v. Hubbell*, 530 U.S. 27 (2000).

50 Orders compelling users to unlock their devices or provide plaintext versions of their contents are variously referred to as "decryption orders" and "unlock orders." We use the term "decryption order" in this paper to describe a court order mandating that a user assist law enforcement in accessing that user's data from an encrypted device.

51 *See Fisher*, 425 U.S. 391; *Doe*, 487 U.S. 201.

52 *See U.S. v. Gavegnano*, 305 Fed. Appx. 954 (4th Cir. 2009); *U.S. v. Fricosu*, 841 F.Supp.2d 1232 (D. Colo. 2012); *In re Boucher*, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009); and *Commonwealth v. Gelfgatt*, 468 Mass. 512 (2014).

53 *See U.S. v. Doe*, 670 F.3d 1335 (11th Cir. 2012); *SEC v. Huang*, 2015 U.S. Dist. LEXIS 127853 (E.D. Pa. Sept. 23, 2015); and *Comonwealth v. Baust*, 89 Va. Cir. 267 (2014). The District of Oregon has also noted that "courts are reluctant to order a defendant to decrypt an encrypted hard drive because it may implicate the defendant's Fifth Amendment right against self-incrimination." *U.S. v. Shaw*, 2016 U.S. Dist. LEXIS 25697 (Dist. OR 2016)(declining to order defendant to decrypt his hard drives where he sought their return from the government and the government had not been able to determine whether they contained child pornography, due to their encrypted state).

a device, they are unable to attest to the existence of specific files with any certainty before they search the device. In jurisdictions which adopt this approach, only in very unusual circumstances can law enforcement officers compel a user to unlock his device.

The advent of fingerprint sensors on smartphones presents another possible means for law enforcement to compel users to unlock their devices. Unlike the combinations of numbers, letters, and symbols that make up a passcode, biometric data like a fingerprint is generally not considered to be protected by the Fifth Amendment.[54] In one case, a Virginia court held that although a user's passcode was "testimonial," his fingerprint was not, and he could be compelled to unlock his phone with the fingerprint sensor (technology that Apple refers to as "Touch ID").[55] In February 2016, a court in Glendale, California signed a warrant ordering an iPhone user to unlock the device using her fingerprint.[56] And, in May 2016, the Department of Justice asked a court in Lancaster, California to issue a search warrant authorizing agents to require every person on the premises to put his or her finger on the touch sensor of his or her device.[57] All of this suggests that law enforcement may, going forward, be able to compel defendants to unlock newer-model iPhones, if users have enabled Touch ID. Of course, not every user enables this feature. Moreover, even when TouchID is enabled, iPhones require the entry of the passcode after 48 hours of inactivity, or when the device restarts.[58] And higher courts may still determine that compelled production of biometric information does implicate the Fifth Amendment.

When no other options exist, the government might try to induce a user to unlock his or her device by granting some form of immunity.[59] Of course, in most cases this isn't a

---

54 There is also no Fourth Amendment protection with respect to the "seizure" of a person's fingerprint. *See Maryland v. King,* 133 S. Ct. 1958, 1977 (2013), *United States v. Dionisio*, 410 U.S. 1 at 77-78 (1972). The Fourth Amendment does, however, prohibit the use of fingerprint evidence obtained as the result of an unlawful detention. *Davis v. Mississippi*, 394 U.S. 721 (1969); *Hayes v. Florida*, 470 U.S. 811, 816 (1985) (noting fingerprint evidence obtained as the result of unlawful, warrantless detention was inadmissible, but "a brief detention in the field for the purpose of fingerprinting" not based on probable cause may be permissible).

55 *Commonwealth v. Baust*, 89 Va. Cir. 267, 271.

56 *In the Matter of the Search of iPhone Seized from 3254 Altura Avenue in Glendale, California*, Case 2:16-mj-00398 DUTY (Central Dist. CA, Feb. 25, 2016). *See also* Kaveh Wadell, "Police Can Force You to Use Your Fingerprint to Unlock Your Phone," *The Atlantic*, May 3, 2016, available at *http://www.theatlantic.com/technology/archive/2016/05/iphone-fingerprint-search-warrant/480861*

57 *See* Thomas Fox-Brewster, "Feds Walk Into a Building, Demand Everyone's Fingerprints to Open Phones," *Forbes,* October 16, 2016, available at http://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/#5e0cd74d8d9d.

58 *See* "Use Touch ID on iPhone and iPad," available at https://support.apple.com/en-us/HT201371

59 Federal courts have determined that both use immunity and derivative use immunity are required where there is Fifth Amendment protection for the compelled disclosure. *Kastigar v. United States*, 406 U.S. 441 (1972); *Hubbell*, 530 U.S. at 38, 45; *Doe*, 670 F.3d at 1350. In New York, if disclosure was compelled in the context of a grand jury proceeding, the suspect would be granted transactional immunity. *See* Criminal Procedure Law §190.40. If the compelled disclosure took place outside of a grand jury proceeding, the suspect may be entitled only to use immunity. *See, e.g., Brockway v. Monroe*, 59 N.Y.2d 179, 181 (1983).

desirable alternative, because it precludes the government from using any of the information in a prosecution against the suspect – in many cases, the information would be useless.

Finally, electronic privacy advocates have argued that decryption orders are fundamentally different from orders to produce other types of documents, because they technically require the defendant to create files that do not exist at the time of the order.[60] They note that encrypted information on a computer or other device exists only in its encrypted format, and that when the government has the encrypted device, it has everything that the user has – it just can't read it without assistance. Unlike an order to hand over the key to a safe, a decryption order essentially requires the user to create a new, plaintext, version of the information.[61] The only court to consider this argument in the context of a decryption order, the Third Circuit Court of Appeals, has yet to render a decision.[62]

B. Compelling Assistance from Apple

Even if clear judicial authority to compel a user to unlock his own device existed, it would be insufficient to meet the investigative needs of law enforcement. In many cases, the user of a recovered device is unknown. In other cases, the user is known but unavailable; the user could be the victim of a homicide or a kidnapping, for example. A user may also opt to violate a court order and be held in contempt rather than provide evidence of a more serious crime.

In the past, as discussed in the Report, law enforcement often sought assistance from Apple in extracting data from encrypted iPhones after a court-ordered search warrant had been obtained. Apple routinely complied with these requests, provided (i) the device was running a pre-iOS 8 operating system and (ii) the requests used specific language that Apple considered sufficient to establish the requisite legal authority. Then, without explanation, Apple changed its position and refused to comply with court-issued extraction orders, regardless of the operating system running on the device. Today, based on at least one recent judicial decision and a highly-publicized court battle, law enforcement's ability to obtain assistance from Apple (and other providers) is much less certain.

On October 8, 2015, the U.S. government filed an application asking a magistrate judge in the Eastern District of New York to issue an order[63] requiring Apple to assist in the

---

60 *See*, *e.g.*, *U.S. v. Apple MacBook Pro Computer*, 3d Cir. Case No. 2:15-mj-00850-001, Brief of *Amici Curiae* Electronic Frontier Foundation and American Civil Liberties Union in Support of Movant-Appellant and Reversal, April 6, 2016.

61 *Id., citing* Jeffrey Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment*, 24 B.U. Pub. Int. L.J. 53, 77 (2015).

62 In the case pending before the Third Circuit, a magistrate judge signed an order compelling a defendant to unlock his encrypted devices to enable law enforcement to search them. The defendant initially agreed, and "attempted" to enter his passcodes in the presence of law enforcement. It was determined that the defendant was not being truthful when he said he had forgotten his passcodes, and he was held in contempt. He then appealed the magistrate judge's decryption order. *U.S. v. Apple MacBook Pro Computer*, 3d Cir. Case No. 2:15-mj-00850-001.

63 The government cited the All Writs Act as the authority for issuing the order. 18 U.S.C. §1651. The All Writs Act has been routinely used by the federal government to seek and obtain the

execution of a search warrant on a lawfully-seized Apple device.[64] The judge declined to issue the order, and instead asked Apple to respond in writing and state (i) whether compliance with the order would be "technically feasible," and (ii) if so, whether it would be "unduly burdensome."[65]

Apple responded on October 19, 2015, stating that although it could probably technically comply with the proposed order, compliance would be "unduly burdensome." Apple claimed that although an individual request to extract data from a single phone would not be particularly costly or time-intensive, the burden to Apple increases with each government request, resulting in significant expenditure of time and resources.[66] Apple also noted that compliance with the court order could "substantially tarnish Apple's brand."[67]

Ultimately, the judge denied the government's request, finding that the government lacked the legal authority to seek this kind of order.[68] He also observed that the record was unclear as to whether Apple's assistance was absolutely necessary, based on the availability of "private sources" who might be able to assist with extracting the sought data.[69] This portion of the opinion might be read to require an "exhaustion" showing by the government, which is what is required when the government seeks court-ordered eavesdropping.[70] The judge ended his opinion by urging Congress and other legislators to take action: "that debate must happen today, and it must take place among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive."[71]

---

type of orders to Apple described above, which ordered Apple to assist in the extraction of data pursuant to a search warrant. State law enforcement agencies have also sought, and obtained, similar orders, citing various state and federal provisions. But given Apple's position in the Eastern District litigation, it is unlikely it would be responsive, going forward, to any state court order requiring the same type of assistance. Additionally, if this issue were left solely to state legislatures to address, legal authority to compel assistance could vary significantly from state to state, resulting in potentially different or even inconsistent approaches across the country.

64 *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, 2015 U.S. Dist. LEXIS 138775 (E.D.N.Y. 2015).

65 *Id.* at 1.

66 *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, Case No. 1:15-mc-01902, Apple Inc.'s Response to Court's October 9, 2015 Memorandum and Order (E.D.N.Y. 2015).

67 *Id.* at 4. In connection with the San Bernardino assistance order, discussed below, Apple posted on its website a document entitled "Answers to Your Questions About Apple and Security." In that document, Apple claimed that its refusal to comply with government orders was "absolutely not" related to marketing or business strategy concerns. Available at http://www.apple.com/customer-letter/answers.

68 *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, 149 F.Supp.3d 341, 354-360 (E.D.N.Y. 2016).

69 *Id.* at 373.

70 *See*, *e.g.,* 18 U.S.C. § 2518; N.Y.C.P.L. § 700.20(d).

71 *Id.* at 376.

Around the same time (and as discussed above), in February 2016, Apple refused to comply with an order[72] from a federal magistrate judge in California which directed it to help the government access the contents of an iPhone used by one of the perpetrators of the San Bernardino mass shooting.[73] In that case, rather than ordering Apple to extract data from the phone, the court instructed Apple to create and upload an operating system that would disable the feature on the target phone that prevented "brute force" attacks. As discussed in the Report, and elsewhere, a "brute force" attack is one in which someone gains access to a password-protected device simply by trying one passcode after another until the correct passcode is determined. Apple's devices protect against these attacks by erasing all of their contents, or by preventing additional attempts, after ten incorrect password attempts. Disabling that security feature would allow law enforcement officers to use software to guess various passcodes, ultimately gaining access to the phone (although potentially after a very lengthy process).

Apple's response, in the form of a letter posted to its website, gave a laundry list of possible implications of the order, suggesting that law enforcement would "extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge."[74] FBI Director James Comey responded by posting his own letter on the FBI's website, urging the public to resist the doomsday scenario offered by Apple and clarifying that the FBI's request was narrow in scope.[75]

Ultimately, the government withdrew its request for the order, stating that a third party had been able to decrypt the contents of the phone. While the FBI declined to publicize the third party's identity or the specific methods it used, Director Comey revealed that the process was costly and unlikely to be successful on newer iPhones.[76] So, while the passcode bypass technology may have been useful in a case involving terrorism and an older-model iPhone, it is not likely to be a solution to the problem going forward.

Two further points deserve mention. First, most of the litigation seeking to compel Apple to open mobile devices has been federal, and one of the key questions has been whether the federal courts have authority under the All Writs Act[77] to issue orders compelling Apple to devise a means to unlock, or assist in government efforts to unlock, a particular mobile

---

72 *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, Order Compelling Apple, Inc. to Assist Agents in Search, Case No. ED 15-041M (Central Dist. CA, February 16, 2016).

73 *See* Tim Cook, "A Message to Our Customers," February 16, 2016, available at http://www.apple.com/customer-letter.

74 *Id.* It is worth noting that all of these activities would require prior judicial authorization.

75 James Comey, "FBI Director Comments on the San Bernardino Matter," February 21, 2016, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter.

76 *See* Devin Bartlett, "FBI Paid More Than $1 Million to Hack San Bernardino Phone," *Wall Street Journal*, April 21, 2016, available at http://www.wsj.com/articles/comey-fbi-paid-more-than-1-million-to-hack-san-bernardino-iphone-1461266641.

77 28 U.S.C. § 1651.

device. State courts' authority would not derive from the All Writs Act, but from particular statutory or constitutional provisions, or common law principles, in each state. Some state courts might have authority that is greater than the All Writs Act gives to federal courts. (Of course, others might have less authority than federal courts.) There is reason to believe that Apple would oppose these orders. New York's Judiciary Law § 2(b) provides that courts may "devise and make new process and forms of proceedings, necessary to carry into effect the powers and jurisdiction possessed" by them.[78] Apple used to comply with decryption orders citing Judiciary Law § 2(b), but it ceased complying with such orders after the Eastern District litigation described above, even though that litigation did not touch on whether New York State law provided authority for state courts to issue these orders.

Second, rather than seeking an order to compel Apple to unlock a locked mobile device, or to decrypt the contents of such a device, prosecutors might seek a grand jury subpoena compelling Apple to provide extant documents or materials containing the technical information (*e.g.,* source code, signing key) that could be used by the government's technical experts to devise means to unlock the device or decrypt its contents. With that information, and with appropriate engineering advice and expertise, the government might be able to unlock mobile devices. There are no reported instances of such grand jury subpoenas, but, given the secrecy of grand jury proceedings, it is impossible to say whether or not such subpoenas have been issued.

IV. Legislative Attempts to Address the Encryption Problem Have Stalled

A. Federal Bills

There are currently two legislative proposals in Congress that seek to address the encryption and public safety issue. Only one of these, the Digital Security Commission Act, has been formally introduced.

1. Digital Security Commission Act

House Homeland Security Committee Chairman Michael McCaul (R-Texas) and Senator Mark Warner (D-VA) introduced the Digital Security Commission Act of 2016 on February, 29, 2016. The bill establishes a National Commission on Security and Technology Challenges in the legislative branch to examine "the intersection of security and digital security and communications technology in a systematic, holistic way."[79] The Commission would be composed of eight members appointed by the Speaker of the House and Senate Majority Leader, eight members appointed by the House Minority Leader and the Senate Minority Leader, and one member appointed by the President to serve as an *ex officio*, non-voting member. Individuals appointed to the Commission must have relevant experience in the following fields: cryptography, global commerce and economics, federal law enforcement, state and local law enforcement, consumer-facing technology sector, enterprise technology

---

78 NY CLS Jud. § 2-b. This statute was enacted in 1963.

79 Digital Security Commission Act of 2016, S. 2604, 114th Cong. (2016), available at https://www.congress.gov/bill/114th-congress/senate-bill/2604/text; H.R. 4651, 114th Cong. (2016), available at https://www.congress.gov/bill/114th-congress/house-bill/4651/text.

sector, the intelligence community, and the privacy and civil liberties community. The Commission would provide several interim reports, and a final report, all of which would be unclassified (but could include classified annexes). The preliminary report would be required to be submitted no later than six months after the Commission's initial meeting, and to include "an outline of the activities of the Commission to date, a plan of action moving forward, and any initial findings." The Commission's final report would be submitted to the specified congressional entities no later than twelve months after the Commission's initial meeting. The findings, conclusions, and recommendations included in the reports would have to be agreed to by at least twelve of the sixteen voting members.

The Act was referred to the House Homeland Security Committee Subcommittee on Crime, Terrorism, Homeland Security, and Investigations and the Senate Homeland Security and Government Affairs Committee.

The proposal has garnered bipartisan support in the Senate and the House. However, it has been criticized by a number of civil liberties groups and technical experts, including the American Civil Liberties Union and the Electronic Frontier Foundation.[80] Such groups have criticized its "overly broad mission," the makeup of the Commission, the subpoena power of its members, and the redundancy of convening yet another group to prolong the encryption conversation.

2. Compliance with Court Orders Act of 2016

A second proposal has been promoted by Senators Richard Burr (R-NC) and Dianne Feinstein (D-CA), both members of the Senate Select Committee on Intelligence. A discussion draft of the "Compliance with Court Orders Act of 2016" (CCOA) was circulated in April 2016, but the bill has yet to be formally introduced.[81]

The bill was drafted in the aftermath of the San Bernardino terrorist attack, and in response to Apple's repeated refusals to assist law enforcement despite the existence of court orders requiring them to do so. It would require covered entities to "provide responsive, intelligible information or data, or appropriate technical assistance to a government pursuant to a court order."[82] "Covered entities," as defined in the discussion draft, include device manufacturers, software manufacturers, electronic communication services, remote computing services, and persons or entities that are providers of such services.[83] Under the bill, court orders could issue in connection with the prosecution or investigation of only

---

80 *See, e.g.,* Neema Singh Guliani, ACLU Legislative Counsel, "4 Problems with Creating a 'Commission on Encryption,'" March 9, 2016, available at https://www.aclu.org/blog/washington-markup/4-problems-creating-commission-encryption; Mark Jaycox, "EFF Opposes McCaul-Warner Encryption Commission," March 7, 2016, available at https://www.eff.org/deeplinks/2016/03/eff-opposes-mccaul-warner-encryption-commission.

81 A discussion draft of the bill was made available to the public in a press release issued by Senator Dianne Feinstein on April 13, 2016, available at http://www.feinstein.senate.gov/public/index.cfm?a=files.serve&File_id=5B990532-CC7F-427F-9942-559E73EB8BFB.

82 *Id.*

83 *Id.*

certain, particularly serious crimes.[84] The bill also includes a provision for the covered entities to receive compensation for "such costs as are reasonably necessary and which have been directly incurred in providing such technical assistance or such data in an intelligible format."[85]

The draft bill has failed to gain support from within Congress, and has been criticized by a number of individuals and groups.[86] Senators Burr and Feinstein have since been soliciting input from the public and key stakeholders.

B. State Bills

Three bills have been introduced at the state level to address the sale of smartphones and similar devices equipped with warrant-proof encryption.

New York: Assembly Bill A.8093A was introduced in 2015 in the New York State Assembly by Assemblyman Matthew Titone.[87] The bill amends the New York general business law to require that any smartphone sold or leased in New York be "capable of being decrypted and unlocked by its manufacturer or its operating system provider."[88] Any seller or lessor that sells a smartphone that is not capable of being decrypted and unlocked by its manufacturer or operating system provider would be subject to a civil penalty of $2,500 per smartphone if it can be demonstrated that the seller "knew at the time of the sale or lease that the smartphone was not capable of being decrypted and unlocked."[89] The bill provided that it could be enforced by either the district attorney in the county in which the sale or lease occurred, or by the State Attorney General.[90]

---

84 *Id.* The draft legislation lists the following crimes as ones for which a court order may issue:
- (A) a crime resulting in death or serious bodily harm or a threat of death or serious bodily harm;
- (B) foreign intelligence, espionage, and terrorism, including an offense listed in chapter 113B of title 18, United States Code;
- (C) a Federal crime against a minor, including sexual exploitation and threats to physical safety;
- (D) a serious violent felony (as defined in section 3559 of title 18, United States Code);
- (E) a serious Federal drug crime, including the offense of continuing criminal enterprise described in section 408 of the Controlled Substances Act (21 U.S.C. 848); or
- (F) State crimes equivalent to those in subparagraphs (A), (B), (C), (D), and (E).

85 *Id.*

86 *See, e.g.,* Tweet by Senator Ron Wyden (D-OR), Apr. 13, 2016, available at https://twitter.com/ronwyden/status/720344113279840256; Internet Association, "Statement on the Compliance with Court Orders Act of 2016," April 11, 2016, available at https://internetassociation.org/041116encryption/; Andy Greenberg, "The Senate's Draft Encryption Bill is 'Ludicrous, Dangerous, Technically Illiterate," *Wired*, April 8, 2016, available at https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/.

87 Assembly Bill A.8093A (N.Y. 2016), available at http://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A08093&term=2015&Summary=Y&Text=Y.

88 *Id.*

89 *Id.*

90 *Id.*

The bill was re-introduced in 2016, was recommitted to the Committee on Consumer Affairs and Protection, and has three Democratic co-sponsors in the Assembly.

California: Assembly Bill 1681 was introduced in the California State Assembly in January 2016 by Assemblyman Jim Cooper. The bill's preamble stated that smartphones are a "weapon of choice" for "criminals and criminal organizations involved in human trafficking and sexual exploitation of children."[91] In its original form, the bill was in all relevant respects the same as the New York bill just discussed: It imposed a civil penalty of $2,500 per phone upon sellers or lessors who sold or leased a smartphone that was not capable of being decrypted or unlocked by its manufacturer or its operating system provider.[92]

The bill was amended in March 2016, however, so that it changed its focus from sellers and lessors to technology companies. As amended, the bill imposes a penalty of $2,500 on manufacturers or operating system providers of smartphones for each instance in which the manufacturer or operating system provider is unable to be decrypt the contents of the smartphone pursuant to a state court order.[93] The amended bill prohibits any manufacturer or operating system provider who pays the civil penalty from passing on any portion of it to smartphone purchasers.[94]

The amended California bill, unlike its original version or the New York bill, does not impose penalties on sellers and lessors of encrypted smartphones. Instead, as noted above, it imposes penalties on the manufacturers and operating system providers. This means that California would have the authority to penalize Apple and Google, the entities that are directly responsible for default device encryption on smartphones. And rather than imposing penalties for each impenetrable smartphone sold or leased, the amended California bill only imposes penalties for each instance in which a smartphone cannot be decrypted pursuant to a court order. Therefore, the amended bill – as compared to its original version and the New York bill – would authorize authorities to seek the civil penalty in far fewer instances.

The bill as amended died in the Committee on Privacy and Consumer Protection in April 2016,[95] and as of this writing, it is unclear whether it will be re-introduced in the Assembly.

Louisiana: Louisiana's bill was introduced in light of a particularly dramatic example of the harm to public safety that is caused by impenetrable smartphones. The bill, House Bill 1040, also called the "Louisiana Brittney Mills Act," was introduced by Representative Ted James (D-Baton Rouge) in April 2016. It was inspired by the case of Brittney Mills, who was

---

91 Assembly Bill No. 1681 (Cal. 2016), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1681.

92 *See* California Assembly Bill No. 1681 as introduced on January 20, 2016, available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1681.

93 *See* California Assembly Bill No. 1681 as amended on March 28, 2016, available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1681.

94 *See id.*

95 *See* Jeremy B. White, "California phone decryption bill defeated," *Sacramento Bee,* Apr. 12, 2016, available at http://www.sacbee.com/news/politics-government/capitol-alert/article71446037.html.

killed in April 2015 at age 29. Mills was eight-months pregnant at the time of the murder, and her child, born on the day of Ms. Mills' death, died seven days later. Her locked iPhone was found at the scene of the murder, and police had information that led them to believe that the smartphone contained information that might identify her killer. The police have still not been able to unlock the phone, however, and her case remains unsolved.

The bill would require that any smartphone sold at a retail location or delivered to a consumer within the state of Louisiana be "capable of being decrypted and unlocked by either its manufacturer or its operating system provider without the necessity of obtaining the user passcode."[96] Like the New York bill, the Louisiana bill imposes a $2,500 civil penalty on the sellers or lessors of impenetrable smartphones.[97] The bill empowers the Attorney General to seek the civil penalty, and further provides that the Attorney General *must* seek the penalty "when the user of the smart phone, which is incapable of being decrypted and unlocked by either its manufacturer or its operating system provider, is the victim of a homicide."[98]

The motion to pass the bill failed with a tie vote of 6-6. The legislators who opposed the measure cited cost concerns and asserted that federal legislation was preferable to individual state laws.[99] According to media reports, representatives from mobile service carriers – including Verizon, AT&T, and Sprint – also objected to the measure.[100] Representative James asked to defer the bill voluntarily, with plans to re-introduce it later in the session.

The New York and Louisiana bills provide that the seller, lessor, manufacturer, and operating system designer would not be liable if a third party – typically, an app developer – is responsible for the impregnability of the smartphone.

V. Foreign Nations' Efforts to Address the Encryption Problem Have Been Inconsistent

As has often been noted, encryption is used around the world, and it can pose a problem for law enforcement worldwide. Other nations, often spurred by terrorist activity within their borders or by the fear of such activity, have taken steps to address the encryption problem. They have done so in one or both of two ways.

---

96 *See* House Bill 1040 (La. 2016), available at http://www.legis.la.gov/legis/BillInfo.aspx?&i=230315.

97 *See id.*

98 *Id.*

99 *See* Kevin Frey, "Brittney Mills Act fails to pass in La. House committee," *WAFB,* May 3, 2016, available at http://www.wafb.com/story/31866353/brittney-mills-act-fails-to-pass-in-la-house-committee.

100 *Id.; see also* Associated Press, "Louisiana lawmaker shelves bill to give police access to locked phones," *Baton Rouge Advocate,* May 3, 2016, available at http://www.theadvocate.com/baton_rouge/news/politics/legislature/article_bc5ea2e0-57e0-5ab6-8181-3051e2c66834.html.

A. Legislation Authorizing Law Enforcement to Compel Individuals to Provide Their Passcodes Under Appropriate Circumstances

At least two nations, the United Kingdom and Singapore, have enacted legislation that would make it a crime punishable by up to five years' imprisonment for a person to withhold her or his passcode from the government. The British legislation, the Regulation of Investigatory Powers Act, provides that law enforcement can compel an individual (including a suspect or defendant) to disclose encryption keys or to decrypt encrypted data if it is found that disclosure is necessary in the interests of national security, for the purpose of preventing or detecting crime, or in the interests of the economic well-being of the United Kingdom. An individual's refusal to comply with this order may result in a five-year prison sentence in cases relating to national security or child indecency, and a two-year prison sentence in all other cases.[101]

Under Singapore's Criminal Procedure Code, a law enforcement officer can "require any person whom he reasonably suspects to be in possession of any decryption information to grant him access to such information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence."[102] If the defendant refuses to comply with this order, he can face a fine of up to $10,000, up to three years in prison, or both.[103]

Legislation like that passed in Britain and Singapore would almost certainly be unconstitutional in the United States, as it would violate the Fifth Amendment's prohibition against self-incrimination.[104]

B. Legislation Requiring Technology Companies to Retain the Ability to Decrypt Material on Smartphones Under Appropriate Circumstances

Several nations have enacted legislation, or are considering legislation, that would require technology companies to retain the ability to decrypt material on smartphones under appropriate circumstances. This is, of course, what is contemplated in the CCOA, described above,[105] and it is what this Office proposes, as set forth below.[106]

1. United Kingdom

In March 2015, Her Majesty's Government introduced an amendment to the Investigatory Powers law, which clarifies and codifies existing powers, such as interception of targeted data and communications, and hacking, and creates one new power – bulk collection of metadata. It also establishes a new judicial oversight committee. Notably, the bill maintains a requirement on Communications Service Providers (CSPs) in the UK to have the ability to

---

101 The Regulation of Investigatory Powers Act of 2000, Chapter 23, Part III, § 4956 (United Kingdom).

102 Criminal Procedure Code, Chapter 68, §§ 40(1) and 40(2)(c) (Singapore).

103 Criminal Procedure Code, Chapter 68, § 40(3) (Singapore).

104 *See supra* at 16 - 17.

105 *See supra* at 23 - 24.

106 *See infra* at 32 - 33.

remove encryption applied by the CSP. This bill makes it clear that companies can be asked to remove only encryption that they themselves have put in place, and only if doing so is technically feasible and not unduly expensive. A company ordered to break encryption can appeal to the Secretary of State that doing so would pose a prohibitively costly or otherwise damaging challenge. The act applies only to domestic companies; foreign companies will not be required to remove encryption.

The House of Commons passed the bill shortly after its introduction, and the House of Lords is currently debating it.

2. France

French legislators are debating a bill that would punish technology companies who refuse to decrypt messages for law enforcement in terrorism-related cases. Company executives would face up to five years in jail and a €350,000 fine.[107]

3. The Netherlands

In July 2015, the Dutch government released for public comment a proposed bill updating the country's Intelligence & Security Act of 2002, which would authorize intelligence agencies to compel assistance with decryption of data. However, in January 2016, the Dutch government announced that it would not require technology companies to share encrypted communications with security agencies.[108]

4. The European Union

In August 2016, France and Germany called on the European Union to adopt a European-wide law requiring technology companies to provide law enforcement agencies with access to encrypted messages.[109] The countries' joint proposal stated that "[e]ncrypted communications among terrorists constitute a challenge during investigations. Solutions must be found to enable effective investigation… while at the same time protecting the digital privacy of citizens by ensuring the availability of strong encryption."[110]

---

107 "French parliament votes to penalise smartphone makers over encryption," *The Guardian,* March 3, 2016, available at https://www.theguardian.com/technology/2016/mar/03/french-parliament-penalise-smartphone-makers-over-encryption.

108 "Dutch Government Says No to 'Encryption Backdoors," *BBC*, January 7, 2016, available at http://www.bbc.com/news/technology-35251429.

109 *See* Katie Bo Williams, "France, Germany Push for Encryption Limits," *The Hill*, August 23, 2016, available at http://thehill.com/policy/cybersecurity/292330-france-germany-push-for-encryption-limits.

110 Quoted in *id.*

VI. We Need Federal Legislation

There is an urgent need for federal legislation that would compel software and hardware companies that design or build mobile devices or operating systems to make such devices amenable to appropriate searches.[111] While people certainly have a right to privacy in the contents of their mobile devices, that right should be protected in the same way that peoples' right to privacy – in their homes, their papers, and their effects – has been protected ever since the Bill of Rights was adopted: by the warrant requirement of the Fourth Amendment.[112] In other sectors, Congress has recognized the need for law enforcement to be able to obtain certain data with proper authorization, and has enacted legislation to ensure that companies can comply with lawful requests for information.[113] And, as the Report argued, federal legislation is strongly preferable to state legislation, given the broad market for, and portability of, mobile devices.[114]

---

111 Crime victims and their advocates have been particularly emphatic about the need for such legislation. *See, e.g.,* statement of Dr. Tia T. Mills, sister of homicide victim Brittney Mills and aunt of 8-day-old homicide victim Brenton Mills, Manhattan District Attorney's Office, April 18, 2016 (http://manhattanda.org/press-release/district-attorney-vance-nypd-crime-victims%E2%80%99-advocates-call-congress-unlockjustice) ("It hurts us every day to know that the identity of my sister's killer remains sitting inside a phone in an evidence room. As a family, we call on our elected leaders to pass comprehensive legislation to allow law enforcement access to valuable information. We ask this for victims' families like ours, who live in pain every day. We owe this fight to my sister and nephew, and for all of our nation's victims and their family members, as well"); statement of Ernie Allen, Founding Chairman and former President and CEO of the National Center for Missing & Exploited Children, id. ("We need to find the right balance"); statement of Joyful Heart Foundation Managing Director Sarah Haacke Byrd, id. ("Leaders, including policymakers, law enforcement, victim advocates, and survivors, must come together to work with technology companies to ensure that law enforcement has the necessary tools at its disposal to fully investigate crimes and to hold violent offenders accountable. Jointly we must examine how current encryption policies, while attempting to preserve privacy, may be diminishing the ability of law enforcement from doing all that they can to seek justice for victims of sexual assault, domestic violence and child abuse, and provide some level of closure for their families").

112 *See* Report at 15.

113 *See, e.g.,* Sarbanes Oxley Act, Pub. L. 107-204, 116 Stat. 745 (2002)(requiring, inter alia, accountants to retain audit records for 5 years, and criminalizing the destruction of documents after a government request has been made); Securities and Exchange Commission, 17 CFR Part 210 (requiring retention of audit documents for a period of 7 years); Occupational Safety and Health Administration, 29 CFR Part 71.8 (requiring indefinite retention of correspondence related to certain complaints); Department of Health and Human Services, 45 CFR Part 160, Subpart C (requiring indefinite retention of certain records relating to protected healthcare information); Federal Energy Regulatory Commission, 18 CFR Part 225.3 (requiring retention periods of 4, 5, 6, 10, and 25 years for various records maintained by natural gas companies); US Equal Employment Opportunity Commission, 29 CFR Part 1602 (requiring private employers to retain employment records for one year, and public employers to retain such records for two years); Federal Communications Commission, 47 CFR Part 2.938 (requiring retention of certain records relating to communications equipment for one to two years).

114 *See* Report at 13.

A. Doing Nothing Will Lead to an Untenable Arms Race

As discussed above, some technology experts and privacy advocates have opposed any legislation, arguing that a technological "arms race" between private industry and the government will lead to a socially optimal result.[115] In the words of one technology expert, the government should "develop twenty-first century capabilities for conducting investigations," rather than seek assistance from the device manufacturers, operating system designers, or other private entities.[116]

For the reasons already stated, these experts and critics are incorrect, for such an arms race would not adequately address the specific needs of state and local law enforcement agencies. The majority of these agencies do not have the resources to train, let alone hire, staff members to "lawfully hack" these devices; thus, any expectation that agencies could build their own in-house cyber labs is unrealistic. Nor do these agencies have the resources to pay outside vendors to perform data extractions and analysis on each lawfully-seized device. Furthermore, this argument assumes that these labs will be able to develop the capabilities necessary to extract data from the newest devices, but even today's top cryptographic experts cannot extract the contents of the latest iPhones, and appear to be several iPhone models behind Apple.

B. State Legislation is Inadequate

Although the proposed state legislation described above would be useful if enacted, it is plain that impenetrable encryption of mobile devices is a national problem that requires a national solution. Mobile devices can be purchased in one state, and easily taken into another. If one state (like New York or Louisiana) threatens sellers of smartphones with criminal liability, then the sellers in neighboring states (like New Jersey or Mississippi) will simply take up the slack and sell the phones that New York's or Louisiana's smartphone dealers cannot. And even California's proposed legislation, which imposes a penalty on smartphone manufacturers whose smartphones are impenetrable, cannot fully address the problem, because the penalties contemplated by the legislation are so small that they would likely add up to no more than a few thousand dollars per year for these extraordinarily large entities.[117]

---

115 *See, e.g.,* Report by the Chertoff Group, "The Ground Truth About Encryption And The Consequences Of Extraordinary Access," available at https://chertoffgroup.com/files/238024-282765.groundtruth.pdf; Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report, "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," available at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8; Susan Landau, "The real security issues of the iPhone case," available at http://science.sciencemag.org/content/352/6292/1398.

116 *See* Susan Landau, "Testimony for House Judiciary Committee Hearing on 'The Encryption Tightrope: Balancing Americans' Security and Privacy'," March 1, 2016, available at https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf.

117 Some commentators have suggested that a state bill would violate the "dormant commerce clause." *See, e.g.,* Cyrus Farivar, "Yet Another Bill Seeks to Weaken Encryption-by-Default on Smartphones," *Ars Technica,* January 21, 2016, available at http://arstechnica.com/tech-

C. The Digital Security Commission Act is Inadequate

The Digital Security Commission Act of 2016 does not propose a solution to the public safety problems posed by default device encryption. Rather, it proposes a bipartisan commission to study the problems and make recommendations. However, this issue has been researched, written about, and publicly considered for more than two years, and therefore it is unlikely such a commission would arrive at solutions that have not already been proposed. Furthermore, as the District Attorney's Office previously stated with regard to this Act, the work of the proposed commission should be completed in 90 days, "so there is no unwarranted delay. Time is not a luxury that state and local law enforcement, crime victims, and communities can afford."[118]

D. The Compliance with Court Orders Act is a Reasonable Response to Our Current Situation

The Compliance with Court Orders Act (CCOA), by contrast, would require various entities to provide intelligible information or data, or technical assistance, to a government pursuant to a court order issued in connection with the prosecution or investigation of certain, particularly serious, crimes, set forth in Section 4(3) of the bill. This Office supports this proposed bill, and believes that it would appropriately reset the balance between privacy and security that prevailed prior to late-2014, when Apple introduced default device encryption.

The list of offenses covered by the CCOA is, however, defective, because it omits a number of serious crimes, and so would not provide law enforcement with access to critical evidence in investigating those crimes. It does not include, for example, sex trafficking and certain other sex offenses, as well as serious domestic violence offenses. A better list is readily at-hand: Title 18 U.S.C. § 2516 – the federal statute authorizing judges to approve the interception of wire, oral, or electronic communications – sets forth a list of crimes for which wiretaps may be used. The same list could and should be used in the CCOA.[119]

This Office would also support a bill like the CCOA that included an exhaustion requirement modeled on the exhaustion requirement set forth in the federal Title III wiretapping statute.[120] That statute requires an applicant for a wiretap order to provide a sworn, "full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[121] Requiring law enforcement to try other methods that are feasible under

---

policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones/. We believe, however, that any such bill would be within the state's authority and would not violate the Constitution. *See generally Maryland Commission on Taxation v. Wynne*, 135 S. Ct. 1787 (2015).

118 Statement by Manhattan District Attorney Cyrus R. Vance Jr., on Apple-Supported Congressional Commission to Study Encryption," Feb. 23, 2016.

119 This position has been articulated to the drafters of the proposed bill in a letter to Senator Feinstein sent by this Office on April 13, 2016, available at http://manhattanda.org/sites/default/files/4.13.16%20feinstein%20letter.pdf.

120 18 U.S.C. § 2518

121 *Id.* at § 2518(1)(c).

the circumstances of the particular case to gather information before being permitted to obtain an order to gain access to a person's mobile device would be a reasonable step to address the legitimate concerns of critics.

E. The Manhattan District Attorney's Proposed Bill is a Reasonable Response to Our Current Situation

This Office has also drafted proposed legislation that would address the problem of impenetrable mobile devices. Our proposed legislation would require those who design operating systems to do so in a way that would permit law enforcement agents with a search warrant to gain access to the mobile devices. Specifically, it is as follows:[122]

(a) Capability Requirements

A designer of an operating system used on smartphones or tablets manufactured, leased, or sold in the United States shall ensure that the data on any such smartphone or tablet using the designer's operating system is capable of being accessed by the designer in unencrypted form pursuant to a search warrant or other lawful authorization when the designer is in possession of the smartphone or tablet.

(b) Limitations

1. Design of system configurations

This chapter does not authorize any law enforcement agency or officer:

a. to require any specific design of operating systems to be adopted by any designer of operating systems; or

b. to prohibit the adoption of any specific design of operating systems by any designer of operating systems.

2. Third-Party Encryption

An operating system designer shall not be responsible for decrypting, or ensuring the government's ability to decrypt, data encrypted by a user, unless the encryption used was part of the design of the operating system.

As with respect to the CCOA, it may be appropriate to include an exhaustion requirement so that government can gain access to a mobile device only as a last resort. The proposed legislation could also be adapted to provide that search warrants or other legal process could issue only in connection with investigations or prosecutions of certain crimes, and the list of such crimes could be taken from the analogous list in CCOA.

---

122 This proposal has been submitted as part of District Attorney Vance's testimony before the Senate Armed Services and House Judiciary Committees.

VII. Conclusion

Default device encryption poses a severe threat to our safety. To respond to the threat by ignoring it, or hurling bromides ("Privacy," "Security") as if they resolved matters, would be ill-advised. The genius of our legal system has been its ability to adapt to change, including technological change. With default device encryption, the legal system is faced with a technological change, just as it was with the advents of automobiles and telephones. As it did with respect to those technologies, the legal system must respond. The proposals set forth in this report outline ways that it may do so.