THIRD REPORT OF THE
MANHATTAN DISTRICT ATTORNEY'S
OFFICE ON

SMARTPHONE ENCRYPTION AND PUBLIC SAFETY

November 2017

CONTENTS

Introduction

In November 2015, this office issued a white paper titled *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* ("the 2015 Report").[1] The focus was an announcement a year earlier by Apple Inc. that its latest 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, even to Apple, and even in the face of a judicially-issued search warrant. As discussed in the 2015 Report, Apple's decision was almost immediately followed by Google.[2]

The 2015 Report detailed the devastating impact of this business decision on criminal investigations, big and small, across the country. These days, such investigations almost always rely to some degree on evidence contained on smartphones and other devices, and criminals of all sorts responded with enthusiasm to the news that they could now conduct business on such devices without fear that their correspondence would become the stuff of criminal prosecution. The 2015 Report described the particular value of data stored on smartphones, and the real-world consequences of full-disk encryption to public safety. It explained that, prior to Apple's encryption decision, there was no evidence that Apple devices were particularly susceptible to hacking, and that law enforcement's reliance on judicially-issued search warrants protected personal privacy interests, as search warrants have done in other contexts for over two hundred years. Finally, the 2015 Report predicted that the decisions by Apple and Google would yield a counterproductive "arms race" between the companies and law enforcement unless legislation was enacted.

In November 2016, this office issued an update to the 2015 Report ("the 2016 Report"), which described the unfolding public-safety impact of the Apple and Google encryption schemes, and the gathering debate on how the public and private sectors should respond to the competing challenges of protecting the public in criminal inquiries while ensuring that individual privacy interests were not compromised.[3] In particular, the 2016 Report discussed examples, including the recent San Bernardino massacre, to demonstrate that the public safety issues created by full-disk encryption were growing. The 2016 Report also emphasized that the dichotomy between privacy and security in the encryption debate is illusory, since lawful searches can be performed while still maintaining security and safeguarding users' privacy rights. Finally, it detailed the efforts of our nation's courts to adjudicate legal issues arising as a result of full-disk encryption, and concluded that litigation is an ineffective means of solving this problem.

---

[1] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, November 18, 2015, *available at* http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

[2] *Id.* at i.

[3] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An update to the November 2015 Report*, November 17, 2016, *available at* http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

This is our office's third annual Report, which provides a further update on the ongoing debate, and how these encryption policies - enacted by companies for their own commercial reasons - continue to frustrate efforts to solve crimes and protect the public on a daily basis. Unfortunately, the news is not good: although law enforcement has had some success using workarounds (*see* Section II, *infra*), those methods are costly and unavailable to the vast majority of prosecutors and investigators. As technology companies continue to roll out new devices, workarounds become less available and more expensive, creating a landscape in which solving crime depends largely on a law enforcement agency's ability to spend money on private-sector solutions. This "privatization" of crime fighting is exactly the "arms race" predicted in the 2015 Report, which will result in greater and greater expenditures on the part of federal, state, and local governments. More problematic, it will result in unequal access to justice for crime victims across the country.

By way of overview, this report addresses the following issues:

- Section I summarizes the issue as it stands in 2017, noting that the "arms race" predicted in 2015 has intensified. The number of investigations that involve full-disk encrypted smartphones continues to balloon, in cases ranging from white collar crime to homicides. To solve these crimes, law enforcement is increasingly relying on expensive "workarounds" developed by third parties, while providers work to thwart even lawful access to smartphone data. Apple's compliance with recent policy directives in China demonstrates that technology companies can only be relied upon to provide assistance to law enforcement when there is a legislative requirement or a clear business reason to do so.

- Section II deals with the emerging argument that encryption "workarounds" are the solution to the problem. The term "workarounds" refers generally to any means by which law enforcement can access the plaintext (i.e., unencrypted) data on a device without assistance from the end user or the software manufacturer. While workarounds like "lawful hacking" have been used by law enforcement with some success over the past year, they are not a realistic solution to the problem going forward – they are time-consuming and costly, and become obsolete when new devices and operating systems are released, creating an endless cat-and-mouse system that strains resources and undermines public safety.

- Section III provides an overview of recent judicial developments. Law enforcement officials have, in some instances, sought orders to compel users to provide plaintext copies of their data, and such requests have on occasion been granted requiring users to unlock their devices using the fingerprint sensor technology. But judicial authority on the Fourth and Fifth Amendment implications of these orders remains divided, and Apple's recent iOS features make it unlikely that such orders will be a viable path forward. More importantly, orders compelling this type of assistance, even when granted, can be of limited practical utility.

- Section IV provides an overview of international efforts to address this issue. Recognizing the public safety implications of default device encryption, and the need for a legislative solution, nations including Germany, France, and the United Kingdom have proposed laws that would require providers to render reasonable assistance when presented with a lawfully-issued order.

- Section V concludes by reiterating that a legislative solution that compels compliance with court-ordered production of plaintext data is necessary to ensure that justice is served in criminal cases, without regard to where crimes occur or the third-party resources available.

I. In the Absence of Legislation, the Public/Private "Arms Race" Over Encryption Has Intensified

As the era of default device encryption enters its fourth year, the inaccessibility of smartphone data remains, in more and more cases, an insurmountable obstacle for law enforcement and victims of crime. In one recent and tragic example, federal law enforcement officials investigating the mass shooting at First Baptist Church in Sutherland Springs, Texas on November 5, 2017 – the deadliest shooting in Texas history – publicly acknowledged that they have been unable to extract evidence from a smartphone linked to the assailant.[4] Of course, investigators confront this problem daily in less publicized cases. Criminals, like everyone else, operate increasingly in the digital realm. Traditional investigative techniques – searches of targets' homes, physical surveillance, wiretaps on telephones – often fall short when it comes to gathering enough evidence to solve and prosecute today's criminal activity. Unfortunately, much of today's evidence exists in a space that, prior to 2014, was largely unheard-of: warrant-proof smartphones that have been designed to keep law enforcement out.[5]

---

[4] Simon Romero et al., *Texas Gunman Once Escaped From Mental Health Facility*, N.Y. Times, Nov. 7, 2017, *available at* https://www.nytimes.com/2017/11/07/us/texas-shooting-church.html?_r=0 (quoting Special Agent in Charge Christopher H. Combs: "Unfortunately, at this point in time, we are unable to get into that phone," and refusing to name the brand of phone so as not to encourage other criminals to seek out that make and model). For its part, Apple has suggested that if law enforcement had requested assistance within 48 hours of the shooting, Apple may have been able to offer suggestions for accessing the phone's contents (presumably by using the TouchID unlock feature). *See* Karma Allen, *Apple Says it Reached out to FBI to Assist with Texas Shooter's Phone*, ABC News, Nov. 9, 2017, *available at* http://abcnews.go.com/US/apple-reached-fbi-assist-texas-shooters-phone/story?id=51033326.

[5] Although encryption is used today to shield numerous categories of data, this Report focuses (as the previous Reports did) specifically on default, warrant-proof smartphone encryption. This technology, referred to herein as "default device encryption," pertains exclusively to data at rest (the data stored on a user's phone); the report does not discuss encryption of data in motion (or "end-to-end" encryption), which applies to information that is transmitted from one user to another. Nor does it discuss "off-the-shelf" encryption software that is widely available to users of electronic storage and communication devices. Instead, the report is limited to the technology that, by default, renders data on a smartphone impenetrable to law enforcement, regardless of judicial authorization to search the device. This technology poses a particular threat to public safety because it operates by default, on the devices that are now ubiquitous in our culture.

As Deputy Attorney General Rod Rosenstein recently observed:

> Encrypted communications and devices pose the greatest threat to public safety when they are part of mass-market consumer devices and services that enable warrant-proof encryption by default. No solution will be perfect. If only major providers refrain from making their products safe for terrorists and criminals, some sophisticated criminals may migrate to less-used platforms. But any progress in preserving access to communications methods used by most criminals and terrorists would still be a major step forward. The approach taken in the recent past — negotiating with technology companies and hoping that they eventually will assist law enforcement out of a sense of civic duty — is unlikely to work. Technology companies operate in a highly competitive environment. Even companies that really want to help must consider the consequences. Competitors will always try to attract customers by promising stronger encryption.[6]

A. Investigators Are Increasingly Forced to Reply on Expensive "Lawful Hacking" Alternatives

As this office and other observers predicted when iOS 8 was announced, the encryption decisions by Apple and other technology companies have resulted in a costly cycle in which law enforcement has expended significant resources attempting to obtain lawful access to smartphones, while the technology sector has expended far greater resources to prevent such access. We are in the midst of the "untenable arms race" discussed in the 2016 Report, "in which private industry makes devices that are more and more inaccessible, and the government chases after industry, straining to find more and more sophisticated ways to hack lawfully into the devices."[7]

While law enforcement has had some success (with the aid of paid outside vendors) accessing encrypted smartphones once a warrant is obtained, these efforts come with a hefty price tag (for example, it was widely reported that the FBI's efforts to unlock the phone belonging to one of the San Bernardino shooters resulted in an expenditure of around $1 million[8]). This creates a vicious cycle: each time a new device or operating system is released, "lawful hacking" companies spend months or years searching for vulnerabilities to exploit; in response, the tech industry spends time and money to "patch" every vulnerability that law enforcement exposes. Putting aside the costs incurred, in many cases the access to smartphone data comes too late, after statutes of limitations or speedy trial requirements have run out. Of

---

[6] Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy, Oct. 11, 2017, *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

[7] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An update to the November 2015 Report*, *supra* note 3, at 7, 30.

[8] *See, e.g.,* Mark Hosenball, *FBI Paid Under $1 Million to Unlock San Bernardino Phone: Sources*, Reuters, Apr. 28, 2016, *available at* https://www.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUSKCN0XQ032.

course, most state and local law enforcement agencies do not have the resources of the federal government or this office, and cannot afford to rely on expensive lawful hacking solutions in everyday investigations (and, of course, the overwhelming majority of criminal cases in this country are handled by state and local agencies).[9]

None of this is likely to subside anytime soon. For example, this office has recovered (and obtained court-ordered warrants or consent to search) 1,200 devices in the first ten months of 2017. Of those, over 700 were locked using full-disc encryption. Over half of all devices received by our digital forensics unit are locked when we receive them; 72% of Apple devices, and 37% of Android devices. As the following table depicts, these numbers have increased steadily since 2014:

SMARTPHONE ENCRYPTION STATISTICS
October 1, 2014 – October 31, 2017

	2014	2015	2016	2017	Grand Total
iOS					
Unlocked	40	145	171	199	555
Locked	59	382	538	466	1445
iOS Total	**99**	**527**	**709**	**665**	**2000**
ANDROID					
Unlocked	103	324	371	382	1180
Locked	19	188	259	236	702
ANDROID Total	**122**	**512**	**630**	**618**	**1882**
Grand Total	**221**	**1039**	**1339**	**1283**	**3882**

On the federal side, the FBI reports that approximately 7,000 devices – more than half of those seized this fiscal year – remain inaccessible due to default encryption.[10] At the state

[9] *See* Bureau of Justice Statistics, *Felony Sentences in State Courts, 2004*, July 1, 2007, *available at https://www.bjs.gov/index.cfm?ty=pbdetail&iid=909* (94% of felony convictions occurred in state court, the remaining 6% in federal court).

[10] Michael Balsamo, *FBI Couldn't Access Nearly 7K Devices Because of Encryption*, Oct. 23, 2017, Forensic Mag, *available at* https://www.forensicmag.com/news/2017/10/fbi-couldnt-access-nearly-7k-devices-because-encryption?et_cid=6147116&et_rid=454847037&location=top&et_cid=6147116&et_rid=454847037&linkid

level, as discussed in the 2016 Report,[11] an initiative launched by state and local law enforcement entities, in partnership with National Domestic Communications Assistance Center (NDCAC), has been collecting data from across the country about impenetrable mobile devices seized by law enforcement. So far, 238 state and local agencies have signed onto the initiative, and 160 have begun to keep track of their locked devices (these 160 agencies come from 37 states). The total number of locked devices so far is in the thousands, and is growing every day.

B. Technology Companies Continue to Make Encryption Decisions Based on Their Own Private Business Interests

Like all businesses, technology firms make decisions based on commercial interests, not public policy concerns. Without legislative action, these corporations will "continue to focus on customer and shareholder value," while government entities will "try to demonstrate the critical public safety price they (meaning we) pay for 'warrant-proof' platforms."[12] In this regard, Apple's refusal in recent years to accede to court orders and legitimate requests from law enforcement[13] stands in stark contrast to its conduct in China. There – to the dismay of privacy advocates and others[14] – Apple has recently complied with the government's directives that businesses locate their servers within mainland China, and has taken other steps that pose threats to customer privacy.[15] (Not surprisingly, China is Apple's second-largest market.)

=https%3a%2f%2fwww.forensicmag.com%2fnews%2f2017%2f10%2ffbi-couldnt-access-nearly-7k-devices-because-encryption%3fet_cid%3d6147116%26et_rid%3d%25%25subscriberid%25%25%26location%3dtop.

[11] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An update to the November 2015 Report*, *supra* note 3, at 10.

[12] Daniel Richman, *Getting Encryption onto the Front Burnder*, Lawfare, Oct. 26, 2017, *available at* https://www.lawfareblog.com/getting-encryption-front-burner.

[13] For example, in response to a court order requiring Apple to assist the F.B.I. in the wake of the 2015 San Bernardino attack, CEO Tim Cook asserted that helping the government unlock the terrorist's phone would set "a dangerous precedent" that would "undermine the very freedoms and liberty our government is meant to protect." Tim Cook, *A Message to Our Customers*, Apple, Feb. 16, 2016, *available at* https://www.apple.com/customer-letter.

[14] *See* Cory Bennett and Katie Bo Williams, *Apple Defends China Moves Amid FBI spat*, The Hill, Mar. 20, 2016, *available at* http://thehill.com/policy/cybersecurity/273629-apple-defends-china-moves-amid-fbi-spat; Stewart Baker, *Deposing Tim Cook*, Wash. Post, Feb. 25, 2016, *available at* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/25/deposing-tim-cook/?utm_term=.b6c590a5c967; Amul Kalia and Eva Galperin, Electronic Frontier Foundation, *Deciphering China's VPN Ban*, Aug. 2, 2017, *available at* https://www.eff.org/deeplinks/2017/08/deciphering-chinas-vpn-ban ("Apple took a dispiriting step in the policing of its Chinese mainland App store … the company has once again aided the Chinese government in its censorship campaign against its own citizens").

[15] Apple has made other concessions to the Chinese government in recent years, including: removing Virtual Private Network (VPN) apps from the China App Store, removing news apps created by The New York Times, and submitting new iPhone models to "security audits" before they can be sold in China. *See generally* Farhad Manjoo, *Apple's Silence in China Sets a Dangerous Precedent*, N.Y. Times, July 31, 2017, *available at* https://www.nytimes.com/2017/07/31/technology/apple-vpn-china-dangerous-precedent.html?_r=1; *Apple and Other Tech Titans Should Tread Carefully in China*, Wash. Post, July 22, 2017, *available at* https://www.washingtonpost.com/opinions/apple-and-other-tech-titans-should-tread-carefully-in-china/2017/07/22/1734eaca-6b1e-11e7-9c15-177740635e83_story.html?utm_term=.07d8823b2d1a.

Notably, the Chinese government imposed these new requirements through legislation, not by seeking court orders, and Apple's CEO Tim Cook, in defending Apple's decisions in China, stated simply, "we follow the law wherever we do business."[16] In other words, the only way to resolve the encryption dilemma in the United States will be through legislation too.

In growing recognition of this reality, lawmakers on both sides of the aisle are acknowledging that companies in the technology sector will necessarily act in their own self-interests absent regulatory oversight, even if the result is contrary to the interests of public policy or public safety. Revelations about Google, Facebook, and Twitter profiting from the proliferation of "fake news" advertisements in the run-up to the 2016 election have drawn scrutiny from Congress, with some senators supporting disclosure requirements for political advertisements.[17] Targeted advertising based on hate speech has also drawn ire.[18] Facebook and Google recently lobbied to prevent the passage of a bipartisan bill that would enable the prosecution of companies that facilitate sex trafficking on their websites.[19] One of the bill's sponsors, Senator Richard Blumenthal of Connecticut, noted that in today's climate there is "much stronger agreement among me and my colleagues that there needs to be more aggressive enforcement action on tech companies like Google."[20]

As lawmakers turn their attention to regulatory oversight of the technology industry, the question of court-ordered access to lawfully-seized encrypted devices must not be overlooked. It is an issue that affects citizens and businesses victimized by crime, law enforcement agencies tasked with ensuring public safety, and the judges and juries who make critical judgments in criminal cases.

II. Recent Developments Have Continued to Show that Temporary Workarounds are Not a Solution

As discussed above, the debate over lawful access to smartphone evidence has, in some quarters, shifted away from whether technology companies should be required to comply with court orders to the purported availability of alternative means for investigators to "break into" devices – generally referred to as "workarounds." Rather than pursue a legislative solution, some argue, we should require law enforcement to rely on workarounds to execute search

---

[16] Saheli Roy Choudhury, *Apple CEO Tim Cook Defends Decision to Remove VPN Apps in China*, CNBC.COM, Aug. 1, 2017, *available at* https://www.cnbc.com/2017/08/01/apple-ceo-tim-cook-defends-decision-to-remove-vpn-apps-in-china.html.

[17] Cecelia Kang, *Internet Giants Face New Political Resistance in Washington*, N.Y. Times, Sept. 20, 2017, *available at* https://www.nytimes.com/2017/09/20/technology/internet-giants-face-new-political-resistance-in-washington.html.

[18] Sapna Maheshwari and Alexandra Stevenson, *Google and Facebook Face Criticism for Ads Targeting Racist Sentiments*, N.Y. Times, Sept. 15, 20117, *available at* https://www.nytimes.com/2017/09/15/business/facebook-advertisingantisemitism.html?action=click&contentCollection=Technology&module=RelatedCoverage&region=EndOfArticle&pgtype=article.

[19] *Id.*

[20] *Id.*

warrants and access data.[21] Workarounds include some straightforward solutions, such as guessing a user's password or obtaining the device while it is in use (and therefore unlocked). Obviously, those solutions are of limited utility because they depend largely on luck and are not feasible in the vast majority of cases. A more sophisticated and commonly-cited workaround is to exploit a flaw in the encryption scheme.[22] In other words, law enforcement, either alone or in conjunction with a third-party contractor, must find a way to break a device's encryption. This has powered an emerging market for "lawful hacking" products, which has its own adverse implications for both information security and transparency.[23]

Faced with growing backlogs of encrypted devices, some law enforcement agencies have begun working with private-sector partners to attempt to develop workarounds to obtain contents from otherwise "warrant-proof" Apple and Android phones. This office, with our relatively considerable resources, is one of the few local agencies that can afford to pursue this kind of solution. Other offices lack such resources, which creates an unequal system in which access to justice depends on a particular jurisdiction's financial capacity. Examples of some of our "workaround" efforts are summarized below.

- In a sexual assault case, we recovered an iPhone 4S running iOS 8 from a defendant who is charged with abusing his niece, a child, over a long period of time. Information provided by the victim suggested that there would be evidence of the assaults on the phone, and so we obtained a search warrant. Because of Apple's default encryption, we were unable to unlock the phone for several months. Recently, with the assistance of a paid third party, we accessed the phone. Videos were recovered depicting numerous sexual assaults by the defendant, which corroborated the testimony of the child witness. It is impossible to overstate the value of this kind of direct evidence, particularly in a case where the only eyewitness is a child victim.

- In a homicide case, an iPhone 6 running iOS 8 was recovered from the victim, who had been stabbed to death on the street. Because the device belonged to the decedent, there was no privacy issue – a search warrant would not have been necessary. Nonetheless, default device encryption

[21] *See, e.g.*, Orin Kerr & Bruce Schneier, *Encryption Workarounds*, GWU Law School Public Research Paper No. 2017-22, May 22, 2017; Ben Buchanan, *Bypassing Encryption: "Lawful Hacking" is the Next Frontier of Law Enforcement Technology*, Salon.com, Mar. 22, 2017; Alina Selyukh, *Lawful Hacking: Should, or Can, the FBI Learn to Overcome Encryption Itself?*, npr.org, Apr. 19, 2016.

[22] *See* Kerr & Schneier, *Encryption Workarounds*, GWU Law School Public Research Paper No. 2017-22, May 22, 2017.

[23] Daniel Richman, *Getting Encryption onto the Front Burner*, Lawfare, Oct. 26, 2017, *available at* https://www.lawfareblog.com/getting-encryption-front-burner ("We already face the risk of government hacking tools escaping. How much greater is the risk when the market expands? Moreover, if forced to rely on vulnerability exploitation, law enforcement cannot be expected to tolerate the disclosure of each tool – developed or bought – whenever they bring a prosecution using its fruits.").

prevented a search of the phone. Approximately two years later, with the assistance of a paid private vendor, we were able to access the phone's contents. The phone contained videos, taken less than an hour before the murder, showing the defendant and the victim together. This material was vitally important to the case, and was unavailable via any other means.

- Another homicide case involved a woman who was killed and then burned in a Manhattan building. A suspect was identified, but his relationship to the victim was unknown. Several months after the crime, we were able to unlock the suspect's phone, again with third-party assistance. The phone contained chats between the suspect and the victim, establishing their relationship as well as a timeline for the murder.

- In a sexual assault case, the defendant assaulted the victim after breaking into her home. He later claimed that he was intoxicated and committed the crimes by mistake. Evidence obtained from his locked smartphone, particularly text messages and internet history from immediately prior to the incident, refuted that claim and conclusively established his intent.

- In a multi-defendant homicide case, the victim's phone was unlocked with third-party assistance after several months. The phone revealed a text sent from the victim's phone by one of the defendants, attempting to gain access to the victim's safe.

- In a complex larceny scheme, two suspects were acting together to commit credit card fraud. One suspect's phones were unlocked with the assistance of a third party; the other suspect's phones were inaccessible. On the unlocked phones, investigators saw dozens of additional stolen credit card accounts, linking that suspect to months' worth of fraud. The other suspect, despite likely involvement in that fraud, cannot be charged.

These examples confirm what state and local law enforcement agencies have been saying since 2014: default device encryption results in evidence, whether exculpatory or incriminating, being removed from consideration by prosecutors, investigators, judges, and juries. Because obtaining this evidence is extremely costly in the expanding "lawful hacking" marketplace (the overall cost of these workarounds to our office to date is in the hundreds of thousands of dollars), it is available only in cases handled by a small minority of well-funded agencies. Crime victims thus have unequal access to justice, depending on the resources of the city or county in which they live.

Putting aside cost, these workarounds, by definition, lag behind smartphone technology; each time a new device or operating system is released, it takes months, and sometimes years, for lawful hacking solutions to catch up. That time can mean that evidence is not available when investigators and prosecutors need it, and no amount of money can change that.

Finally, smartphone data can also be critical in exonerating innocent defendants. For example, in one recent case, two men were indicted for a gunpoint robbery based, in part, on eyewitness identifications. The eyewitnesses were steadfast, but one defendant was adamant he had not been involved. Data extracted from his co-defendant's smartphone revealed the true identity of the other perpetrator, confirming that this defendant had been misidentified and wrongfully charged. His case was accordingly dismissed. Without this evidence, the case against the misidentified defendant might have gone forward, resulting in a miscarriage of justice.[24]

III. Court Decisions Again Demonstrate a Judicial Remedy is Not Realistic

With efforts to obtain court-ordered decryption assistance from technology companies at a standstill, investigators and prosecutors have few alternative means to access encrypted devices. As discussed above, they can employ techniques, at a significant cost, to try to break encryption on their own. Alternatively, they can attempt to obtain the passcodes for encrypted devices from the devices' users. This is not always feasible – users might be unknown, unavailable, or deceased. When the users are known and available, they will often be suspects in a criminal investigation, and obtaining their cooperation presents a host of issues.

From a legal standpoint, as discussed in the 2016 Report, the issue is that the compelled production of a user's passcode generally implicates that person's Fifth Amendment privilege against self-incrimination.[25] Whether and how law enforcement can compel a user to unlock his or her device depends on how courts view the Fifth Amendment's protections in this context. The 2016 Report described the framework in which courts apply the Fifth Amendment, and discussed some recent outcomes in cases involving "decryption orders." Over the past year, courts have continued to address government requests for decryption orders, but no clear trends have emerged.

---

[24] It might seem likely that, where a smartphone contains exonerating evidence, the user will simply consent to the search, making assistance unnecessary. But, for one thing, this evidence often resides on smartphones belonging to others – in the case described here, the phone belonged to a (properly charged) co-defendant. Moreover, defendants often refuse to consent to searches of phones even when they believe there is exculpatory evidence to be found there. Frequently, there is also evidence of uncharged crimes that they do not want to disclose. Prosecutors are thus forced to make charging decisions without the benefit of what might be critical exculpatory evidence.

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

Assuming a user has properly invoked the Fifth Amendment, law enforcement may still be able to compel the user to decrypt his device by demonstrating that any privileged information sought is already known to the government – legally speaking, a "foregone conclusion."[26] Courts have held that, when the government already knows of the "existence and location" of the information it seeks, the Fifth Amendment does not apply – providing the information becomes a question of "surrender," not "testimony."[27] The 2016 Report described two divergent approaches to applying the "foregone conclusion" doctrine to decryption orders: some courts have required the government to demonstrate that the contents of the device are known ahead of time,[28] while others have asked only whether the existence of the passcode, and the user's knowledge of it, are known facts.[29] Going forward, law enforcement's ability to compel decryption, by users, of smartphones and other devices will depend largely on which of these approaches courts favor.

The question is far from settled. In March of this year, the Third Circuit Court of Appeals in Pennsylvania affirmed a contempt order against a defendant who refused to comply with a lower court's order to decrypt two hard drives.[30] According to the lower court, the government had satisfied the "foregone conclusion" test by showing that the devices existed and contained the evidence sought (*i.e.*, child pornography).[31] Because the government had already examined other devices belonging to the defendant and found child pornography on them, there was reason to believe the encrypted drives contained similar material.[32] The appeals court affirmed the contempt order, noting the government had met the burden of showing that child pornography was on the devices. By contrast, in an earlier case, a different federal court, the Eleventh Circuit Court of Appeals, rejected the government's "foregone conclusion" argument because there had been no evidence that any files existed on the devices, or that the suspect could access them.[33]

Both of these decisions turned on whether the government had shown that it knew of the existence of certain *contents* of the encrypted devices. In other words, the courts employed the more onerous test, rather than the simpler question of whether the existence of the password, and the defendant's knowledge of it, were known ahead of time. Notably though, the Third Circuit hinted that, in future cases, it might take the view that the government need only show that the password's existence is a "foregone conclusion." In a footnote, the court made a point of saying that, because it was simply reviewing the lower court's decision for

[26] *See Fisher*, 425 U.S. 391; *Doe*, 487 U.S. 201.
[27] *Id.* at 411.
[28] *See United States v. Doe*, 670 F.3d 1335 (11th Cir. 2012); *SEC v. Huang*, 2015 U.S. Dist. LEXIS 127853 (E.D. Pa. Sept. 23, 2015); and *Commonwealth v. Baust*, 89 Va. Cir. 267 (2014).
[29] *See United States v. Gavegnano*, 305 Fed. Appx. 954 (4th Cir. 2009); *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012); *Commonwealth v. Gelfgatt*, 468 Mass. 512 (2014).
[30] *United States v. Apple Mac Pro Computer et. al.*, 851 F.3d 238 (3d Cir. 2017).
[31] *Id.* at 243, 248.
[32] *Id.* at 248.
[33] *Id.* (discussing *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335 (11th Cir. 2012)).

plain error, it was not weighing in on the "correct focus" of the foregone conclusion analysis.[34] It noted that

> a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is "I, John Doe, know the password for these devices.[35]

While the court did not explicitly disagree with the Eleventh Circuit, it strongly suggested that, if presented with the issue, it would adopt the less onerous application of the foregone conclusion doctrine.

As courts are increasingly asked to decide whether to issue decryption orders, or hold defendants in contempt for violating them, it is possible that the view espoused in the Third Circuit's footnote (as well as in some earlier decisions[36]) will take hold. At least one commentator believes that would be the correct result.[37] This would mean that, in order to obtain a decryption order, law enforcement would have to demonstrate that the target of the order (presumably the device's user) knows the password – generally, a fairly easy case to make. But compliance with the order is a different issue; a user might decide that a contempt finding is preferable to whatever punishment might be imposed if he reveals the encrypted material. So far, the user in the Third Circuit case has opted to remain in jail rather than unlock his hard drives.[38]

Finally, many devices are now accessible not only via their passcodes but also with the user's fingerprint. And Apple's newest technology eliminates the fingerprint identification in favor of facial recognition technology.[39] As documented in the 2016 Report, biometric data like a fingerprint (and, presumably, a user's face) is generally not considered to be protected

---

[34] *Apple Mac Pro Computer, et. al.*, 851 F.3d at 248.

[35] *Id.*

[36] *See* note 29, *supra.*

[37] Orin Kerr, *Third Circuit Doesn't Resolve Standard for Forced Decryption under the Fifth Amendment*, Wash. Post, Mar. 20, 2017, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/20/third-circuit-doesnt-resolve-standard-for-forced-decryption-under-the-fifth-amendment.

[38] *See* Olivia Solon, *Man Jailed Until He Unlocks Encrypted Hard Drives in Child Abuse Images Case,* The Guardian, Mar. 23, 2017, *available at* https://www.theguardian.com/technology/2017/mar/23/francis-rawls-philadelphia-police-child-abuse-encryption.

[39] With the release of iPhone 8 this year, Apple has introduced 3D facial recognition scanning in place of fingerprint Touch ID. The increased number of data points in a facial recognition scan may enhance security ordinarily, but it is unclear how this may affect the legal approach to ordering unlock using biometric features. This mechanism would foreclose workaround options employed by some law enforcement officials, for example, making a 3D print of a fingerprint to unlock a victim's phone. It is unclear whether courts may issue orders to unlock a device using biometric identifiers in this context or prohibit an enforcement official from holding the phone in front of the user's face without consent in order to unlock.

by the Fifth Amendment.[40] At least one court has held that a user can be ordered to unlock his device via the fingerprint sensor,[41] and in some instances, law enforcement, including this office, has sought and obtained search warrants that include provisions ordering occupants of the target premises to use their fingerprints to unlock any Touch ID-enabled devices.[42] However, even if this became standard practice for law enforcement, its utility would be limited, as iPhones require the entry of the passcode after 48 hours of inactivity, or when the phone restarts.[43] Apple's newest technology also undermines law enforcement's ability to use fingerprints to unlock a Touch ID-enabled device.[44]

More importantly, there is reason to believe courts may view these blanket orders with skepticism. A federal magistrate judge in Illinois recently denied a search warrant provision ordering occupants of a premises to unlock devices with their fingerprints, finding the government had not established probable cause to detain every person on the scene for the purpose of obtaining their fingerprints.[45] While there was no "protectable Fourth Amendment interest" in the fingerprints themselves, the detention of all occupants for the purpose of getting their fingerprints was deemed a violation.[46] The court also found a Fifth Amendment issue, for the same reasons – without knowledge of who the occupants might be, or what

---

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

[41] *Commonwealth v. Baust*, 89 Va. Cir. 267, 271.

[42] *In the Matter of the Search of iPhone Seized from 3254 Altura Avenue in Glendale, California*, Case 2:16-mj-00398 DUTY (C.D. Cal., Feb. 25, 2016). *See also* Kaveh Wadell, *Police Can Force You to Use Your Fingerprint to Unlock Your Phone*, The Atlantic, May 3, 2016, http://www.theatlantic.com/technology/archive/2016/05/iphone-fingerprint-search-warrant/480861; Thomas Fox-Brewster, *Feds Walk Into a Building, Demand Everyone's Fingerprints to Open Phones*, Forbes, Oct. 16, 2016, *available at* http://www.forbes.com/sites/thomasbrewster/2016/10/16/doj-demands-mass-fingerprint-seizure-to-open-iphones/#5e0cd74d8d9d.

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

[44] Since Apple released iOS 11 on September 19, 2017, even when a device is unlocked with a fingerprint, it will require a passcode once an external device is connected. This means that law enforcement can look at the contents of a phone that has been unlocked using Touch ID, but cannot perform a forensic acquisition of the data contained on the device using an external tool. In other words, law enforcement cannot create an image of the device, which is considered to be the best practice in cellphone forensic analysis. This prevents access to potentially critical evidence on the device, such as recently-deleted SMS, MMS, and iMessages and deleted internet history, which are not visible during a manual exampination of the phone. Additionally, with iOS 11, Apple created a "kill switch" that an iPhone owner can use to temporarily disable Touch ID by pressing and holding the side button and one of the volume button or by touching the power button five times in rapid succession. *See* Apple, "Use Emergency SOS on your Phone," *available at* https://support.apple.com/en-us/HT208076. *See also* Tom Warren, *iOS 11 Has a "Cop Button" to Temporarily Disable Touch ID*, The Verge, Aug. 17, 2017, *available at* https://www.theverge.com/2017/8/17/16161758/ios-11-touch-id-disable-emergency-services-lock. This means that a user who is approached by law enforcement can quickly and surreptitiously disable that feature. These innovations in iOS 11 have the potential to limit severely Touch ID access by law enforcement.

[45] *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017).

[46] *Id.*

devices they might possess, the government could not satisfy the "foregone conclusion" test.[47] That decision was later overruled by a District Court judge who found no Fifth Amendment problem.[48] That judge noted that the court was not weighing in on whether this investigative tactic should be regulated, because "the legislature is better positioned to balance the interests of law enforcement and privacy interests."[49]

Although the law remains unsettled, fingerprint unlock orders are unlikely to become standard in search warrant applications. Establishing probable cause, and the requisite foregone conclusion showing, requires "individualized," "fact-intensive" inquiries.[50] In some scenarios, facts may be available about specific occupants and devices prior to the execution of a search warrant. But in many cases, law enforcement will only learn of the basis for a fingerprint decryption order after the search has been conducted. Because of the time-sensitive nature of the Touch ID technology, that will almost certainly be too late.

In short, nothing in recent court decisions suggests that this encryption problem can be solved through litigation. Courts across jurisdictions, at state and federal levels, will invariably adopt different approaches. Even if courts were to agree on a single approach that enables law enforcement to access data on a seized device through a judicially-approved search warrant, technology companies could simply manufacture their devices to circumvent that type of access. A legislative solution is the only way to ensure a proper balance of safety and security interests, that is, to encourage innovation by device manufacturers which ensuring access to critical evidence by law enforcement.

IV. Other Countries are Making Efforts to Strike the Balance Between Privacy and Public Safety

While there has been a standstill in legislative efforts in the United States, foreign nations are continuing to seek legislative solutions to the encryption issue. Unfortunately, these efforts will likely have little practical effect in investigations and prosecutions in the United States.

European Union

European nations have recently recognized "the unacceptability of the status quo, in terms of encryption, which makes the police and judicial authorities powerless."[51] The European Commission has suggested several measures to address the problem. First, it has

---

[47] *Id.* at 11-18.

[48] *In the Matter of the Search Warrant Application for [REDACTED]*, Case No. 17 M 85, (N.D.Ill. Sept. 18, 2017). *See also* Michael Tarm, *Case Reveals Legal Rules of Thumb Tricky with iPhone Sensors*, Associated Press, Oct. 17, 2017, *available at* https://www.seattletimes.com/nation-world/case-reveals-legal-rules-of-thumb-tricky-with-iphone-sensors.

[49] *Id.*

[50] *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. 2017).

[51] *Compte-rendu, Reunion sur L'impact du Chiffrement dans les Investigations Criminelles*, Sept. 18, 2017.

proposed additional resources for Europol, with the aim of developing decryption capability.[52] Second, the Commission proposes a network of subject-matter experts at the European level, to facilitate collaboration among member-states. Third, member states are encouraged to develop "a toolbox of alternative investigation techniques" to access encrypted evidence. Fourth, the Commission recommends "a better and more structured collaboration between authorities, service providers and other industry partners" to understand better the challenges that exist in all sectors. Fifth, resources will be devoted to training programs aimed at enabling investigators to obtain and secure electronic evidence. And, finally, the Commission will continue to assess and evaluate the role of encryption in legal criminal investigations from a legal and technical perspective, and will support other efforts to that end.[53] The Commission is also attempting to facilitate access to electronic evidence across member state lines.[54] A European Commission working group on the topic of encryption has specifically suggested compelling providers to technically assist law enforcement in accessing data.[55]

The E.U. is also mindful of privacy concerns. In July 2017, a European Parliament committee proposed an amendment to pending legislation ("ePrivacy directive") that would prevent member states from trying to decrypt encrypted communications, and compel all tech companies to use end-to-end encryption.[56]

France and Germany

French authorities report that France and Germany have recently put forward a joint proposal for technical and legal solutions to the problems posed by encryption. The proposal is, in part, a response to the ePrivacy directive described above. It notes the importance of strengthening "the capabilities of our law enforcement authorities, which respecting the legitimacy of encrypted communications."[57] The technical measures contemplated include (i) developing practical guidelines for law enforcement to follow; (ii) creating a framework for technical collaboration with private partners; (iii) cooperating with app developers to allow law enforcement to execute, e.g., lawful wiretap orders; (iv) ensuring the security of any tools developed to aid law enforcement; (v) providing enhanced access to VoIP calls for law enforcement; and (vi) developing and implementing abstractions for law enforcement's use of digital forensics tools.[58]

On the legislative side, the countries propose (i) standardizing the regulatory requirements that affect electronic evidence among member states (retention times, file formats, etc.); (ii) requiring that electronic communications providers designate a

---

[52] *Communication from the Commission to the European Parliament, the European Council, and the Council*, *Elevent Progress Report Towards an Effective and Genuine Security Union,* Oct. 18, 2017.
[53] *Id.*
[54] *Id.*
[55] *Compte-rendu, Reunion sur L'impact du Chiffrement dans les Investigations Criminelles*, Sept. 18, 2017.
[56] The proposal must be approved by Parliament and then reviewed by the EU Council.
[57] Memorandum from Secrétariat général des affaires européennes to la Représentation permanente de la France auprès de l'Union européenne (Sept. 5, 2017) (on file with author).
[58] *Id.* at 3-4.

representative for each Member State to respond to law enforcement requests, including search warrants; (iii) proposing a European code for electronic communications that would cover services like Skype and WhatsApp; (iv) drafting "umbrella legislation" that would harmonize the legal framework for dealing with different types of apps and services; (v) creating a framework for cooperation between the E.U. and U.S. as an alternative to the lengthy MLAT process; (v) finding a way to secure law enforcement access to metadata without undermining privacy rights; (vi) adopting a clear obligation for providers to provide law enforcement with necessary technical assistance; (vii) creating a legal framework for the interception of 4G and 5G communications; and (viii) creating an enforcement framework, including sanctions and restrictive measures.

Australia

The Australian government has recently introduced legislation to address the encryption issue, which the Attorney General described as "potentially the greatest degradation of intelligence and law enforcement capability that we have seen in our lifetimes."[59] The legislation is based on the United Kingdom's Investigatory Powers Bill, and would require device manufacturers to provide "appropriate assistance" to law enforcement, "where it is necessary to interdict or in the case of a crime that may have been committed, it is necessary to investigate and prosecute serious crime, whether it be counter terrorism, whether it be serious organised crime, whether it be for example, the operation of pedophile networks."[60]

Australia's Attorney General has emphasized that the legislation does not alter the nation's legal principles, but merely moves them into the modern era: "It has always been accepted that in appropriate circumstances there is a compellable obligation on citizens, including corporate citizens, to cooperate with law enforcement authorities in order to resolve or prevent crime."[61]

In Queensland, the parliament also recently passed the "Counter-Terrorism and Other Legislation Amendment," which gives law enforcement the legal authority to hack into devices related to terror attacks, including the implanting of remote software. The text of the bill includes an amendment that will require "a person to provide access codes, passwords, or encryption keys" when "a person's life or safety is seriously endangered."[62]

---

[59] Australia, Office of the Prime Minister, Press Conference with the Attorney-General, Senator the Hon. George Brandis QC and the Acting Commissioner of the Australian Federal Police, Mr. Michael Phelan APM, July 14, 2017, *available at* https://www.pm.gov.au/media/2017-07-14/press-conference-attorney-general-senator-hon-george-brandis-qc-and-acting.

[60] *Id.*

[61] *Id.*

[62] Counter-Terrorism and Other Legislation Amendment Bill 2017 (Cth.), July 20, 2017, *available at* https://www.legislation.qld.gov.au/browse/bills.

United Kingdom

In the U.K., the Investigatory Powers Bill, discussed in the 2016 Report, recently passed the House of Commons and is being debated by the House of Lords. The law clarifies and codifies existing powers, such as interception of targeted data and communications, and hacking, and authorizes bulk collection of metadata.[63] With respect to encryption, the bill requires communications service providers (CSPs) in the UK to have the ability to remove encryption applied by the CSP, provided it is technically feasible and not unduly expensive. There is an appeals process for orders to break encryption, wherein CSPs can assert that compliance would be prohibitively expensive or otherwise damaging. The law does not require the installation of "backdoors," it merely requires CSPs maintain the ability (already mandated in the UK) to remove encryption. It does not apply to CSPs in other countries. Apple opposes the bill.[64]

V. Federal Legislation Remains the Only Effective Option

Default device encryption remains a significant public safety concern – it hamstrings law enforcement agencies in their efforts to investigate, solve, and prosecute crime. Recent developments in encryption workarounds have provided some measure of relief, but pitting law enforcement and the technology sector in an endless cat-and-mouse game is ill-advised, costly, and untenable. It also offers no remedy to the huge majority of law enforcement agencies that cannot afford to pursue "lawful hacking" solutions.

It is true that, as some commentators point out, if smartphone providers were required by law to comply with decryption orders issued by state and federal courts, some more sophisticated criminals might migrate to foreign providers, or employ additional encryption technology not subject to such regulations. But the fact is that criminals, like all users, prefer software and devices that are reliable and user-friendly, and most of them will continue to use iPhones and Androids for that reason. Indeed, for this same reason, search warrants executed on United States-based email accounts often yield critical evidence, even though criminals could choose to use foreign email providers who are not subject to U.S. legal process.

As discussed in the 2015 Report, prior to October 2014, U.S. smartphone providers routinely complied with court-issued "unlock orders," with no discernable cost to information security.[65] And technology companies continue to maintain the ability to access certain

---

[63] *See* United Kingdon Parliament*,* Investigatory Powers Act of 2016, https://services.parliament.uk/bills/2015-16/investigatorypowers.html.

[64] In a series of interviews following the circulation of the draft bill, CEO Cook noted that any requirement to provide technical assistance to the U.K. government would have "very dire consequences." *See* Ben Quinn, *UK Surveillance Bill Could Bring 'Very Dire Consequences,' Warns Apple Chief*, The Guardian, Nov. 9, 2015, *available at* https://www.theguardian.com/world/2015/nov/10/surveillance-bill-dire-consequences-apple-tim-cook.

[65] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, November 18, 2015, *supra* note 1. In March, 2016, in written testimony before the House Judiciary Committee, Apple's then-General Counsel Bruce Sewell stated that "The process Apple used to extract data from locked iPhones running iOS 7 or earlier operating systems was not, to our knowledge, compromised." *The Encryption Tightrope: Balancing*

encrypted data for their own business reasons.[66] The legislative solution previously proposed in our 2015 and 2016 Reports[67] would simply require that similar capabilities exist when the data is sought by a judge, investigator, or grand jury, after the requisite showing of probable cause.

In the past year, conversations about such legislation have stalled. But this issue has not gone away, and is not going away any time soon. Workarounds like lawful hacking are not a meaningful solution. We should insist that Apple, Google, and other smartphone providers play by the rules, rather than writing them.

---

americans' Security and Privacy Before the H. Comm. on the Judiciary, th Cong. (2016) (statement of Bruce Sewell, General Counsel for Apple, Inc.).

[66] *See* Section II, *supra*; Daniel Richman, *Getting Encryption onto the Front Burner*, Lawfare, Oct. 26, 2017, *available at* https://www.lawfareblog.com/getting-encryption-front-burner.

[67] *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An update to the November 2015 Report*, *supra* note 3, at Part V, Point VI.