



**REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE
ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY**

November 2015

Foreword

Most people today live their lives on smartphones, and, in this regard at least, criminals are no different. While in the past criminals may have kept evidence of their crimes in file cabinets, closets, and safes, today that evidence is more often found on smartphones. Photos and videos of child sexual assault; text messages between sex traffickers and their customers; even a video of a murder victim being shot to death – these are just a few of the pieces of evidence found on smartphones and used to prosecute people committing horrific crimes.

Last fall, a decision by a single company changed the way those of us in law enforcement work to keep the public safe and bring justice to victims and their families. In September 2014, Apple Inc. announced that its new operating system for smartphones and tablets would employ, by default, what is commonly referred to as “full-disk encryption,” making data on its devices completely inaccessible without a passcode. Shortly thereafter, Google Inc. announced that it would do the same.

Apple’s and Google’s decisions to enable full-disk encryption by default on smartphones means that law enforcement officials can no longer access evidence of crimes stored on smartphones, *even though the officials have a search warrant issued by a neutral judge.*

Apple and Google are not responsible for keeping the public safe. That is the job of law enforcement. But the consequences of these companies’ actions on the public safety are severe. That is why my Office has been working with our law enforcement partners around the world to craft the solution recommended in this Report. We believe there is a responsible way to balance safety and security.

This Report is intended to:

- 1) Summarize the smartphone encryption debate for those unfamiliar with the issue;
- 2) Explain the importance of evidence stored on smartphones to public safety;
- 3) Dispel certain misconceptions that many privacy advocates hold about law enforcement’s position related to encryption, including the myth that we support a “backdoor” or government-held “key;”
- 4) Encourage an open discussion with technology companies, privacy advocates, and lawmakers; and
- 5) Propose a solution that protects privacy *and* safety.

Executive Summary

Parts I and II of this Report summarize the issue at hand and the relevant technology.

Part III explains how traditional means of investigation cannot be used to unlock a device using an operating system running full-disk encryption. In this paper, the term “full-disk encryption” means the encryption of data at rest on personal devices in such a manner that the passcode is required to decrypt the data. This use of the term is different from the technical definition, which involves encrypting all data on a device using the same key. The definition that we use is more colloquial. As used in this paper, a device running full-disk encryption is one that is effectively impregnable so that law enforcement cannot access any of the information on the device. Full-disk encryption has been a significant hindrance to the investigation and prosecution of criminals because certain types of evidence exist only on smartphones. While many privacy advocates point to the cloud as an alternative source of data for law enforcement, this Report explains why the cloud is not a sufficient alternative.

Part IV provides case examples to show the cost to public safety when operating system designers use full-disk encryption to render their devices immune from search warrants. Our discussion of smartphone encryption is not an academic exercise. Every day, we face real cases with real victims who suffer from the actions of criminals. We are obligated to do everything we can to bring these criminals to justice. But smartphone encryption has caused real – not hypothetical – roadblocks to our ability to solve and prosecute crimes.

Part V sets forth a proposed solution: Congress should enact a statute that requires any designer of an operating system for a smartphone or tablet manufactured, leased, or sold in the U.S. to ensure that data on its devices is accessible pursuant to a search warrant. Such a law would be well within Congress’s Commerce Clause powers, and does not require costly or difficult technological innovations.

Part VI considers some of the principal objections that have been made to our proposed solution:

- Our proposal and discussions on encryption are limited only to data at rest on smartphones and tablets, and not to data in transit. Data at rest is information that is stored on various sources after the data-creating event has occurred. Data in transit is live information that is in the process of being transferred from one source to another, or in other words, travelling across a network.
Many of the reports written about encryption and cyber-privacy focus on law enforcement’s ability to access data in transit and the security improvements gained through encrypting live data transfers or communications. This Report takes no position on issues relating to the encryption of data in transit.
- The harm to personal security and privacy if the proposal were to be implemented would be minimal.
 - Previous Apple and Google operating systems allowed law enforcement to access data on devices pursuant to search warrants. There is no evidence of which we are aware that any

- security breaches have occurred relating to those operating systems. Apple and Google have never explained why the prior systems lacked security or were vulnerable to hackers, and thus, needed to be changed. Those systems appeared to very well balance privacy and security while still being accessible to law enforcement through a search warrant.
- Technologists and forensics experts have indicated that if a hacker were able to learn Apple’s decryption process – which Apple guards extremely closely – that hacker would also need the actual device to steal data from that device. Likewise, a thief who steals a person’s locked smartphone would also need to know either the victim’s passcode or Apple’s highly guarded decryption process to obtain the device’s data.
 - Apple’s and Google’s new device encryption schemes do nothing to protect users from large-scale institutional data breaches or spyware.
 - While some have analogized any proposed legislation with the federal government’s failed efforts to impose the “Clipper Chip” on all phones, this Report does not propose using any technology similar to the Clipper Chip. This Report does not propose any new technology, nor does it propose that governments hold a key to any smartphones.
 - The proposal is similar to efforts being discussed in other countries that, like ours, value both personal privacy and the rule of law.
 - The proposal would not violate international human rights law or harm human rights activists. Rather, it would comport with the United Nations Human Rights Council’s standard in determining when a government can restrict encryption.
 - Technology companies and privacy advocates argue that if they give the U.S. government access to smartphone data pursuant to search warrants, then they must give the same data to all governments, including repressive regimes. This argument ignores the fact that local law enforcement in the U.S. seeks access to information only through a lawful judicial process. If a foreign nation’s government, repressive or not, wanted information from an American company, it also would have to go through lawful processes in the U.S.

Part VII lists questions – the answers to which are known only to Apple and Google – that must be answered to advance the debate. The Manhattan District Attorney’s Office sent questions to Apple and Google, but at the time of this Report’s publication, has yet to receive a response. Informed cooperation or legislation requires debate and open discussion.

In **Part VIII**, the Report concludes that while generally, data encryption offers significant benefits to the public, the harm that full-disk encryption on smartphones imposes on crime victims and public safety requires that it be regulated.

Contents

I.	The Problem.....	1
II.	Background Of Relevant Technology.....	2
	A. Apple	2
	B. Google.....	3
III.	The Inadequacy Of Extant Technological And Legal Tools For Collecting Evidence.....	4
	A. Prosecutors’ Historically-Useful Tools - The Search Warrant And The Unlock Order - Are No Longer Effective For Obtaining Evidence From Smartphones	4
	1. Attempts To Unlock Apple Devices	4
	2. Attempts To Unlock Google Devices	5
	B. The Difficulty Of Getting Passcodes From Defendants.....	5
	C. Certain Data Exists Only On Smartphones	6
IV.	The Cost Of Evidence Made Inaccessible Through Apple’s Encryption	9
V.	A Proposed Solution: Make Smartphones Amenable To Search Warrants	13
VI.	Responses To Potential Objections.....	14
	A. This Is A Limited Proposal That Addresses Only Data At Rest On Personal Devices.....	14
	B. The Loss Of Personal Security Would Be Minimal.....	14
	C. Personal Privacy Is Effectively Protected By The Fourth Amendment	14
	D. This Is Different From “Clipper Chips”.....	15
	E. Other Nations Are Exploring Similar Solutions.....	16
	F. Lawful Government Access To Smartphone Data Comports With International Human Rights Law, And Would Not Harm Human Rights Activists.....	17
VII.	Questions For Apple And Google	20
VIII.	Conclusion.....	23
Appendix I: Memorandum from 62 District Attorneys in New York State, April 16, 2015		
Appendix II: Letter from Manhattan District Attorney Cyrus R. Vance, Jr. to Jane Horvath, March 31, 2015; Letter from DA Vance to Kent Walker, April 1, 2015		

I. The Problem

In September 2014, Apple Inc. announced that its new operating system, iOS 8, would be designed such that when a phone or other device running iOS 8 locks, no one but the user, or another person with the device's passcode, could open it. Its subsequent operating system, iOS 9, released in September 2015, shares this feature.¹ When iOS 8 was released, Apple advertised that users' devices,² once locked, would be impervious to attempts by law enforcement to review the contents of the phones, even when law enforcement had obtained search warrants.³ Shortly after Apple's announcement, Google Inc. announced a similar plan: Its operating system, too, would be constructed to be impervious to all decryption efforts, including legally-authorized efforts of state and federal governments.⁴

Even before Apple's and Google's announcements, many devices had given users the option of enabling such powerful encryption. The significance of the companies' change in practice was that this type of encryption would be the default setting on their new devices. Apple's and Google's announcements led to an immediate response by law enforcement officials, who pointed out that allowing a phone to be locked such that it would be beyond the reach of lawful searches and seizures was unprecedented, and posed a threat to law enforcement efforts – in effect, a boon to dangerous criminals.⁵ The issues have been widely debated, especially on the internet⁶ and the editorial pages,⁷ and they have been the subject of congressional testimony.⁸

The debate may be characterized as one weighing individuals' rights to privacy against society's interest in providing governments with the tools that they require to maintain safety and provide security. But to characterize the debate is merely the first step towards resolving it: Privacy and safety may conflict in some instances – that is nothing new. The questions are, and have always been, where to draw the line between them, and how might they be balanced to the best advantage of the greatest part of society.

II. Background Of Relevant Technology

Encryption involves converting readable data (sometimes referred to as “plaintext”) into scrambled, unreadable data (sometimes referred to as “ciphertext”) using an algorithm that renders the data unreadable by a human or computer without the proper cipher and key to decrypt it. Data transmitted between phones, computers, and other digital devices can be encrypted (i) while in transit between those devices and (ii) on the devices themselves.

“Data at rest” is information that is stored on devices after the data-creating event has occurred. Data at rest could include, for example, a text message that has been received by a smartphone and has not been deleted from the device. In this paper, the term “full-disk encryption” means the encryption of data at rest on personal devices in such a manner that the passcode is required to decrypt the data.

“Data in transit” refers to information in the very moment that it is being transferred from one source to another, for example, information communicated in a phone conversation is data in transit while it is being transferred. A different type of encryption (not full-disk encryption), involving distinct security concerns and features, is used to encrypt data in transit. This report relates to full-disk encryption of data at rest on devices only. It does not address the issues arising from the encryption of data in transit.

A. Apple

Mobile devices manufactured by Apple include phones (called iPhones), tablets (iPads), and portable media players that play audio and video files (iPods). The operating system used by an Apple device is called iOS. Particular versions of the operating system are given numerical names – e.g., iOS 8. All Apple devices and the associated operating systems are manufactured and engineered by Apple.

iMessages are messages, which may contain text, photos, and other data, sent between Apple devices. iMessages can be sent over a Wi-Fi or cellular connection, and are routed through Apple’s systems rather than a phone service provider’s networks. SMS and MMS messages⁹ can be used on Apple and non-Apple devices. They are sent over a cellular connection only and are sent through a phone service provider’s networks, not Apple’s or other device makers’ systems.

Users of Apple devices can protect the data on their devices in two ways. They can establish passcodes, and, on some of the Apple devices, they can enable a feature that allows the device to be unlocked with the user’s fingerprint. If a user enters an incorrect passcode a certain number of times in a row on a device, the data on the device may automatically become permanently inaccessible.

Users can “back up” the contents of their Apple devices – that is, copy and store the content elsewhere such that, for example, if one were to lose one’s phone, one could get a new phone, access the backup copy, and restore it to the new phone. Apple devices can be backed up to a computer, an external hard drive, or a cloud service.

“The cloud” refers to networks of computers and servers that are used to store data. Many users utilize cloud storage to store photos, videos, documents, and messages. Using cloud storage keeps

storage space available on the user's device, and the items stored in the cloud can be accessed by all of a user's different devices, as long as those devices have an internet connection.

Apple's cloud is called iCloud. Users of Apple devices, Mac computers, and computers using particular Windows operating systems may set up iCloud accounts. The first five gigabytes of storage on an iCloud account are free, but if users want more space, they must buy it. Of course, no user of an Apple device is required to use iCloud. Users may prefer not to back up their devices at all, or they may back up to a computer, hard drive, or non-Apple cloud storage. Even if they take advantage of the five gigabytes of free storage space in iCloud, they may choose not to purchase any additional space.

B. Google

Devices running Google's mobile platform use the Android operating system. These devices include phones, tablets, and other devices. Each version of the Android operating system has both a numerical identifier – *e.g.*, version 5.0.1 – and a name, which has historically been the name of a dessert or candy – *e.g.*, Ice Cream Sandwich. Unlike Apple devices, Android devices are manufactured by a variety of different manufacturers, often referred to as Original Equipment Manufacturers or OEMs.

Users of Android devices can set up a “pattern unlock” passcode, which is a line connecting at least 4 dots in a 9-dot grid, to protect the data on their devices. Devices with certain operating systems (Froyo 2.2 and later) offer the ability to lock the device using a numeric or alphanumeric passcode. Some Android devices have fingerprint readers incorporated into the hardware of the device. The fingerprint reader is not incorporated into all Android devices, however, due to the variety of OEMs making Android devices. As with Apple devices, if a user enters an incorrect passcode a certain number of times in a row on a device, the data on the device may automatically become permanently inaccessible.

Google offers cloud storage in Google Drive and other locations. Data can be backed up to Google's cloud from an Android device, an iPhone, an iPad, or a computer. Users of Android devices are not required to back up to the cloud, or, if they do, to use Google's clouds rather than some other entity's cloud. Users of Google Drive receive 15 gigabytes of free storage and can purchase additional storage space. Many Android phones have a minimum of 16 gigabytes of storage space, and some can hold up to 128 gigabytes.

Android phones do not back up to Google cloud storage by default. Thus, a user must affirmatively choose to back up to the cloud, and the choice is not a single, all-or-nothing choice, but a series of choices, one for each type of data. It is, therefore, not uncommon for Android users to back up to Google's cloud only certain types of data from their smartphones, like photos and videos.

III. The Inadequacy Of Existing Technological And Legal Tools For Collecting Evidence

A. The Search Warrant And The Unlock Order – Prosecutors’ Historically-Useful Tools – Are No Longer Effective For Obtaining Evidence From Smartphones

When a prosecutor or investigative agency collects a passcode-protected phone, it might, if the circumstances permit, seek the owner’s permission to search the phone. In many instances, though, the owner is a defendant or suspect, and will not consent to a search. Sometimes, the phone owner’s identity is unknown (for example, if a phone is found at a crime scene), so the owner cannot be asked for permission to search the device. Even when the identity of the phone’s owner is known, in some cases, that person is unavailable to consent to a search of the device because, for example, he or she has been abducted or killed, as when the phone belongs to a kidnapping or murder victim.

When prosecutors have probable cause to believe that a phone contains evidence of a crime, they may apply to a court for a search warrant authorizing a search of the phone for that evidence.¹⁰ But even when prosecutors obtain a search warrant, they still have to unlock the phone to be able to search it.

1. Attempts To Unlock Apple Devices

For the iPhone 4, earlier versions of iPhones, and certain other Apple devices, forensic analysts can attempt to ascertain the device’s passcode by using “brute force,” *i.e.*, by systematically trying combinations of passcodes (e.g., “1, 1, 1, 1,” “1,1,1,2,” “1,1,1,3,” . . .) until the correct one is found. The process may be time-consuming and, for the reasons discussed below, can be used effectively on only certain Apple devices.

With respect to the iPhone 4s and later models of iPhones and other Apple devices running iOS versions through iOS 7, “brute force” attempts may result in the contents of the device becoming permanently inaccessible once the maximum number of passcode attempts is reached. For these devices, law enforcement requires the assistance of Apple to obtain the devices’ contents safely. The prosecutor or investigator obtains a search warrant and an order (often referred to as an “unlock order”) instructing Apple to assist with extracting data from the device. The prosecutor or investigator then sends Apple a copy of the warrant, the unlock order, the device, and a blank external hard drive. Apple uses a proprietary method to extract data from the device, and sends a copy of the data to law enforcement on the external hard drive.

For Apple devices running iOS 8, Apple can no longer comply with unlock orders. iOS 8 prevents Apple from accessing data on the device unless Apple has the user’s passcode. But, Apple does not keep users’ passcodes. Thus, it is no longer possible for Apple to extract data as it did for devices running prior operating systems. According to Apple, as of October 19, 2015, approximately 61% of all Apple devices currently in use run iOS 9, and approximately 30% use iOS 8. Only nine percent use an earlier iOS version.¹¹

2. Attempts To Unlock Google Devices

There are a larger variety of Android devices than Apple devices. Forensic examiners are able to bypass passcodes on some of those devices using a variety of forensic techniques. For some other types of Android devices, Google can reset the passcodes when served with a search warrant and an order instructing them to assist law enforcement to extract data from the device. This process can be done by Google remotely and allows forensic examiners to view the contents of a device.

For Android devices running operating systems Lollipop 5.0 and above, however, Google plans to use default full-disk encryption, like that being used by Apple, that will make it impossible for Google to comply with search warrants and orders instructing them to assist with device data extraction.

Full-disk encryption has not yet been implemented as a default on all Android devices running Lollipop 5.0 and later systems, but has been implemented on certain Nexus (Google-controlled) devices. Generally, users have the option to enable full-disk encryption on their current Android devices, whether or not the device is running Lollipop 5.0, but doing so causes certain inconveniences, risks, and performance issues, which are likely to exist until OEMs are required to standardize certain features.¹² As of October 5, 2015, approximately 23% of Android users were running Lollipop 5.0 or higher.¹³

B. The Difficulty Of Getting Passcodes From Defendants

Case law holds almost universally that a defendant cannot be compelled (by, *e.g.*, a grand jury subpoena or order of the court) to provide the government with her or his passcode, because such compulsion would violate the defendant's Fifth Amendment right against self-incrimination.¹⁴ There are two potential exceptions to this rule.

First, it is an open question whether, instead of being compelled to provide the government with a passcode, the defendant might be compelled to unlock her or his phone *using* the passcode. There have been no cases considering this precise question, and although a court might conclude that it is no different from the situation in which a defendant is compelled to provide the government with the passcode, it might also determine that the situations are somewhat different.¹⁵

Second, if the existence of evidence on the phone is a foregone conclusion, then the defendant may have no Fifth Amendment privilege with respect to the contents of the phone, and thus may be compelled to provide the government with the passcode.¹⁶ It would be difficult in most circumstances, however, for the government to establish with the requisite degree of certainty the existence of evidence in a phone that would clear the "foregone conclusion" hurdle.¹⁷

In any event, even if the government could lawfully compel a defendant to disclose her or his passcode – or to open her or his phone using the passcode – there is a substantial likelihood that any defendant who faces potentially serious criminal charges would simply refuse to comply with the subpoena or order, and go into contempt.¹⁸

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

C. Certain Data Exists Only On Smartphones

It is frequently argued that we live in a “golden age of surveillance,” and that because law enforcement has access to numerous sources of information, it does not need access to locked devices.¹⁹ The argument is unconvincing, because much important data may be found only on smartphones.

The below chart summarizes whether law enforcement officials can obtain particular types of data from a device, iCloud, Google cloud storage, or the phone service provider pursuant to legal process, if the data is not encrypted with full-disk encryption. Green boxes in the chart indicate that the type of data listed can be obtained from the location (if not encrypted with full-disk encryption), red boxes indicate when the type of data listed cannot be obtained from the location listed, and yellow boxes indicate that certain data may be obtained from the location, with caveats.

The chart and below discussion make clear that many types of important data are available only on devices.

Comparison of Data Sources				
	Device	iCloud	Google Cloud Storage	Phone company
iMessage content	Yes	No(1)	N/A	No
iMessage detail (dates, times, phone numbers involved)	Yes	No(1)	N/A	No
SMS/MMS content	Yes	No(1)	Perhaps(2)	Perhaps(3)
SMS/MMS detail (dates, times, phone numbers involved)	Yes	No(1)	Perhaps(2)	Yes
Phone call detail (dates, times, phone numbers involved, duration)	Yes	Yes	Perhaps(2)	Yes
Historical cell site data ²⁰	No	No	Perhaps(2)	Perhaps(4)
Historical other cell tower-related data ²¹	Perhaps(5), (6)	No	Perhaps(7)	No
Historical Wi-Fi network data	Perhaps(6)	Yes	Perhaps(7)	No
Historical GPS or other satellite data ²²	Perhaps(6)	Perhaps, some(2), (8)	Perhaps(7)	No
Contacts	Yes	Perhaps(2)	Perhaps(2)	No
Photos/Videos	Yes	Perhaps(2)	Perhaps(2)	No
Internet Search History	Yes	Perhaps(2)	Unknown	No
Internet Bookmarks	Yes	Perhaps(2)	Unknown	No
Third-Party App Data	Perhaps(6)	No	Unknown	No

- (1) Apple's website states that it can provide this information (http://images.apple.com/privacy/docs/us_le_guidelines_final_20150916.pdf, p. 8). In response to search warrants, however, Apple has not provided such information for backups of phones running iOS 8.
- (2) The information would be available to law enforcement only if the device user chose to back up to the cloud and included this type of data. *See* discussion immediately following chart.
- (3) Most carriers do not retain content. Some that do, retain for only a short period (*e.g.*, 3-5 days).
- (4) This data can be obtained by law enforcement while the data is retained by the phone service provider. There is no requirement, however, that wireless carriers maintain this type of data at all or for any particular length of time. In addition, cell site data is not retained by certain phone carriers for text messages. Given that many people now primarily communicate through text messages, this limits the amount of location information investigators can learn through cell site data.
- (5) May be available for only certain devices.
- (6) Forensic analysts are able to extract this information from devices. When Apple provides device data pursuant to an unlock order, however, they do not include this data.
- (7) May be available from Google when stored in its servers. This type of data does not appear to be stored in Google's cloud.
- (8) Certain types (*e.g.*, GPS EXIF data) may be available, but not all (*e.g.*, Google Maps data).

Some have argued that so long as cloud accounts are amenable to lawful searches, there is no need to require personal devices to be amenable to such searches.²³ The chart shows the weakness of that argument: Even under the best of circumstances, the cloud does not have all of the information that would be available on a personal device. And, there are several further reasons the cloud is a poor substitute for personal devices as a source of information important to law enforcement.

First, even if a person backs up his or her personal device to the cloud, it may be impossible for law enforcement to identify which cloud service the person has used. Many companies offer cloud storage, including Apple, Google, Microsoft, Dropbox, Box, and others. Even after the police seize a smartphone or other device that might be backed up to the cloud, without being able to access data in the device, the police would have no reasonable way that would work in all cases of determining which particular cloud service(s) a person uses for storage. Even if, through the issuance of subpoenas, the police learn which cloud service(s) the person uses, by the time the police learn that information, the evidence in the account(s) may have been destroyed by the smartphone owner or one of his accomplices.

Second, smartphone users are not required to set up a cloud account or back up to the cloud, and therefore, many device users will not have data stored in the cloud. Even minimally sophisticated wrongdoers who use their devices to perpetrate crimes and who have cloud accounts will likely take the relatively simple steps necessary to avoid backing up those devices, or data of interest, to the cloud. In most instances, only one or two selections must be made in the device's settings to turn off the back-up function or to remove certain types of content from the back up.

Third, even if a user chooses to back up all of his or her data to the cloud, a device will not be backed up to the cloud until it is connected to Wi-Fi or, for Android phones, a cellular connection. So, if evidence is stored on a device when it is disconnected from Wi-Fi or cell service, and the device is recovered by law enforcement officials before it is reconnected to such service, then the evidence would exist only on the device itself.

Fourth, although it may be possible to recover at least some deleted data from an Apple device, Apple states that once data has been deleted from an iCloud account, Apple cannot provide it in response to a search warrant.²⁴ Thus, the Apple device is the only route to evidence that has been deleted – which may, of course, be among the most probative evidence.²⁵

IV. The Cost Of Evidence Made Inaccessible Through Apple's Encryption

The harm caused by encryption is often discussed in the context of international terrorism. The greatest cost of default full-disk encryption, however, is likely borne by local law enforcement and the victims of domestic crime. Smartphones are ubiquitous, and there is almost no kind of case in which prosecutors have not used evidence from smartphones. Evidence from smartphones has been used across the country to investigate and prosecute homicides, rapes, assaults, domestic violence, narcotics rings, kidnappings, larcenies, frauds, and robberies. It is the rare case in which information from a smartphone is *not* useful; rather, it is often crucial.

Between September 17, 2014 and October 1, 2015, the Manhattan District Attorney's Office was unable to execute approximately 111 search warrants for smartphones because those devices were running iOS 8. The cases to which those devices related include homicide, attempted murder, sexual abuse of a child, sex trafficking, assault, and robbery. Because information stored on devices is so often probative, it is reasonable to believe that in many of these cases the data that is out of the reach of law enforcement would have been relevant to the case and to the investigation of additional crimes or perpetrators.

The following list of recent cases from this office demonstrates this point. It includes cases in which evidence from devices that were able to be searched was helpful in either prosecuting or exonerating a defendant.

- **Homicide:** *People v. Hayes*, Indictment Number 4451/12: The victim was filming a video using his iPhone when he was shot and killed by the defendant. The video captured the shooting. Because the iPhone was not passcode-locked, the video was recovered and admitted into evidence at trial. The video corroborated eyewitness testimony. The defendant was convicted of murder and sentenced to 35 years to life.
- **Rape and Robbery Conspiracy:** *People v. Sandel, Rivera, and Cruz*, Indictment Number 3158/15: The defendants are charged with committing predatory sexual assault, conspiring to rape and rob several victims, and numerous related crimes. During some of the rapes, they used mace on the victims. Significant evidence against the defendants was recovered from phones belonging to two of the defendants. Internet browsing history relating to mace was found on a phone. Text messages between the defendants were also crucial. For example, Rivera sent a text message to Sandel stating in substance, "just bring that pepper spray & taser," and Rivera sent a text message to Sandel stating in substance, "Soon we will terrorize NYC again." On the highest charge alone, each defendant is facing up to 25 years to life.
- **Child Pornography:** *People v. Hirji*, Superior Court Information Number 3650/15: The defendant was arrested after he began speaking with a cab driver about his interest in having sex with children and after showing the driver a child pornography image. An iPhone and an Android tablet were recovered from the defendant. Investigators obtained a search for the

devices, and a forensic analyst determined the passcode for both. Upon searching the iPhone, investigators discovered a large number of child pornography images. The defendant was convicted of Promoting a Sexual Performance by a Child.²⁶

- **Sex Trafficking:** *People v. Brown*, Indictment Numbers 865/12, 3908/12, and 3338/13: The defendant directed a sex trafficking operation involving at least four women, using physical violence, threats of force, and psychological manipulation to coerce the women to engage in prostitution. Evidence recovered from electronic devices seized from the defendant's home proved crucial to his conviction at trial. In particular, the defendant's smartphones contained photographs showing him posing his victims for online prostitution advertisements, and showing that he had "branded" multiple women, with his nickname tattooed onto their bodies; text messages between him and several victims confirmed that he had engaged in acts of violence against the testifying witness and others. The defendant was convicted of multiple counts of sex trafficking and promoting prostitution and was sentenced to 10-20 years in prison.
- **Sex Trafficking:** *People v. Rosado*, Indictment Number 5591/14: The defendant ran a sex trafficking operation involving multiple women and underage girls. He advertised their prostitution services on a website called Backpage, and used physical force to keep the girls and women in prostitution. When the defendant was arrested, he was in a car with a pregnant 16-year-old. An unlocked Android smartphone was recovered from him. Pursuant to a search warrant, our office analyzed the contents of the phone. Significant evidence was recovered, including text messages between the defendant and male customers about prostitution, the defendant's web browser history, which showed his access of Backpage, and photographs of the prostitutes that the defendant had posted in Backpage ads. This evidence was admitted at the defendant's trial. The defendant was convicted of Sex Trafficking and Promoting Prostitution, and sentenced to a prison term of seven to fourteen years.
- **Cybercrime and Identity Theft:** *People v. Jacas et al.*, Indictment Number 42/12, and *People v. Brahms et al.*, Indictment Number 5151/11: This case involved the successful prosecution of a 29-member identity theft ring. An iPhone was recovered from a waiter who was arrested for stealing more than 20 customers' credit card numbers by surreptitiously swiping those credit cards through a card reader that stored the credit card number and other data. When the phone was searched pursuant to a warrant, law enforcement officials discovered text messages between the waiter and other members of the group regarding the ring's crimes. Based in large part on information obtained from the phone, investigators were able to obtain an eavesdropping warrant, and ultimately arrested 29 people, including employees of high-end restaurants who stole credit card numbers, shoppers who made purchases using counterfeit credit cards containing the stolen credit card numbers, and managers who oversaw the operation. The group compromised over 100 American Express credit card numbers and stole

property worth over \$1,000,000. All of the defendants pled guilty, and more than \$1,000,000 in cash and merchandise were seized and forfeited.

- **Unlawful Surveillance:** *People v. Lema*, Indictment Number 4117/13: The defendant was arrested for unlawful surveillance after a police officer observed the defendant using his phone to film up women’s skirts, which is known as “upskirting.” The defendant consented to a search of his phone, but the passcode he provided did not work. Investigators obtained a search warrant and unlock order for the phone. The phone was sent to Apple, Apple extracted data from the phone, and the phone and data were returned to the prosecutor. Two upskirting videos were found on the phone, both filmed on the date of the defendant’s arrest. Following the trial, at which both videos were entered into evidence, the defendant was convicted as charged, of two counts of unlawful surveillance. Had the defendant been using an iOS 8, these videos would not have been recovered.
- **Homicide Exoneration:** *People v. Rosario*, Indictment Number 1859/10: A detective obtained a search warrant and an unlock order for certain iPhones found at the scene of a homicide. He sent the phones to Apple, which assisted in extracting data from them. The phone data demonstrated inaccuracies in what investigators initially thought to be the timeline of the events, and that a particular suspect was not, in fact, involved in the murder. A phone number stored in one of the iPhones was eventually linked to another individual, who later confessed and pled guilty to the killing. He is currently serving a sentence of 17 1/2 years’ imprisonment.

There are many other cases – almost too many to count – that could have been selected, but they all establish a single point: We risk losing crucial evidence in serious cases if the contents of passcode-protected smartphones remain immune to a warrant.

The enormity of the loss is fully appreciated by wrongdoers who use smartphones. The following telephone call, made earlier this year, from a prison inmate to a friend, shows that the inmate hoped that his phone had the new, impregnable Apple operating system. (Phone calls made by inmates are recorded by the Department of Corrections, and inmates are repeatedly advised that their calls are recorded.)

Inmate: I need you to open up your iPhone and go to your operating system.
If it’s on operating system 8, a iO8, they can’t get into my phone.
Because when we switched to T-Mobile they gave us brand new phones, right?

Friend: Yeah.

Inmate: And I think they had to do operating systems... what month we switched to T-Mobile?

Friend: Um.... February I think. We didn’t even have these phones for not even long.

Inmate: Good. What happen is in September 17, 2014, they opened up... It's all in the papers... **The DA Cyrus Vance who's prosecuting me is beefing with Apple because they put these phones that can't be [un]encrypted. If our phones is running on the iO8 software, they can't open my phone. That might be another gift from God.** We might have accidentally gotten the new phones and...

Friend: Yeah...²⁷

This defendant's case is hardly unique: His concerns and hopes, expressed in the phone call, about the protection the iOS 8 operating system would afford him are shared by criminals in every jurisdiction in America charged with all manner of crimes, including rape, kidnapping, robbery, promotion of child pornography, and larceny. As recognized by this defendant, criminals benefit significantly from iOS 8, and the safety of all American communities is imperiled by it.

V. A Proposed Solution: Make Smartphones Amenable To Search Warrants

There is no provision of the U.S. Constitution, or of any state constitution, that would require producers of smartphones and operating systems to make smartphones amenable to governmental searches. A federal statute could, however, compel such amenability.²⁸ The Commerce Clause gives the federal government the authority to “regulate Commerce . . . among the several States,” and “with foreign Nations.”²⁹ Because smartphones are part of interstate and foreign commerce, a federal statute regulating smartphones would comfortably fall within the power of Congress to regulate activities “that substantially affect interstate commerce.”³⁰

Any state could also regulate smartphones sold or used within its borders. Each of the 62 District Attorneys in New York State have, indeed, proposed such legislation.³¹ It is clear, however, that federal legislation is preferable to state legislation. The problem under consideration here requires a nationwide solution, and only federal legislation can provide it.

The federal legislation would provide in substance that any smartphone manufactured, leased, or sold in the U.S. must be able to be unlocked, or its data accessed, by the operating system designer. Compliance with such a statute would not require new technology or costly adjustments. It would require, simply, that designers and makers of operating systems not design or build them to be impregnable to lawful governmental searches.

VI. Responses To Potential Objections

A. This Is A Limited Proposal That Addresses Only Data At Rest On Personal Devices

This white paper addresses only questions relating to law enforcement's ability to access data at rest on personal devices. Many of the reports written about encryption and cyber-privacy focus on law enforcement's ability to access data in transit and the security improvements gained through encrypting live data transfers or communications.³³ This paper takes no position on issues relating to the encryption of data in transit.

The ability to decrypt data in transit presents unique risks that are simply not presented by the ability to decrypt data at rest. Most significantly, the ability to decrypt data in transit creates the possibility of unlawful eavesdropping on live communications; such eavesdropping is not at issue in connection with data at rest.

B. The Loss Of Personal Security Would Be Minimal

The principal argument in favor of making devices impregnable to the government is that any effort that would allow the government to collect evidence lawfully from devices would necessarily lessen the devices' security, and thus increase the possibility of a bad actor unlawfully accessing device data.

There is a cost-benefit analysis to be considered: The loss in personal security that would be occasioned by the proposed statute must be weighed against the gain in societal safety that it would create.

Some experts have stated that there is no practicable way to quantify the loss of personal security that results from making devices amenable to government search warrants. There are, however, at least four reasons to believe that the loss of security would not be significant if this paper's proposal was adopted.

First, rendering devices running iOS 8 or Lollipop 5.0 amenable to search warrants would put such devices on the same footing as those that run all previous version of iOS and Android operating systems. There has been no evidence of which we are aware of security breaches that have affected the latter types of devices, let alone any breaches attributable to the feature of the operating systems that rendered them amenable to search warrants. Apple and Google have never explained why the prior systems lacked security or were vulnerable to hackers and, thus, needed to be changed. It is therefore unclear why it would be unsafe for Apple and Google to retain the ability to access data on devices pursuant to search warrants.

Second, this office's investigation to date, which has included consultation with technologists and forensic experts, has indicated that even were a person to learn Apple's decryption process improperly, that person would need the actual device he wished to decrypt to use that process. Apple's passcode-bypass process cannot be used remotely or, in other words, without possession of the targeted device. The ability to decrypt does not, alone, give Apple or a hacker access to information stored on a device.³⁴

Third, Apple and Google are able to provide some readable data stored by users in their cloud accounts, pursuant to a search warrant. It is unclear why, if Apple's and Google's ability to decrypt data stored on devices presents a security problem, the same problem is not caused by the ability of the companies to access, in unencrypted form, data stored by their users on the companies' cloud servers.

Fourth, if a user's phone were to be stolen, as long as the user had previously enabled the Find My iPhone app³⁵ or a specific setting in Android Device Manager,³⁶ he or she could remotely lock the phone and wipe the phone's data, preventing the data from getting into the thief's possession. These options can effectively prevent thief-hackers from obtaining a phone's data.³⁷

C. Personal Privacy Is Well Protected By The Fourth Amendment

For the above reasons, were Apple and Google once again to give themselves the ability to decrypt data stored on their devices, there would not be a significant loss of security. This, in combination with the safeguards provided by the Fourth Amendment, means that personal privacy would be successfully protected.

The Fourth Amendment dictates that search warrants may be issued only when a judge finds probable cause to believe that a crime has been committed and that evidence or proceeds of the crime might be found on the device to be searched.³⁸ The warrant requirement has been described by the Supreme Court as “[t]he bulwark of Fourth Amendment protection,”³⁹ and there is no reason to believe that it cannot continue to serve in that role, whether the object that is to be searched is an iPhone or a home.

In fact, what makes full-disk encryption schemes remarkable is that they provide greater protection to one's phone than one has in one's home, which, of course, has always been afforded the highest level of privacy protection by courts. Apple and Google should not be able to alter this constitutional balance unilaterally. Every home can be entered with a search warrant. The same should be true of devices.

D. This Is Different From The “Clipper Chip”

The recent encryption debate has drawn parallels to the “Crypto Wars” of the 1990s when the Clinton Administration proposed requiring that telephone and electronic communications devices be equipped with a “Clipper Chip,” which would have given the government a “key” to decrypt communications.⁴⁰ Despite the comparisons, however, this paper does not propose using any technology similar to the Clipper Chip.

The Clipper Chip was a small hardware chip that would encrypt the private communications of two parties and provide both ends with a cryptographic key to decipher the message. Any device with a Clipper Chip also would be assigned an additional key given to the government “in escrow.” If a government agency obtained a court-ordered wiretap to intercept communications made using a particular device, the key would be given to that agency so that all data transmitted could be decrypted.⁴¹

The government intended for the chip to be implanted into almost all telephone and electronic communications devices manufactured in the U.S. But the technology was abandoned by the government after research showed that it would have been technologically unworkable, and that there was a flaw in the technology that would have allowed a third party to encode communications so that even the government's key could not unscramble it.⁴²

This paper does not propose any new technology, nor does it propose that governments hold a key to smartphones. It proposes an arrangement that worked without any significant, documented security problems before iOS 8 and Lollipop 5.0. And, the only keys would be held by the operating system designers.

E. Other Nations Are Exploring Similar Solutions

Some critics have suggested that the U.S. is insufficiently protective of privacy and technological innovation, and that requiring software to be amenable to government searches will somehow put the U.S. out-of-step with the rest of the world. Of course, being out-of-step with the rest of the world, for the right reasons, would not be a bad thing, but, in any event, this paper's proposal is not.

Other nations, recognizing the dangers posed by impregnable encryption, have enacted legislation, or are considering legislation, that would guarantee government access under appropriate circumstances. Although much of this legislation relates to data in transit rather than data at rest, it evidences these countries' deep concerns regarding undecryptable data.

United Kingdom

In a January 12, 2015 speech, British Prime Minister David Cameron said that governments must have all necessary tools to protect their citizens, including access to private communications under appropriate circumstances: “[T]he question is are we going to allow a means of communications which it simply isn't possible to read. My answer to that question is: no, we must not. The first duty of any government is to keep our country safe.”⁴³

Prime Minister Cameron pledged to propose legislation that would enable his government to access both metadata and content of communications. He argued that this surveillance—which would require approval by the home or foreign secretary—would be consistent with a “modern, liberal democracy.”⁴⁴ He explained that communications data is “absolutely crucial not just to fight terrorism but finding missing people, murder investigations.”⁴⁵ Of course, precisely the same is true in the U.S.

Prime Minister Cameron reaffirmed his position in June 2015 and said that his government will propose legislation in the fall of 2015. In response to a question in Parliament, Cameron said:

We have always been able, on the authority of the home secretary, to sign a warrant and intercept a phone call, a mobile phone call or other media communications, but the question we must ask ourselves is whether, as technology develops, we are content to leave a safe space—a new means of communication—for terrorists to communicate with each other. My answer is no, we should not be, which means that we must look

at all the new media being produced and ensure that, in every case, we are able, in extremis and on the signature of a warrant, to get to the bottom of what is going on.⁴⁶

As of the publication of this Report, no such legislation has been introduced.

France

In February 2015, French Interior Minister Bernard Cazeneuve visited U.S. technology companies in Silicon Valley, including Apple and Google, and urged them to ease encryption policies that block government access to terroristic and other criminal communications.⁴⁷ During an interview before the trip, Minister Cazeneuve noted that encryption was a central issue. “We are facing a new threat. We need tech companies to realize that they have an important role to play,” he said.⁴⁸

The Netherlands

In July 2015, the Dutch government released for public comment a proposed bill updating the country’s Intelligence & Security Act of 2002. The bill would, among other things, authorize intelligence agencies to compel assistance with decryption of data, including communications.⁴⁹

* * *

These statements and pieces of proposed legislation are not all the same, nor are they identical to what is proposed here. The significance of each of them, however, is that they evidence the recognition by sophisticated governments, in societies that value individual privacy highly, as ours does, that it is a government’s principal responsibility to keep its residents safe, and that a government cannot fulfill that responsibility if huge amounts of vital information directly related to public safety are inaccessible to the government. That same recognition should guide the U.S.

F. Lawful Government Access To Smartphone Data Comports With International Human Rights Law, And Would Not Harm Human Rights Activists

Some have suggested that making smartphones accessible to lawful governmental searches would violate international human rights law and might be harmful to human rights activists.⁵⁰ Neither point is persuasive.

The U.N. Human Rights Council addressed encryption and privacy rights in two recent reports: a June 30, 2014 report entitled “The Right to Privacy in the Digital Age” by the Office of the United Nations High Commissioner for Human Rights, and a May 22, 2015 report entitled “The Promotion and Protection of the Right to Freedom of Opinion and Expression” by the U.N. Human Rights Council Special Rapporteur Professor David Kaye.⁵¹ In both reports, the United Nations Human Rights Council stated that court-ordered decryption does not violate international human rights and is permissible if the government intrusion is lawful, narrow, and necessary. Where there is a legitimate aim — such as the prevention of terrorism or crime — and where appropriate safeguards are in place, “a State might be allowed to engage in quite intrusive surveillance.”⁵² In his report, Professor Kaye explained that:

Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.⁵³

Following these principles, the U.N. Human Rights Council enunciated a three-part test to determine when a government can restrict encryption:

- 1) The government restriction must be provided for by law. That law must be “sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances.”⁵⁴ The law also must provide strong procedural and judicial safeguards in order protect individuals’ due process rights.⁵⁵
- 2) The government restriction may be imposed to achieve a legitimate objective, *i.e.*, to protect specified rights, including “rights or reputation of others; national security; public order; public health or morals.”⁵⁶
- 3) The government must demonstrate that the restriction is both necessary and proportionate to the specific risk being addressed.⁵⁷

Our proposal plainly satisfies these criteria. First, a smartphone would be searchable only pursuant to a judicially-issued warrant upon a showing of probable cause. The legal principles pursuant to which such warrants are issued are well-known and precise. They provide for “strong procedural and judicial safeguards” to protect individuals’ due process rights, as required by the United Nations.⁵⁸

Second, the United Nations states that limitations on individuals’ privacy may be justified to protect national security, public order, and public health.⁵⁹ Law enforcement’s efforts to solve crimes fall within the definition of “public order.”

Third, as demonstrated above, obtaining information on smartphones has been crucial in solving and prosecuting a variety of types of crimes, including very serious ones.⁶⁰ Requiring technology companies to retain the ability to decrypt data, which resulted in no appreciable harm to security or public safety, is a proportionate and necessary solution to the problems caused by default full-disk encryption.

One of the arguments consistently raised by those who argue in favor of default full-disk encryption of data stored on devices is that if the U.S. government were to have the right to access a smartphone’s contents, then all governments would have that right. And, the argument continues, if a repressive government exercised that right, dissidents and human rights advocates in the repressive country would be injured, because the repressive government would seek access to smartphones to spy on, prosecute, and otherwise oppress the dissidents and human rights advocates.⁶¹

This argument unravels upon close inspection. Apple and Google could keep information regarding their decryption processes in the U.S., and give access to the data stored on phones to only those countries that abide by certain standards of human rights and liberties. Technology companies are

not required to treat requests from all nations equally. Some companies choose not to do business in foreign countries with oppressive governments, or to do only limited business in them. If Apple and Google were to cater to the whims of repressive countries, it would be because they chose to do so, not because they were forced to.

The technology companies' claims that if the U.S. government demands access to information, the government will "have little room to object"⁶² to repressive regimes' demands ignores the fact that local law enforcement in the U.S. seeks access to information only through a lawful judicial process. If a foreign nation's government, repressive or not, wanted information from an American company, it also would have to go through lawful processes in the U.S., either pursuant to a Mutual Legal Assistance Treaty (MLAT)⁶³ or a letter rogatory.⁶⁴ If the foreign government used the MLAT process, the executive branch of the federal government would decide whether, in its discretion, the foreign government's request was proper. If the foreign government used a letter rogatory, a federal court would make that determination.⁶⁵ In either case, the request could be refused if the information was sought for use in a proceeding that would violate human rights. "At a minimum, the Constitution requires that a request not be honored if the sought-after information would be used in a foreign judicial proceeding that 'depart[s] from our concepts of fundamental due process and fairness.'"⁶⁶

VII. Questions For Apple And Google

Certain information regarding Apple's and Google's technology and their responses to foreign government requests for customer information is known only to Apple and Google. The Manhattan District Attorney's Office has previously sent letters to Apple and Google that asked some of the questions necessary to a fully-informed debate regarding their technology and its implications for criminal cases, privacy, and security. Neither company has responded.⁶⁷ Immediately below are several additional questions that Apple and Google should answer – and that only they have the information to answer – so that the best possible balance of all the concerns involved can be reached.

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 he use it to remotely attack devices or would he need possession of the device?

Why This Is Important To Know: If the risk addressed by the new encryption schemes would require knowledge of Apple's or Google's decryption process and possession of the device to be hacked, the risk would appear to be much smaller than if knowledge of the decryption process alone could allow a hacker to access a device remotely.

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?*
- b. *Is the likelihood of a successful cloud hack decreased by the new encryption scheme? If so, why and how much?*

Why This Is Important To Know: In order to determine the appropriate balance between the added security of the new encryption schemes and the harm to criminal investigations and prosecutions, it is important to understand the scope of the problems on each side.

Question 3

If there are significant security problems posed by the ability of Apple and Google to decrypt data on devices with earlier operating systems, do those same security problems exist as to cloud data as a result of Apple's and Google's current ability to provide readable data stored on their cloud servers? If not, why not?

Why This Is Important To Know: If there are security problems of importance that result from the ability of technology companies to decrypt data on their devices, it is difficult to understand why these concerns would not exist in relation to their ability to provide readable cloud data. If the same security problems exist as to data currently stored in the cloud, why aren't the companies providing their customers with impregnable encryption for their cloud data? If the same security problems exist as to cloud data, but the technology companies don't feel it necessary to impregnablely encrypt that data, is it not fair to infer that the scope of the security problems solved by the current encryption schemes is limited?

Question 4

How did Apple and Google respond to requests for customer data, including content and non-content data, from foreign governments prior to iOS 8 and Lollipop 5.0?

- a. *What type of legal process was required for Apple or Google to provide content from a device to another country? Does it depend on the country? If so, describe the difference in what was required from different countries and what could be provided to different countries.*
- b. *In the transparency report for the second half of 2014, Apple indicates that it provided no content to China from accounts. Was any requested? If so and none was provided, how could Apple refuse to provide content? Was any content from devices provided (as opposed to iCloud content or other content stored on Apple's servers)?*
- c. *Has Google ever refused to provide content upon receiving a request to do so from a foreign government when it was technologically possible to provide that content? If so, how could Google make such a refusal?*
- d. *Do Apple's and Google's purported needs to respond to law enforcement requests from foreign government result in any way from their choices to do business in those countries? Do Apple and Google respond to law enforcement requests from countries in which it does not do business? If so, by what process?*
- e. *How do Apple and Google respond to foreign government requests for data stored on their clouds? What type of legal process is required? Are these requests ever denied? If so, on what basis? If these requests are made by oppressive foreign governments, how do Apple and Google deal with that problem?*

Why This Is Important To Know: Some people contend that if Apple and Google have the ability to decrypt content stored on their devices pursuant to U.S. legal process, then they will also be required to decrypt content pursuant to foreign government requests. While this contention is unpersuasive, see *supra* Section VI(F), it would, in any event, be informative to learn how Apple and Google previously responded to foreign government requests for device data and currently respond to foreign government requests for cloud data.

Question 5

In this office's experience (and, it appears, other offices' experiences) with Apple's responses to iCloud search warrants for devices running iOS 8, thus far, Apple has provided either no iMessage, SMS message, and MMS message content or has provided encrypted, unreadable message content. It is unclear why Apple is not providing decrypted, readable message content for iCloud accounts, particularly given that its law enforcement guidelines state that this content can be turned over to law enforcement pursuant to a search warrant (http://images.apple.com/privacy/docs/us_le_guidelines_final_20150916.pdf, p. 8). Why isn't Apple providing decrypted iMessage, SMS message, and MMS message content from iCloud in response to search warrants?

Why This Is Important To Know: iMessage, SMS message, and MMS message content is crucial to criminal investigations and prosecutions. Since there are no readily apparent obstacles to Apple providing decrypted message content from iCloud accounts in response to a search warrant, and since Apple's law enforcement guidelines say that Apple can provide it, it should explain why it is not doing so.

Question 6

Can Apple and Google recover data deleted from iCloud and Google cloud storage for a customer? Under what circumstances? Can Apple and Google recover data deleted from iCloud and Google cloud storage for law enforcement in those same circumstances? If not, why not?

Why This Is Important To Know: Deleted data can be some of the most probative evidence in a criminal investigation. If deleted data can be recovered for Apple's and Google's cloud customers in certain circumstances, that same data should be able to be provided by the companies to law enforcement in response to a search warrant.

VIII. Conclusion

Technology benefits us in ways too many to count and in amounts impossibly large to calculate. But it can also be used to harm us, and unless we regulate it intelligently and carefully, we may suffer great harm. Smartphones are technological bank vaults, but unlike bank vaults, which, no matter how strong, are accessible to search warrants, smartphones are becoming beyond the reach of law enforcement. The result will be crimes that go unsolved, harms that go unanswered, and victims who are left beyond the protection of the law.

ENDNOTES:

¹ For simplicity, this report refers to iOS 8 throughout, but, unless otherwise noted, the topics discussed relate to iOS 8 and 9.

² The technology discussed in this paper affects smartphones, tablets, and certain other devices. In some places, for simplicity, this report refers only to phones. The concerns discussed in those places relate to all of these types of devices, unless otherwise noted.

³ See <https://www.apple.com/privacy/government-information-requests>

⁴ See, e.g., Timberg, “Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police,” *The Washington Post*, September 18, 2014 (<http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/>).

⁵ See Bobic and Reilly, “FBI Director James Comey ‘Very Concerned’ About New Apple, Google Privacy Features,” *Huffington Post*, September 25, 2014 (http://www.huffingtonpost.com/2014/09/25/james-comey-apple-encryption_n_5882874.html); Vance, Jr., “Apple and Google Threaten Public Safety with Default Smartphone Encryption,” *The Washington Post*, September 26, 2014 (https://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b43f-1a7368204804_story.html); Nakashima and Gellman, “As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security,” *The Washington Post*, April 10, 2015 (https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ce745911a4ff_story.html).

⁶ See, e.g., Poulsen, “Apple’s iPhone Encryption Is a Godsend, Even if Cops Hate It,” *Wired*, October 8, 2014 (<http://www.wired.com/2014/10/golden-key/>); Green, “Is Apple Picking a Fight With the U.S. Government?,” *Slate*, September 23, 2014 (http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html); Wittes, “Five Hard Encryption Questions,” *Lawfare*, August 7, 2015, (<https://www.lawfareblog.com/five-hard-encryption-questions>).

⁷ See, e.g., Editorial Board, “Compromise needed on smartphone encryption,” *The Washington Post*, October 3, 2014 (https://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html); Editorial Board, “Government Agencies Shouldn’t Get Keys to Unlock Our Encrypted Devices,” *Los Angeles Times*, July 27, 2015 (<http://www.latimes.com/opinion/editorials/la-ed-encryption-20150727-story.html>).

⁸ See <http://www.judiciary.senate.gov/hearings/watch?hearingid=ef7e62c1-5056-a055-64e2-f2954aaa5e15> (video of July 8, 2015 “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy” Hearing Before the Senate Judiciary Committee).

⁹ SMS or Short Messages Service messages are text messages of up to 160 characters in length. MMS or Multimedia Messaging Service messages include messages with multimedia content, like photos.

¹⁰ The U.S. Supreme Court has recently ruled that warrants are required for searches of mobile phones, absent an exception to the warrant requirement. See *Riley v. California*, 573 U. S. ___, 134 S. Ct. 2473 (2014).

¹¹ <https://developer.apple.com/support/app-store> (accessed October 21, 2015).

¹² With the release of its latest operating system, Marshmallow, Google has required that full-disk encryption be enabled by default on certain devices. See Constantin, “Google Requires Full-Disk Encryption and Secure Boot for Some Android 6.0 Devices,” *Computerworld*, October 20, 2015 (<http://www.computerworld.com/article/2994985/android/google-requires-full-disk-encryption-and-secure-boot-for-some-android-60-devices.html>).

¹³ <http://developer.android.com/about/dashboards/index.html#2015> (accessed October 21, 2015).

¹⁴ The Fifth Amendment provides that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.” U.S. Const., amend. V. The amendment’s prohibition against self-incrimination has been “incorporated” so that it applies to state criminal proceedings, as well as federal. See *Malloy v. Hogan*, 378 U.S. 1, 6 (1964); *Griffin v. California*, 380 U.S. 609, 615 (1965). The cases addressing the question whether a defendant may be compelled to provide her or his passcode to the government, and holding that such compulsion would violate the Fifth Amendment include: *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *U.S. v. Kirschner*, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010); *SEC v. Huang*, No. 15-269 (E.D.Pa.) (Sept. 23, 2015) (slip op. at 4-5); *Commonwealth v. Baust*, 89 Va. Cir. 267, 270-71 (Circuit Ct. of the City of Virginia Beach) (Oct. 28, 2014).

¹⁵ Professor Orin Kerr has suggested that because it is (or may, in many cases be) a “foregone conclusion” that a person knows the passcode to her or his own smartphone, it would not violate the Fifth Amendment to compel a phone owner to use her or his passcode to open the phone. See Kerr, “Apple’s Dangerous Game,” *The Washington Post*, September

19, 2014 (<https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/>) (citing *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009)). This may be correct, although it has not been tested in any case (*Boucher* suggests that if the *content* of the smart phone is known (a “foregone conclusion”), then requiring the passcode may not implicate the Fifth Amendment; it does not say that a person’s knowledge of her or his passcode would satisfy the foregone conclusion requirement.).

¹⁶ See, e.g., *People v. Havrish*, 8 NY3d 389, 395 (N.Y. 2007); *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009) at *3; *In re Fricosu*, 841 F. Supp.2d 1232, 1237 (D. Colo. 2012).

¹⁷ Professor Kerr has also explored the argument that compelling a person to provide her or his password may not violate the Fifth Amendment because the provision of the password may not be incriminating, as that term is by the Supreme Court in cases such as *Hoffman v. U.S.*, 341 U.S. 479 (1951), and *Fischer v. U.S.*, 425 U.S. 391 (1976). See Kerr, “A Revised Approach to the Fifth Amendment and Obtaining Passcodes,” *The Washington Post*, September 25, 2015 (<https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/25/a-revised-approach-to-the-fifth-amendment-and-obtaining-passcodes/>). Professor Kerr’s analysis may be right, although it does not appear that any courts have adopted it, and therefore there are still questions about the application of the Fifth Amendment to efforts to compel persons to provide their passcodes to the government.

¹⁸ See, e.g., *In re Weiss*, 703 F.2d 653, 660-65 (2d. Cir. 1983).

¹⁹ See, e.g., Peter Swire, Encryption and Globalization, 13 Colum. Sci. & Tech. L. Rev. 416 (2012); Rosenzweig, “iPhones, the FBI, and Going Dark,” *Lawfare*, August 4, 2015 (<https://www.lawfareblog.com/iphones-fbi-and-going-dark>) (reprinting a blog post from Nicholas Weaver, arguing that even though “an iOS device is perhaps the most secure, general purpose communication device available,” there are numerous ways for law enforcement lawfully to obtain a great deal of information about a smartphone user, including the cloud, phone carriers, and Apple itself).

²⁰ Cell site data, which is typically held by phone companies, is less precise than certain other types of location data because it may tell investigators only the location of a cell tower that was used to transmit a person’s communication rather than the caller’s location. Further, this type of data is captured only when a communication is made and not at times when a phone is not being used.

²¹ Certain phones capture data relating to reception of signals from cell towers, including at times when the phone is not being used to communicate. This information may include the location of towers whose signals the phone picked up as well as towers near those towers.

²² Specific types of location data include historical cell site data, historical other cell tower-related data, historical Wi-Fi network data, and historical GPS or other satellite data.

²³ See, e.g., Dujardin, “Law Enforcement Worries Over Beefed-Up Phone Encryption,” *Daily Press*, April 12, 2015 (<http://www.dailypress.com/news/crime/dp-nws-phone-encryption-20150412-story.html>); O’Connor, “Encryption Makes Us All Safer,” *Center for Democracy & Technology*, October 8, 2014 (<https://cdt.org/blog/encryption-makes-us-all-safer/>).

²⁴ http://images.apple.com/privacy/docs/us_le_guidelines_final_20150916.pdf, p. 8.

²⁵ The same appears to be true for Android devices and Google’s cloud storage, but Google should clarify whether they can provide deleted cloud data to law enforcement. See *infra* Section VII, Question 6.

²⁶ Initially, a forensic analyst was unable to unlock the iPhone, which was running iOS 8. The analyst was able to determine the passcode for the tablet through brute force. The analyst tried entering that passcode into the iPhone. Luckily, the defendant had chosen the same passcode for both devices, and the forensic analyst was able to search the phone. If the analyst had been unable to determine the tablet’s passcode, or if the tablet’s passcode had not been the same as the iPhone passcode, there would have been no case against the defendant.

²⁷ Later conversations between this inmate and his friend similarly focused on this topic. After the friend told the inmate that she had checked and believed that the iPhone was using the iOS 8 operating system, the inmate was relieved: “That means God might be in my favor. I don’t think they can open it.” Later, speaking to another person, the inmate expressed the hope that his phone could not be unlocked because “I mean, you know how much shit is on that phone.” The inmate then spoke with this friend again, had her confirm that the inmate’s iPhone used the iOS 8 operating system, and also had her call Apple to make sure that the iOS 8 operating system was secure. The friend confirmed that Apple said that it was, and then assured him, “You should be good, as long as they can’t open that phone.”

²⁸ One commentator has argued that a provision ensuring that certain electronic devices be amenable to government searches would not be a preservation of the legal *status quo* but, but an extension of it. See Wittes, “Five Hard Encryption Questions,” *Lawfare*, August 7, 2015 (<https://www.lawfareblog.com/five-hard-encryption-questions>). That is true, and that is why legislation is needed to address the issues raised here. As technology changes, bringing both opportunities and risks, intelligent legislation is the appropriate response. See, e.g., *U.S. v. Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (citing Owen Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102

Mich. L. Rev. 801, 805-06 (2004)); Erin Murphy, The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions, 111 Mich. L. Rev. 485 (2013).

²⁹ U.S. Const. Art. I, § 8, cl. 3.

³⁰ *Gonzales v. Raich*, 545 U.S. 1, 17 (2005). See also *Pension Benefit Guaranty Corporation v. R. A. Gray & Co.*, 467 U.S. 717, 729 (1984) (“[S]trong deference [is] accorded legislation in the field of national economic policy.”); *Hodel v. Indiana*, 452 U.S. 314, 326 (1981) (“This [C]ourt will certainly not substitute its judgment for that of Congress unless the relation of the subject to interstate commerce and its effect upon it are clearly non-existent.” (internal quotation marks omitted)).

³¹ A copy of the proposed legislation and the District Attorneys’ memorandum in support of it is annexed hereto as an appendix.

³² *This footnote has been removed.*

³³ See, e.g., Abelson et al., “Keys Under Doormats: Mandating Insecurity by Requiring Governmental Access to all Data and Communications,” July 6, 2015 (available at <http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8>) (primarily discussing numerous security flaws in data-in-transit-related technology); Jeong, “A ‘Golden Key’ for Encryption is Mythical Nonsense,” *Motherboard*, July 21, 2015 (http://motherboard.vice.com/read/a-golden-key-for-encryption-is-mythical-nonsense?utm_source=mbtwitter); Irwin, “Getting to the Heart(bleed) of the Problem,” *GWToday*, April 16, 2014 (<http://gwtoday.gwu.edu/getting-heartbleed-problem>) (citing examples of security vulnerabilities related to data in transit, such as the “FREAK attack” or the “Heartbleed bug,” which allow hackers to intercept web traffic). Other cybersecurity compromises, such as malware or data breaches at large institutions, are not affected by the ability to decrypt data at rest.

³⁴ As noted above, for certain devices, when served with a search warrant and unlock order, Google can remotely reset the device’s passcode, allowing law enforcement to search the device. It is not clear whether a wrongdoer with knowledge of Google’s passcode-reset process would need possession of a victim’s device to wrongfully access its contents or whether knowledge of the process alone would allow this. This is a question that Google should answer. See *infra* Section VII, Question 1.

³⁵ A similar app is also available for Apple tablets and computers.

³⁶ Wallen, “Remotely Wipe Your Android Device With The Help of Google,” *TechRepublic*, June 18, 2014 (<http://www.techrepublic.com/article/remotely-wipe-your-android-device-with-the-help-of-google/>).

³⁷ There is one risk that making devices impregnable would, in fact, eliminate: the risk that a malicious insider at Apple or Google or a hacker could wrongfully access or share decryption processes for those systems. See Abelson et al., “Keys Under Doormats: Mandating Insecurity by Requiring Governmental Access to all Data and Communications,” July 6, 2015, pp. 2, 7, 15 (available at <http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8>). There is no indication, however, that compromises of these types have occurred or are likely to occur with respect to pre-iOS 8 and pre-Lollipop 5.0 devices. So that the public can assess the probability of a malicious insider or hacker compromising the security of customers’ smartphones, Apple and Google should provide answers to the question on this topic included below. See *infra* Section VII, Question 2.

³⁸ See U.S. Const., amend. IV (“ . . . no Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”); *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (defining probable cause as “a fair probability that contraband or evidence of a crime will be found in a particular place”).

³⁹ *Franks v. Delaware*, 438 U.S. 154, 164 (1978). See also, e.g., *Gonzales v. Beto*, 425 F.2d 963, 967 (5th Cir. 1970) (“The requirement of a search warrant is unquestionably a strong bulwark against the evils at which the fourth amendment is directed.”)

⁴⁰ See Perlroth, “Security Experts Oppose Government Access to Encrypted Communication,” *The New York Times*, July 7, 2015 (http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html?_r=0).

⁴¹ See Levy, “Battle of the Clipper Chip,” *The New York Times*, June 12, 1944 (<http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>).

⁴² See Abelson et al., “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption,” May 27, 1997 (available at <http://academiccommons.columbia.edu/catalog/ac%3A127127>); Perlroth, “Security Experts Oppose Government Access to Encrypted Communication,” *The New York Times*, July 7, 2015 (http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html?_r=0).

⁴³ Quoted in Mason, “UK Spy Agencies Need More Powers, Says Cameron,” *The Guardian*, January 12, 2015 (<http://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-america-paris-attacks>).

44 *Id.*

45 *Id.*

46 Quoted in Bienkov, “David Cameron: Twitter and Facebook Privacy is Unsustainable,” *Politics.co.uk*, June 30, 2015 (<http://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable>).

47 See Gauthier-Villars and Schechner, “Tech Companies are Caught in the Middle of Terror Fight,” *The Wall Street Journal*, February 17, 2015 (<http://www.wsj.com/articles/tech-companies-are-caught-in-the-middle-of-terror-fight-1424211060>); AFP, “France Seeks Silicon Valley Allies in the War on Terror,” *Daily Mail*, February 21, 2015 (<http://www.dailymail.co.uk/wires/afp/article-2963161/France-seeks-Silicon-Valley-allies-war-terror.html>).

48 Quoted in Gauthier-Villars and Schechner, “Tech Companies are Caught in the Middle of Terror Fight,” *The Wall Street Journal*, February 17, 2015 (<http://www.wsj.com/articles/tech-companies-are-caught-in-the-middle-of-terror-fight-1424211060>).

49 See Moody, “New Dutch Law Would Allow Bulk Surveillance, Compelled Decryption,” *Arstechnica UK*, July 3, 2015 (<http://arstechnica.co.uk/tech-policy/2015/07/new-dutch-law-would-allow-bulk-surveillance-compelled-decryption/>).

50 See, e.g., Wong, “Why Encryption Backdoors Threaten Human Rights”, *The Hill*, July 8, 2015 (<http://thehill.com/blogs/congress-blog/technology/247145-why-encryption-back-doors-threaten-human-rights>).

51 Reports available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf and http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

52 U.N. Human Rights Council June 30, 2014 Report at ¶ 25, p. 9.

53 U.N. Human Rights Council May 22, 2015 Report at ¶ 60, p. 20.

54 U.N. Human Rights Council June 30, 2014 Report at ¶ 23, p. 8.

55 U.N. Human Rights Council May 22, 2015 Report at ¶ 32, p. 11.

56 U.N. Human Rights Council May 22, 2015 Report at ¶ 33, p. 11.

57 U.N. Human Rights Council June 30, 2014 Report at ¶ 25, pp. 8-9; U.N. Human Rights Council May 22, 2015 Report at ¶ 34, p. 12.

58 U.N. Human Rights Council May 22, 2015 Report at ¶ 32, p. 11.

59 U.N. Human Rights Council June 30, 2014 Report at ¶ 24, p. 8; U.N. Human Rights Council May 22, 2015 Report at ¶ 33, p. 11.

60 See *supra* Point IV.

61 See open letter to President Barack Obama, May 19, 2015 (https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf). See also Lumb, “Major Tech Companies, But Not Amazon, Sign Letter to Obama Against Security Backdoors (Updated),” *Fast Feed*, May 19, 2015 (<http://www.fastcompany.com/3046469/fast-feed/major-tech-companies-but-not-amazon-sign-letter-to-obama-against-security-backdoor>); Essers, “Tech Industry Redoubles Efforts to Fight US Gov’t Encryption Backdoors,” *PCWorld*, June 9, 2015 (<http://www.pcworld.com/article/2933397/tech-industry-redoubles-efforts-to-fight-us-govt-encryption-backdoors.html>).

62 Open letter to President Barack Obama, May 19, 2015 (https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf).

63 See, e.g., *U.S. v. Global Fishing, Inc.*, 634 F.3d 557, 563 (9th Cir. 2011).

64 28 U.S.C. § 1782. A letter rogatory is a formal request from a court to a foreign court for judicial assistance. Judicial assistance could be requested, for example, to aid with obtaining certain testimony or the service of process.

65 28 U.S.C. § 1782.

66 *U.S. v. Global Fishing, Inc.*, 634 F. 3d at 572 (quoting *In re Request for Judicial Assistance from the Seoul District Criminal Court, Seoul, South Korea (Young Sool Shin v. U.S.)*, 555 F.2d 720, 724 (9th Cir. 1977)). Furthermore, it bears note that the problem identified by the technology companies may be more academic than real. Most countries do not recognize the right against self-incrimination, as the U.S. does, and may use coercion to obtain passcodes, rather than use the elaborate and exacting U.S. judicial process.

67 Copies of the letters are included in the appendix to this report.

APPENDIX I

To: Each of the Members of the Assembly and Senate in New York State

From: Each of the 62 District Attorneys in New York State

Date: April 16, 2015

Re: Our urgent need for legislation requiring companies to make smartphones amenable to lawful searches

We, the 62 District Attorneys of New York State, write to alert you to an urgent problem, and to encourage you to solve the problem through appropriate legislation.

The Problem

Digital evidence plays a crucial role in the vast majority of criminal cases across our state, and, indeed, across the nation. Because so many people put extensive information on their smartphones and hand-held devices, those devices may contain photos, texts, voice messages, or emails that will constitute relevant evidence in virtually every kind of case. We have used material from smartphones to prosecute murders, rapes, kidnappings, fraud, and larceny, among other crimes.

For law enforcement to access the contents of a smartphone or similar device, we typically need and obtain a search warrant.¹ It should be noted that a search warrant cannot be issued unless the applicant demonstrates, to a judge, that there is both probable cause to believe a crime has been committed and probable cause to believe the device contains evidence of that crime. If a smartphone is protected by a passcode, however, then even though the search warrant gives us the legal right to access the contents of the phone, we cannot review the material on the phone because we cannot get “through” the passcode.

Historically, in such instances we have been able to seek the aid of the mobile operating system providers. Upon our presentation to them of the warrant, they have been able to unlock the phones, and provide the information on the phone that was responsive to the warrants.

In the past few months, however, the companies have deliberately designed software, entire operating systems, and mobile devices such that even *they* cannot unlock passcode-protected phones. The companies have touted this development, explicitly advertising their inability to comply with lawful government requests.² As a consequence, the search warrant becomes a nullity, because even law enforcement officers possessing valid search warrants or court orders cannot access the contents

¹ See *Riley v. California*, ___ U.S. ___, 134 S. Ct. 2473 (2014).

² See, e.g., Apple web site: (“On devices running iOS 8, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. **Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8.**”) (Emphasis added). (available at <https://www.apple.com/privacy/government-information-requests/>) (last visited, January 28, 2015). Unfortunately, Google has designed its latest version of the Android operating system so that, like Apple’s iOS 8, it is beyond the reach of lawful search warrants. See, e.g., *Newest Androids will join iPhones in offering default encryption, blocking police*, The Washington Post, September 18, 2014 (available at <http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/>) (last visited February 10, 2015).

of passcode-protected smartphones. In other words, criminals using passcode-protected devices have been granted license to evade a lawful order of a court and are thus quite literally, protected in their criminal endeavors.

It is as if the police get a search warrant for a safe deposit box at a bank because they have reason to believe that the safe deposit box has evidence of a crime -- but they cannot open the box because the bank has thrown away its own key. Indeed, this situation is even worse because whereas a safe deposit box can, ultimately, be opened by force, a passcode-protected smartphone is virtually impregnable, unless the companies maintain the ability to open the phones that it manufactures.

Although the companies tout their new software as a boon for their users' privacy, users' privacy is adequately protected by the Fourth Amendment, and specifically the requirement that a judge or magistrate – that is, a neutral party – issue a search warrant only upon a showing of probable cause that the phone will contain evidence of a crime.³

The fact is that, although the new software may enhance privacy for some users, it severely hampers law enforcement's ability to aid victims. All of the evidence contained in smartphones and similar devices will be lost to law enforcement, so long as the criminals take the precaution of protecting their devices with passcodes. Of course they will do so. Simply stated, passcode-protected devices render lawful court orders meaningless and encourage criminals to act with impunity. The ultimate losers in this equation are crime victims.

The need for a legislative solution

The United States Attorney General, the director of the FBI, and others have severely criticized the companies' efforts to keep evidence immune from lawful process.⁴ Criticism, however, is not enough. The companies benefit immeasurably from the laws protecting intellectual property, as well as from extensive federal regulation. They should not be able to thumb their noses at law enforcement when, with warrant in hand, it comes to seek their help. The safety of the citizenry calls for a legislative solution, and a solution is easily at hand.

We would propose that the New York State Legislature pass the following bill, to penalize those who would sell smartphones that are beyond the reach of law enforcement. If enacted, this bill would provide a significant deterrent to such sellers, and therefore would discourage the companies from continuing to provide such smartphone software.

³ U.S. Const., amend. IV; *see also, e.g., United States v. Karo*, 468 U.S. 705, 717 (1984) (“The primary reason for the warrant requirement is to interpose a ‘neutral and detached magistrate’ between the citizen and ‘the officer engaged in the often competitive enterprise of ferreting out crime.’ *Johnson v. United States*, 333 U.S. 10, 14 (1948).”).

⁴ *See, e.g., FBI Director Calls On Congress To 'Fix' Phone Encryption By Apple, Google*, Huffington Post October 16, 2014 (available at http://www.huffingtonpost.com/2014/10/16/james-comey-phone-encryption_n_5996808.html) (last visited, January 28, 2015); *US top cop decries encryption, demands backdoors*, Arstechnica, October 1, 2014 (available at <http://arstechnica.com/tech-policy/2014/10/us-top-cop-decries-encryption-demands-backdoors/>) (last visited, January 28, 2014).

Proposed Statutory Language

The general business law is amended by adding new section 902 to read as follows:

§ 902 Smartphones

1. For the purposes of this section, the following terms have the following meanings:
 - (A) A “Smartphone” means a cellular radio telephone or other mobile voice communications handset device that includes the following features:
 - (i) Utilizes a mobile operating system.
 - (ii) Possesses the capability to utilize mobile software applications, access and browse the Internet, utilize text messaging, utilize digital voice service, and send and receive email.
 - (iii) Has wireless network connectivity.
 - (iv) Is capable of operating on a long-term evolution network or successor wireless data network communication standards.
 - (B) “Sold in New York,” or any variation thereof, means that the smartphone is sold at retail from a location within the state, or the smartphone is sold and shipped to an end-use consumer at an address within the state. “Sold in New York” does not include a smartphone that is resold in the state on the secondhand market or that is consigned and held as collateral on a loan.
 - (C) “Leased in New York,” or any variation thereof, means that the smartphone is contracted for a specified period of time to an end-use consumer at an address within the state.
2. Any smartphone that is manufactured on or after XX, and sold or leased in New York, shall be capable of being decrypted and unlocked by its manufacturer or its operating system provider.
3. The sale or lease in New York of a smartphone manufactured on or after XX that is not capable of being decrypted and unlocked by its manufacturer or its operating system provider shall subject the seller or lessor to a civil penalty of \$2,500 for each smartphone sold or leased if it is demonstrated that the seller or lessor of the smartphone knew at the time of the sale or lease that the smartphone was not capable of being decrypted and unlocked by its manufacturer or its operating system provider. No seller or lessor who pays the civil penalty may pass any portion of that penalty on to any purchaser of smartphones by raising the sales or lease price of smartphones.
4. The retail sale or lease of a smartphone manufactured on or after XX that is not capable of being decrypted and unlocked by its manufacturer or its operating system provider shall not result in liability to the seller or lessor if the inability of the manufacturer and operating system provider to decrypt and unlock the smartphone is the result of actions taken by any person or entity other than the manufacturer, the operating system provider, the seller, or the lessor so long as such actions were unauthorized by the manufacturer, the operating system provider, the seller, or the lessor *unless* at the time of sale or lease the seller or lessor had received notification that the manufacturer and operating system provider were unable to decrypt and unlock smartphones that had been acted upon in the manner described above.
5. A civil suit to enforce this section may be brought by the following parties and none others: (a) the Attorney General, for any sale or lease of a smartphone in New York, and (b) the district

attorney for any sale or lease of a smartphone in the county represented by the district attorney, *provided however* that the seller or lessor may be subject to not more than a single penalty for each sale or lease of a smartphone.

Conclusion

New York can and should lead the nation in protecting its citizens, and in responding to the misguided and dangerous attempts by digital device manufacturers to turn digital devices into virtual safes that, being beyond the reach of law enforcement, are havens for criminals. Revelations in the recent past about NSA surveillance and similar government intrusions on privacy have made people acutely aware of threats to their privacy. We are not proposing that peoples' privacy be limited. Peoples' privacy is protected by the warrant requirement, as it always has been. This bill would help to protect New Yorkers. We urge that you support it.

APPENDIX II



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

CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

March 31, 2015

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

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

Dear Jane,

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

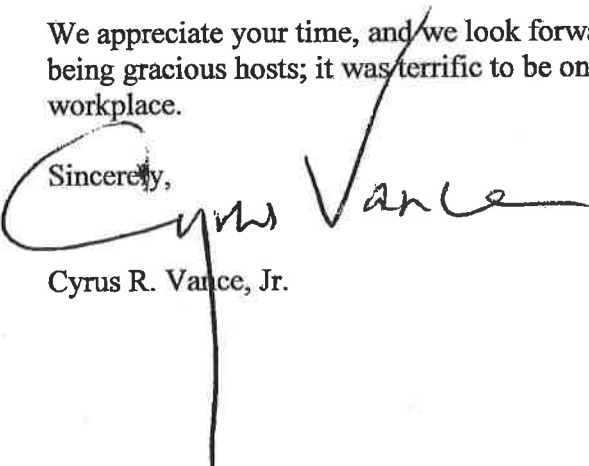
For us better to understand some of the concerns that you expressed at our meeting, we have some additional questions which we hope that you can answer the following questions:

1. There was much discussion at our meeting about mobile phone data being “backed up” in the Cloud. Therefore, could you please advise us:
 - a. What percentage of Apple mobile device users have associated iOS backups stored on Apple’s iCloud servers?
 - b. What percentage of current Apple mobile device users have the iCloud backup option turned on?
 - c. What percentage of current Apple mobile device users have utilized iCloud backup to produce at least one backup stored with Apple?
 - d. What is the retention period of an iCloud backup if the user decides to turn off iCloud backup?
 - e. Are the iOS8 backups stored on the iCloud encrypted?

2. As we explained, our view is that the judicially-issued search warrant is the bulwark for the protection of people's privacy. I understood that Apple believes that if Apple kept a "key" so that it was able to open locked iPhones, some foreign authorities might compel Apple to open iPhones and thus use them against their own citizens. That leads to the following questions:
 - a. Is it accurate that, after the iOS8 upgrade, Apple no longer maintains the ability to unlock iPhones running on iOS8 anywhere in the world market? For example, does Apple no longer maintain the ability to unlock iPhones running iOS8 that it sells in China, India, or other world markets outside of the United States? Even if Apple does not maintain the ability to unlock devices running on iOS8, does Apple provide any foreign agency or entity the right or ability to unlock iOS8 devices?
 - b. In the past five (5) years, how many demands have there been from foreign jurisdictions to unlock iPhones, and has phone content been provided to those jurisdictions in response?
 - c. For the instances identified in 2(b) above, were those demands from foreign jurisdictions made directly to Apple, or through letters rogatory, or in some other fashion?
3. If Apple kept a "key" so that it was able to unlock iPhones, would the iPhones be more vulnerable to hackers than if Apple had no such "key"? Is there any "key" or similar device that Apple might keep without sacrificing the security of iPhones from hackers? Is there a way to measure or quantify the vulnerability to hackers of iPhones (a) if Apple kept a key, as compared to (b) if it did not keep a key?

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

Sincerely,


Cyrus R. Vance, Jr.



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

CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

April 1, 2015

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

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

Dear Kent,

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

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

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

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

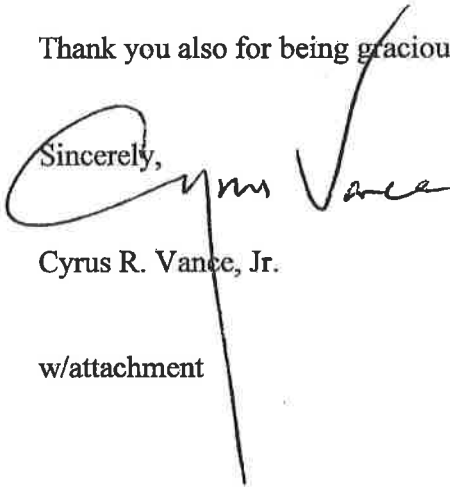
1. In response to our concern about our inability to extract data from cellular phones with full device encryption, it was suggested to us that an alternative means to obtain some of the data from the device would be to obtain data "backed up" to the cloud. Therefore, could you please advise us:
 - a. What percentage of Android mobile device users have associated backups stored on servers?
 - b. What percentage of current Android mobile device users have the backup option turned on?

- c. What percentage of current Android mobile device users have utilized cloud backup to produce at least one stored backup?
 - d. What is the retention period of a cloud backup if the user decides to turn off the backup?
 - e. Are the backups stored on the cloud currently encrypted? If it is not currently encrypted, are their plans to encrypt the cloud content and what is the timeline for such implementation?
2. If Google kept a "key" so that it was able to unlock phones, would the phones be more vulnerable to hackers than if Google had no such key? Is there any key or similar device that Google might keep without sacrificing the security of Android devices from hackers? Is there a way to measure or quantify the vulnerability to hackers of Android phones (a) if Google kept a key, as compared to (b) if it did not keep a key?

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

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

Sincerely,

A handwritten signature in black ink, appearing to read "Cyrus R. Vance, Jr.", with a long vertical line extending downwards from the end of the signature.

Cyrus R. Vance, Jr.

w/attachment



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu