NOTE

Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and Its Chilling Effect on Law Enforcement

*Kristen M. Jacobsen**

ABSTRACT

The encrypted smartphone presents a novel legal issue that is hard to crack. Smartphone data is essential to investigating and prosecuting a range of crimes, such as murder, human trafficking, child pornography, and terrorism. However, Apple and Google's recently reengineered mobile operating systems threaten to lock out law enforcement completely. These operating systems use full-disk encryption technology, which converts everything on a hard drive into an unreadable format until the passcode is entered. Additionally, other security features on the smartphone could result in the data being completely destroyed if the passcode is incorrectly entered a certain number of times. Locked smartphones are thus quickly becoming expensive paperweights filing the evidence rooms of state and federal law enforcement.

This Note provides relevant background information on Apple and Google's use of full-disk encryption technology on their respective mobile operating systems. Based on the necessity of smartphone data in the twenty-first century, this Note explains that the inaccessibility of such crucial data will likely frustrate investigations and prosecutions because law enforcement cannot access it elsewhere. This Note concludes that to prevent "Going Dark,"

* J.D., expected May 2017, The George Washington University Law School; B.A., English, 2014, University of Denver. I would like to thank my parents, Jim Jacobsen and Denise Martin, for their unending support and the staff of *The George Washington Law Review* for their thoughtful comments throughout this process.

Congress must immediately enact an amendment to the Communications Assistance for Law Enforcement Act that subjects the manufacturer and mobile operating system provider to a civil penalty for each instance that law enforcement cannot decrypt a smartphone it has the legal authority to search.

Table of Contents

INTRODUCTION

On December 2, 2015, Syed Farook and Tashfeen Malik murdered fourteen people and wounded twenty-one others in San Bernardino, California, during a mass shooting and attempted bombing at a holiday party.[1] This was the first Al Qaeda- or Islamic State of Iraq and Syria ("ISIS")-inspired attack on U.S. soil where a skilled shooter team used both guns and explosives.[2] Investigators found Farook's locked iPhone 5c[3] and obtained legal authority to search its data.[4] However, the iPhone's hard drive was full-disk encrypted.[5] Law enforcement investigators did not have the technological capability to safely access the iPhone's data without the passcode,[6] and both

1 Michael S. Schmidt & Richard Pérez-Peña, *F.B.I. Treating San Bernardino Attack as Terrorism Case*, N.Y. TIMES (Dec. 4, 2015), http://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

2 Tim Lister et al., *ISIS Goes Global: 143 Attacks in 29 Countries Have Killed 2,043*, CNN (Jan. 16, 2017, 3:02 PM), http://www.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/.

3 Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html. The iPhone was running Apple's iOS 9 operating system. *Id.*

4 Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html. The FBI believed that the iPhone contained information regarding communications with ISIS extremists overseas. *See* Cecilia Kang & Eric Lichtblau, *F.B.I. Error Locked San Bernardino Attacker's iPhone*, N.Y. TIMES (Mar. 1, 2016), http://www.nytimes.com/2016/03/02/technology/apple-and-fbi-face-off-before-house-judiciary-committee.html.

5 Full-disk encryption technology prevents anyone from being able to unlock a device without the end user's unique, personal passcode. U.S. DEP'T OF COMMERCE, GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY § 3.1.1 (2007). Since September 2014, both Apple and Google's respective mobile operating systems include full-disk encryption technology by default. *See, e.g.*, Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

6 The iPhone's contents would be permanently deleted after ten failed attempts at input-

gunmen had died in a shootout with police following the attack.[7] The U.S. Department of Justice ("DOJ") thus turned to Apple. Apple publicly refused to help the government unlock the iPhone,[8] which incited a legal standoff between the DOJ and "the world's most valuable public company."[9] This led to "heated rhetoric from both sides in dueling court filings" and "spurred debates—[with the issue] finding its way onto late night talk shows, and dividing the public."[10] Ultimately, the government ended its legal effort to compel Apple's assistance when an anonymous hacker[11] was able to unlock the iPhone.[12] But immediately following the government's success, Apple released a statement saying that the company "will continue to increase the security of [its] products"[13] and will pursue legal measures to force the government to disclose the exploited security vulnerability so that it may reverse-engineer the problem.[14] Indeed, since the case was filed, Apple has begun developing new security measures that are designed

---

ting the passcode. Eric Lichtblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, N.Y. TIMES (Feb. 16, 2016), http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html.

7 Schmidt & Pérez-Peña, *supra* note 1.

8 Tim Cook, CEO of Apple, wrote a letter to the company's customers:

> The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand. . . . [T]he U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. . . . We feel we must speak up in the face of what we see as an overreach by the U.S government.

Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/38X4-WNDG]; *see also* Katie Benner & Nicole Perlroth, *How Tim Cook, in iPhone Battle, Became a Bulwark for Digital Privacy*, N.Y. TIMES (Feb. 18, 2016), http://www.nytimes.com/2016/02/19/technology/how-tim-cook-became-a-bulwark-for-digital-privacy.html.

9 Benner & Lichtblau, *supra* note 3.

10 *Id.*

11 At the time of this Note's publication, the identity of the hacker is still unknown. *See id.*

12 *See* Government's Status Report, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (SP) (C.D. Cal. Mar. 28, 2016); Benner & Lichtblau, *supra* note 3.

13 Alina Selyukh, *The FBI Has Successfully Unlocked The iPhone Without Apple's Help*, NPR (Mar. 28, 2016, 6:20 PM), http://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help (quoting Apple's statement).

14 *See id.*; Chris Strohm et al., *Thank You for Hacking iPhone, Now Tell Apple How You Did It*, BLOOMBERG TECH. (Mar. 22, 2016, 9:04 PM), http://www.bloomberg.com/news/articles/2016-03-23/thank-you-for-hacking-iphone-now-tell-apple-how-you-did-it; *see also* Complaint at 1–4, Associated Press v. FBI, No. 16-cv-1850 (D.D.C. Sept. 16, 2016) (multiple news organizations sue the FBI under the Freedom of Information Act for disclosure of the hacker's identity and the "so-called iPhone access tool").

to prevent the government from unlocking an iPhone using similar methods.[15]

The effects of full-disk encryption extend beyond the San Bernardino iPhone. Crimes across 3000 local jurisdictions are often impossible to crack when law enforcement cannot access crucial smartphone data.[16] For example, in April 2015, eight-months pregnant Brittney Mills was shot to death on her doorstep by a man investigators believed she knew—and whose identity they suspect is currently locked in her iPhone 5.[17] In June of the same year, Ray C. Owens, a father of six, was found shot to death and robbed with two locked phones next to his body: an iPhone 6 and a Samsung Galaxy 6S Edge running Android.[18] And in July, Sharon Vugusta found her brother, U.S. Marine George Mitego, with a fatal gunshot wound to his head.[19] The coroner ruled Mr. Mitego's death a suicide, but his family believes that evidence of a murder may be trapped in his locked iPhone.[20] Currently, it appears that the Federal Bureau of Investigation ("FBI"), the government agency in possession of the decryption technology provided by the anonymous hacker, will not help unlock smartphones in the majority of local cases frustrated by full-disk encryption.[21] Any informa-

---

15 Matt Apuzzo & Katie Benner, *Apple Is Said to Be Trying to Make It Harder to Hack iPhones*, N.Y. TIMES (Feb. 24, 2016), http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html?_r=0; *see also* Katie Benner et al., *Apple's New Challenge: Learning How the U.S. Cracked Its iPhone*, N.Y. TIMES (Mar. 29, 2016), http://www.nytimes.com/2016/03/30/technology/apples-new-challenge-learning-how-the-us-cracked-its-iphone.html.

16 *See* Michael Learmonth, *FBI Keeps iPhone Hack Secret As Hundreds Of Locked Apple Devices Sit In Local Evidence Rooms*, INT'L BUS. TIMES (Mar. 30, 2016, 1:01 PM), http://www.ibtimes.com/fbi-keeps-iphone-hack-secret-hundreds-locked-apple-devices-sit-local-evidence-rooms-2345548. For a chart detailing the types of data that can only be accessed through the physical smartphone, see *infra* Appendix.

17 *See* Renita D. Young, *Brittney Mills' Locked iPhone Hampers Search for Her Killer*, TIMES PICAYUNE (Aug. 3, 2015, 12:30 PM), http://www.nola.com/crime/baton-rouge/index.ssf/2015/07/brittney_mills_locked_iphone.html; Letter from Hillar C. Moore, III, Dist. Attorney, 19th Judicial Dist. E. Baton Rouge Par., to U.S. Senate Comm. on the Judiciary (July 2015).

18 *See* Cyrus R. Vance Jr. et al., Opinion, *When Phone Encryption Blocks Justice*, N.Y. TIMES (Aug. 11, 2015), http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

19 *See* Andy Pierrotti, *Going Dark: How iPhone Encryption Hurts Law Enforcement*, KVUE (Sept. 25, 2015, 7:15 AM), http://www.kvue.com/story/news/investigations/defenders/2015/09/24/going-dark-how-iphone-encryption-hurts-law-enforcement/72743852/.

20 *See id.*

21 *See* Learmonth, *supra* note 16. *But see* Doreen McCallister, *FBI To Help Arkansas Prosecutor Unlock iPhone Linked To Murder Case*, NPR (Mar. 31, 2016, 5:40 AM), http://www.npr.org/sections/thetwo-way/2016/03/31/472497468/fbi-to-help-arkansas-prosecutor-unlock-iphone-linked-to-murder-case.

tion shared increases the likelihood that Apple will isolate and close any vulnerability on future mobile operating systems.[22]

Unfortunately for law enforcement, defendants are dialed in to the possibilities this new encryption technology presents. The ISIS terrorist group—which claimed responsibility for the November 2015 attacks in Paris and the March 2016 attack in Brussels—instructs its followers on how to use encryption technology to evade law enforcement.[23] But the problem extends beyond international terrorist organizations. A Manhattan felon on a recorded jailhouse call said: "Apple and Google came out with these softwares that can no longer be encrypted [sic: *de*crypted] by the police. . . . If our phones is [sic] running on the iO[S]8 software, they can't open my phone. That might be another gift from God."[24] John J. Escalante, former Chief of Detectives for Chicago's police department, predicts that "Apple will become the phone of choice for the pedophile."[25]

Despite calls for federal legislation,[26] the Obama administration ultimately declined to seek a legislative solution.[27] The Trump administration has not yet stated whether it will champion legislation that bans or limits encryption on smartphones; however, Trump's cam-

---

22 *See* Learmonth, *supra* note 16.

23 *See, e.g.*, Rukmini Callimachi, *How ISIS Built the Machinery of Terror Under Europe's Gaze*, N.Y. TIMES (Mar. 29, 2016), http://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html; Pamela Engel, *A Pro-ISIS Account Is Giving Its Belgian Followers Specific Instructions on How to Evade Authorities*, BUS. INSIDER (Mar. 22, 2016, 4:29 PM), http://www.businessinsider.com/isis-belgian-supporters-encryption-2016-3.

24 *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 17 (2015) [hereinafter *Encryption and Technology Issues Hearing*] (statement of Cyrus R. Vance, Jr., District Attorney, New York County District Attorney's Office).

25 *See* Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, WASH. POST (Sept. 25, 2014), https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html. "Many perpetrators, particularly those who commit sexual offenses, take photos and videos of their acts, and store them on . . . smartphones." *Encryption and Technology Issues Hearing*, *supra* note 24, at 2.

26 *See, e.g.*, *Encryption and Technology Issues Hearing*, supra note 24; *Addressing Remaining Gaps in Federal, State, and Local Information Sharing: Hearing Before the Subcomm. on Counterterrorism & Intelligence of the H. Comm. on Homeland Sec.*, 114th Cong. 14 (2015) [hereinafter *Addressing Remaining Gaps in Federal, State, and Local Information Sharing Hearing*] (statement of Chief Richard Beary, President, International Association of Chiefs of Police); Congressman Peter T. King, *Remembering the Lessons of 9/11: Preserving Tools and Authorities in the Fight Against Terrorism*, 41 J. LEGIS. 173, 183 (2014–2015); Letter from Hillar C. Moore, III, *supra* note 17.

27 *Sen. Ron Johnson Holds a Hearing on Threats to the Homeland: Hearing Before S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2015) [hereinafter *Hearing on Threats to the Homeland*] (statement of James B. Comey, Director, Federal Bureau of Investigation); *see also* Apuzzo & Benner, *supra* note 15.

paign talk indicates that his administration is inclined to do so.[28] In February 2016, at a rally in South Carolina, and later that same day on Twitter, then-Republican presidential candidate Trump urged a boycott of all Apple products because of the company's refusal to help the FBI unlock the San Bernardino iPhone.[29] But assuming Trump follows the action plan of his predecessor, the Trump administration will attempt to achieve a solution via negotiation and forgo any legislative action.[30] Yet it is highly doubtful that tech companies will cooperate.[31] Technology companies—the most vocal of which is Apple—have publicly stated that they will not make their smartphones amenable to search warrants.[32]

Recent legislative proposals further threaten law enforcement's ability to access critical smartphone data. There are currently three pending bills in the U.S. Congress that would each forbid federal government agencies from mandating or requesting an access point into commercial products.[33] On February 11, 2016, a bipartisan group of legislators in Congress introduced the Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016 ("ENCRYPT Act").[34] The Act would prevent states and localities from passing laws banning encryption on smartphones sold in the United States.[35]

---

28 Kif Leswing, *'Boycott Apple'—3 Ways a Trump Presidency Could Affect Apple*, BUS. INSIDER (Nov. 9, 2016, 10:31 AM), http://www.businessinsider.com/how-trump-presidency-will-affect-apple-2016-11.

29 *Id.*; *see also* Pamela Engel, *TRUMP: 'Boycott All Apple Products,'* BUS. INSIDER (Feb. 19, 2016, 3:37 PM), http://www.businessinsider.com/donald-trump-boycott-apple-2016-2.

30 *See Hearing on Threats to the Homeland*, *supra* note 27; Apuzzo & Benner, *supra* note 15.

31 *See* Ellen Nakashima & Andrea Peterson, *Obama Administration Opts Not to Force Firms to Decrypt Data—For Now*, WASH. POST (Oct. 8, 2015), https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data—for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

32 According to Apple's website, "Apple has never worked with any government agency from any country to create a 'backdoor' in any of our products or services. . . . And we never will." Privacy, *Government Information Requests*, APPLE, http://www.apple.com/privacy/government-information-requests/ [https://perma.cc/KRV2-EAHX] (last visited Feb. 6, 2017); *see also supra* note 8.

33 *See* Secure Data Act of 2015, S. 135, 114th Cong. (2015); End Warrantless Surveillance of Americans Act, H.R. 2233, 114th Cong. (2015); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015).

34 Ensuring National Constitutional Rights for Your Private Telecommunications (ENCRYPT) Act of 2016, H.R. 4528, 114th Cong. (2016).

35 *See id.*

This Note calls for Congress to immediately amend the Communications Assistance for Law Enforcement Act ("CALEA")[36] in order to account for the serious law enforcement threat that full-disk encryption poses.[37] Part I begins by providing relevant information on Apple and Google's full-disk encryption technology on their respective mobile operating systems. After establishing the technological basics, Part II explains the importance of smartphone data in twenty-first century investigations and prosecutions. Part II also discusses how full-disk encryption threatens law enforcement by making smartphone data inaccessible. After explaining why current proposals fail in Part III, Part IV introduces the CALEA and discusses its current inapplicability to smartphones. Part V calls for an amendment to the CALEA that makes the Act applicable to smartphones and imposes a civil penalty on both the manufacturer and mobile operating system provider for each instance law enforcement cannot decrypt a smartphone that it has the legal authority to search. Finally, Part VI defends the proposed amendment against potential counterarguments.

I. Full-Disk Encryption Technology on Apple and Google's Mobile Operating Systems

Full-disk encryption automatically converts "everything on a hard drive, including the operating system, into an unreadable form until the proper key (i.e., passcode) is entered."[38] In September 2014, Apple and Google announced that they had reengineered their mobile

---

36 Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001–1010 (2012).

37 This Note is limited to "full-disk" encryption. As such, the problem of "end-to-end" encryption is beyond the scope of this Note. This Note also does not address whether the First Amendment prohibits the government from requiring private companies to make smartphones amendable to search warrants. *Compare* Neil Richards, *Apple's "Code = Speech" Mistake*, MIT Tech. Rev. (Mar. 1, 2016) https://www.technologyreview.com/s/600916/apples-code-speech-mistake/ (requiring companies to make smartphones amenable to governmental search warrants does not violate the First Amendment), *with* Hayley Tsukayama, *We Asked a First Amendment Lawyer if Apple's 'Code Is Speech' Argument Holds Water. Here's What He Said.*, Wash. Post (Feb. 26, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/02/26/we-asked-a-first-amendment-lawyer-if-apples-code-is-speech-argument-holds-water-heres-what-he-said/ (arguing that a government request to build software that circumvents smartphone's security features "would essentially force Apple to say, in code, something" and thus violate the First Amendment).

38 Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals when Third Parties Are Forced to Hand Over Passwords*, 30 Berkeley Tech. L.J. 1, 8 (2015).

operating systems[39] to include full-disk encryption technology by default.[40] Apple and Google also deliberately removed "backdoor"[41] access to passcodes, making it no longer feasible for the companies to comply with government warrants requesting data on locked smartphones.[42] Consequently, up to ninety-nine percent of all smartphones worldwide are rendered inaccessible to authorized government searches.[43] Due to the nuances inherent in the different systems, this Section begins by looking at the two most popular mobile operating system providers separately.

A. Apple

Apple manufactures smartphones, named iPhones, which run an operating system named iOS.[44] Numerical names designate different versions of the operating system (e.g., iOS 8).[45] Apple adopted full-disk encryption by default in September 2014 with iOS 8.[46] For all iPhones running iOS 8 and higher, Apple states that the company

---

39 A mobile operating system "manages the hardware and software components of smartphones." FRANCIS M. ALLEGRA & DANIEL B. GARRIE, PLUGGED IN: GUIDEBOOK TO SOFTWARE AND THE LAW § 5:3 (2015).

40 *See* Devlin Barrett & Danny Yadron, *New Level of Smartphone Encryption Alarms Law Enforcement*, WALL ST. J. (Sept. 22, 2014, 7:42 PM), http://www.wsj.com/articles/new-level-of-smartphone-encryption-alarms-law-enforcement-1411420341.

41 A "backdoor" is the term describing a mechanism or access point in a communications device or network that allows "the creator of software or hardware [to] access [the] data without the permission or knowledge of the user." Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 460 (2012).

42 According to Apple's website:

> On devices running iOS 8 and later versions, your personal data is placed under the protection of your passcode. For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

Privacy, *Government Information Requests*, APPLE, http://www.apple.com/privacy/government-information-requests/ [https://perma.cc/TU8X-T8BW] (last visited Feb. 6, 2017).

Niki Christoff, a Google spokeswoman, stated:

> For over three years Android has offered encryption, and keys are not stored off of the device, so they cannot be shared with law enforcement . . . . As part of our next Android release [Android Lollipop OS], encryption will be enabled by default out of the box, so you won't even have to think about turning it on.

Timberg, *supra* note 5.

43 This information is correct as of Q3 2016. *Smartphone OS Market Share*, 2016 Q3, INT'L DATA CORP., http://www.idc.com/prodserv/smartphone-os-market-share.jsp [https://perma.cc/F8QN-NF9S] (last visited Feb. 6, 2017).

44 *See iPhone*, APPLE, http://www.apple.com/iphone/ (last visited Feb. 6, 2017); *iOS 10*, APPLE, http://www.apple.com/ios/ios-10/ (last visited Feb. 6, 2017).

45 *iOS 10*, *supra* note 44.

46 *See* Barrett & Yadron, *supra* note 40.

"will not perform iOS data extractions [in response to government search warrants] as data extraction tools are no longer effective."[47] The majority of iPhones in circulation now function on software with full-disk encryption. As of January 4, 2017, approximately ninety-four percent of all iOS devices currently in use run iOS 9 and higher.[48]

B. Google

Google's mobile operating system is named Android.[49] Android operating systems are named after a dessert or candy (e.g., Éclair) and have a unique numerical identifier (e.g., 2.1).[50] Unlike iPhones, several manufacturers (called original equipment manufacturers ("OEMs")) produce Android-powered smartphones.[51]

Android users have had the ability to activate full-disk encryption on certain smartphones since the release of Honeycomb 3.0 in January 2011.[52] Shortly after Apple announced iOS 8 in 2014, Google said that it would make full-disk encryption mandatory for new Android-powered smartphones running Lollipop 5.0.[53] However, two months later, Google changed its position from requiring to "very strongly recommend[ing]" OEMs make full-disk encryption a default feature.[54] Despite this, the Google-manufactured Nexus smartphones running Lollipop 5.0 had full-disk encryption by default in 2014.[55]

---

47 *Legal Process Guidelines: U.S. Law Enforcement*, APPLE (Sept. 29, 2015), http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/RW8N-Z3W3].

48 Support, *Apple Developer*, APPLE, https://developer.apple.com/support/app-store/ (last visited Feb. 6, 2017).

49 J. Gregory Sidak, *Do Free Mobile Apps Harm Consumers?*, 52 SAN DIEGO L. REV. 619, 621 (2015).

50 *See* John D. Sutter, *Why Does Google Name Its Android Products After Desserts?*, CNN (Feb. 4, 2011, 11:07 AM), http://www.cnn.com/2011/TECH/innovation/02/04/google.honeycomb.android.names/.

51 OEMs of Android-powered smartphones include Google, Motorola, Samsung, HTC, LG, Sony, Asus, and Acer. *See* Brad Reed, *Here Are the Android OEMs That Do the Best Job of Getting You the Latest Software*, BGR (May 2, 2014, 4:42 PM), http://bgr.com/2014/05/02/android-software-updates-samsung-htc-motorola/.

52 *See* Jerry Hildenbrand, *How to Enable Encryption in Android*, ANDROID CENTRAL (Feb. 26, 2016, 2:31 PM), http://www.androidcentral.com/how-enable-encryption-andorid [https://perma.cc/J4FU-3JGP].

53 *See* Timberg, *supra* note 5; *A Sweet Lollipop, with a Kevlar Wrapping: New Security Features in Android 5.0*, ANDROID OFFICIAL BLOG (Oct. 28, 2014), https://android.googleblog.com/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html.

54 ANDROID, COMPATIBILITY DEFINITION: ANDROID 5.1 § 9.9 (last updated July 10, 2015), https://static.googleusercontent.com/media/source.android.com/en//compatibility/5.1/android-5.1-cdd.pdf.

55 *See* David Ruddock, *Android 6.0 Will Finally Require Manufacturers To Enable Full-Disk Encryption By Default On New Devices*, ANDROID POLICE (Oct. 19, 2015), http://

Google released Marshmallow 6.0 in October 2015.[56] That month, Google published an updated version of the Android Compatibility Definition Document ("CDD")[57] for Marshmallow 6.0 that requires OEMs to make full-disk encryption a default feature on all new Android-powered phones.[58] The percentage of Android-powered smartphones that have full-disk encryption by default is rapidly increasing. As of February 6, 2017, approximately sixty-five percent of Android-powered devices run Lollipop 5.0 or higher.[59]

II. How Full-Disk Encryption Threatens Law Enforcement

This Part starts by explaining the necessity of smartphone data in twenty-first century investigations and prosecutions, giving real life examples that demonstrate its importance. It then discusses how the inaccessibility of smartphone data inhibits law enforcement efforts, as the data is often available only on the physical phone. Finally, this Part ends by explaining how current legal and technological tools cannot access smartphone data protected by full-disk encryption.

A. Smartphones Frequently Contain Evidence Crucial to Criminal Investigations and Prosecutions

As of October 2015, sixty-eight percent of American adults have a smartphone.[60] The Supreme Court has recognized that the term "'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers" that "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[61] And these multiple func-

www.androidpolice.com/2015/10/19/android-6-0-will-finally-require-manufacturers-to-enable-full-disk-encryption-by-default-on-new-devices/.

56 *See* Sarah Mitroff, *Here Are the Android 6.0 Marshmallow Features that Matter*, CNET (Oct. 5, 2015, 8:00 AM), http://www.cnet.com/products/google-android-6-0-marshmallow/.

57 The CDD sets guidelines for OEMs. *See* Ruddock, *supra* note 55.

58 The new rule of mandatory full-disk encryption exempts smartphones launched with older versions of Android that upgraded to Marshmallow 6.0 later and smartphones that do not meet the minimum crypto-performance requirements. Android, Compatibility Definition: Android 7.1 at 80–81 (last updated Dec. 20, 2016), http://static.googleusercontent.com/media/source.android.com/en//compatibility/android-cdd.pdf.

59 According to Google, approximately 10.1% run Lollipop 5.0, 23.3% run Lollipop 5.1, 29.6% run Marshmallow 6.0, 0.5% run Nougat 7.0, and 0.2% run Nougat 7.1. *Dashboards*, Android, https://developer.android.com/about/dashboards/index.html (last visited Feb. 6, 2017).

60 Monica Anderson, *Technology Device Ownership: 2015*, Pew Res. Ctr. (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

61 Riley v. California, 134 S. Ct. 2473, 2489 (2014); *see, e.g.*, United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) ("A cell phone is similar to a personal computer that is carried on one's person . . . .").

tionalities are widely used.[62] Thus, to law enforcement agencies, smartphones are crucial repositories of potentially dispositive information.[63]

Law enforcement's inability to access smartphone data "means that lives may well be at risk or lost and those guilty parties may remain free."[64] Investigations and prosecutions of a wide range of cases rely on evidence found on smartphones. One such example is the Los Angeles Police Department's recent investigation into the death of a two-year-old girl.[65] Officers were able to ascertain that she died from blunt force trauma; however, they were unable to identify any eyewitnesses to the lethal event.[66] Investigators were ultimately able to charge the girl's parents based on text message exchanges stored on their smartphones.[67] These text messages revealed that the mother was responsible for the young girl's death, the father was aware of the lethal assault and failed to prevent it, and both parents failed to seek appropriate medical attention while the child convulsed in her crib.[68] The timely discovery of highly probative text message evidence convinced both parents to plead guilty.[69]

Additionally, smartphone data has exonerated innocent individuals in a variety of cases. In Kansas, cellphone data—a recovered deleted video—proved the innocence of several teens accused of rape.[70] Similarly, in Manhattan, a detective found several iPhones at the

---

62 *See Mobile Technology Fact Sheet*, PEW RES. CTR. (Dec. 27, 2013), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/9/ [https://web.archive.org/web/20160603030022/http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/9/] (stating that as of May 2013, eighty-one percent of adult cell owners use their phones to send or receive text messages, sixty-three percent use their phones to go online, fifty-two percent use their phones to send or receive email, fifty percent use their phones to download apps, and forty-nine percent use their phones to get directions, recommendations, or other location-based information).

63 *See Encryption and Technology Issues Hearing*, *supra* note 24, at 14–17.

64 *Addressing Remaining Gaps in Federal, State, and Local Information Sharing Hearing*, *supra* note 26, at 15. As of April 2016, the Manhattan District Attorney's Office possesses 175 iPhones that it cannot unlock. Katie Benner & Matt Apuzzo, *Narrow Focus May Aid F.B.I. in Apple Case*, N.Y. TIMES (Feb. 22, 2016), http://www.nytimes.com/2016/02/23/technology/apple-unlock-iphone-san-bernardino.html?_r=0.

65 *See* James B. Comey, Dir., Fed. Bureau of Investigation, Speech at the Brookings Institution, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014) (transcript at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course).

66 *Id.*

67 *Id.*

68 *Id.*

69 *See id.*

70 *Id.*

scene of a homicide.[71] Investigators obtained a search warrant and unlock order and, with Apple's cooperation, extracted critical evidence from the smartphones.[72] The iPhone data showed inaccuracies in the investigators' initial timeline and that a suspect was not involved in the homicide.[73] Investigators linked a phone number in one of the iPhones to another individual, who later confessed and pled guilty.[74]

B. A Significant Amount of Data Is Only Contained on the Physical Smartphone

A number of commentators believe that law enforcement's ability to pursue other, more traditional avenues of investigation diminishes the need for smartphone data contained on the physical device.[75] However, a report conducted by the New York County (Manhattan) District Attorney's Office shows that certain crucial data only exists on the physical smartphone.[76] The table in the Appendix shows that iMessage[77] content and details (e.g., dates, times, phone numbers involved), SMS/MMS[78] content, historical cell site data, historical GPS data, contacts, photos/videos, internet search history, internet bookmarks, and third-party app data can only be accessed on the physical phone.[79] Phone companies can likely only provide SMS/MMS and phone call details.[80]

Many critics argue that smartphone operating system providers and manufacturers do not need to make their devices amenable to

---

71 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 11 (Nov. 2015).

72 *Id.* In the past, mobile operating system providers assisted law enforcement agencies in accessing smartphone data. *See infra* notes 148–49 and accompanying text.

73 *Id.*

74 *Id.*

75 *See, e.g.*, MATTHEW G. OLSEN ET AL., BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. U., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 9–15 (2016).

76 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 6–8.

77 iMessage is a service akin to text messaging; it allows iPhone users to "send messages back and forth with anyone on iPad, iPhone, iPod touch, or a Mac running [the operating system] Mountain Lion or later." Bodyxs, Comment to *imessage*, APPLE (Oct. 17, 2014, 7:53 PM), https://discussions.apple.com/thread/6599367?start=0&tstart=0. iMessages may contain text and attachments such as photos, videos, locations, links, and contacts. *See* SUPPORT, *Learn how to use Messages*, APPLE, https://support.apple.com/explore/messages (last visited Feb. 6, 2017).

78 iPhones and Android-powered smartphones can send Short Messages Service ("SMS") messages and Multimedia Messaging Service ("MMS") messages. SMS messages are "text messages of up to 160 characters in length." MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 24 n.9. MMS messages "include messages with multimedia content, like photos [or video]." *Id.*

79 *See infra* Appendix.

80 *See infra* Appendix.

searches because law enforcement can already lawfully search suspects' cloud accounts.[81] But data stored in the cloud does not necessarily reflect all of the data stored within a smartphone device.[82]

Smartphone users do not have to set up a cloud account or back up their data to it.[83] Accordingly, even "minimally sophisticated wrongdoers" can simply choose not to back up their smartphone data to a cloud storage service and successfully obfuscate crimes facilitated through their phones.[84] Indeed, in the San Bernardino case, Farook had disabled iCloud backups for certain apps and data on his phone,[85] and the last backup was made about six weeks before the attacks.[86] But the problem is not limited to the wrongdoer who uses his smartphone in perpetration of crime. A future victim may hinder investigation of the crime(s) committed against him by not regularly backing up all data to a cloud server.

Beyond hiding information from potential law enforcement access, there is a myriad of reasons why a user may not set up a cloud account or back up all his data to it. Cloud providers only offer a small amount of storage space for free; additional space must be purchased.[87] The cost of extra storage space may deter users from backing

---

81 *See, e.g.*, OLSEN ET AL., *supra* note 75, at 9, 11.

82 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 8.

83 *Id.*

84 *Encryption and Technology Issues Hearing*, *supra* note 24, at 6.

85 Backups for "Mail," "Photos," and "Notes" were all turned off on his iPhone. Supplemental Declaration of Christopher Pluhar in Support of Government's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order at 4, *In re* The Search of an Apple iPhone During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (SP) (C.D. Cal. Mar. 10, 2016) [hereinafter Supplemental Declaration of Christopher Pluhar].

86 *Id.* at 3–4.

87 iPhone users can back up information to iCloud. *iCloud*, APPLE, http://www.apple.com/icloud/ (last visited Feb. 6, 2017). The first five gigabytes ("GB") of storage on an iCloud account are free. *Id.* Users can upgrade their iCloud storage to 50 GB for $0.99 per month, to 200 GB for $2.99 per month, to 1 terabyte ("TB") for $9.99 per month, and to 2 TB for $19.99 per month. *Id.* iPhones come with either 16, 32, 64, 128, or 256 GBs of storage space on the device itself. *Compare iPhone models*, APPLE, http://www.apple.com/iphone/compare/ (last visited Feb. 6, 2017). Google has several locations for cloud storage. iPhones and Android-powered smartphones can both back up data to Google's cloud. Google offers an initial 15 GB of cloud storage space at no cost that is shared across three of its services: Google Drive, Gmail, and Google+ Photos. *Pricing Guide*, GOOGLE DRIVE, https://www.google.com/drive/pricing/ (last visited Feb. 6, 2017). After that, a Google cloud user can upgrade to 100 GB for $1.99 per month, to 1 TB for $9.99 per month, to 10 TB for $99.99 per month, to 20 TB for $199.99 per month, and to 30 TB for $299.99 per month. *Id.* Many Android smartphones have a minimum of 16 GB of storage space, *see Phones*, ANDROID, https://www.android.com/phones/ (last visited Feb. 6, 2017), and one can hold up to 640 GB, *see V SQUARED Specs*, SAYGUS, https://www.saygus.com/v2-2/ (last visited Feb. 6, 2017).

up significant portions of their data. Users can also elect to remove certain types of content from the backup process.[88] Many opt to upload a limited number of specific files for a variety of reasons, including conserving storage space and protecting sensitive information from hacker attacks.[89] Additionally, some cloud accounts require the user to access a Wi-Fi connection before backing up data to the cloud.[90] Cloud accounts thus typically contain little or no data of interest to law enforcement—in fact, the "most common use for cloud storage is music."[91]

Without access to a smartphone's data, law enforcement has "no reasonable way" of determining which mobile cloud service(s) a person uses for storage.[92] Even assuming that access to a cloud account produces the same information obtained from a physical phone, law enforcement still must identify the relevant mobile cloud service provider(s) before they can access data stored on the account. Apple, Google, Dropbox, and Microsoft all offer mobile cloud storage.[93] Because locating the user's mobile cloud server(s) is time-intensive, law enforcement may not be able to locate a user's account(s) before the user or an accomplice permanently deletes all evidence.[94]

Additionally, it is more difficult for a prosecutor to establish ownership of a cloud account. A phone may be discovered on a defendant's person or within an area of his control (e.g., house, car), which raises an inference of ownership and would likely only require the testimony of one witness (e.g., the officer who recovered the device).[95] By contrast, to prove ownership of a cloud account, "[a] prosecutor

---

88 *See* SUPPORT, *iCloud: Change iCloud Feature Settings*, APPLE (Dec. 13, 2016), https://support.apple.com/kb/ph2613?locale=EN_US; *cf.* Drive Help, *Back Up Photos & Videos Automatically in Google Drive: Android*, GOOGLE, https://support.google.com/drive/answer/6093613?hl=en&ref_topic=7000756&co=GENIE&co=GENIE.Platform%3DAndroid&oco=1 (last visited Feb. 6, 2017) (describing how users may enable or disable automatic backup).

89 There have been several recent, highly-publicized hacks of cloud accounts. For example, "Celebgate" involved a man hacking 50 iCloud and 72 Gmail accounts of celebrities and leaking personal information contained therein, including nude photographs. *See* Jon Blistein, *Hacker Pleads Guilty to Stealing Celebrity Nude Photos*, ROLLINGSTONE (Mar. 15, 2016), http://www.rollingstone.com/movies/news/hacker-pleads-guilty-to-stealing-celebrity-nude-photos-20160315.

90 *See iCloud*, *supra* note 87.

91 *Apple's iCloud Is Most-Used Cloud Service in the US, Beating Dropbox & Amazon*, APPLEINSIDER (Mar. 21, 2013, 8:55 AM), http://appleinsider.com/articles/13/03/21/apples-icloud-is-most-used-cloud-service-in-the-us-beating-dropbox-amazon; *see* Supplemental Declaration of Christopher Pluhar, *supra* note 85, at 4.

92 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 8.

93 *Id.*

94 *See Encryption and Technology Issues Hearing*, *supra* note 24, at 7.

95 *Id.*

may need to present testimony or records from [the mobile cloud provider] relating to the subscriber information, IP login history, and/or content of the account, testimony or records from internet service providers regarding the subscriber information of certain IP addresses, and/or testimony of forensic analysts."[96] Mere potential access to a cloud account is thus insufficient.

C. Current Legal and Technological Tools Cannot Crack Full-Disk Encryption

Defendants often do not consent to smartphone searches or choose to disclose their passcodes.[97] Sometimes a passcode cannot be obtained because the user's identity is unknown (e.g., a phone found at a crime scene) or the user is unavailable because he has been abducted or killed (e.g., a phone of a kidnapping or murder victim).[98] Law enforcement thus has to turn to alternative methods of gaining access into the phone, including using brute force and asking the service providers themselves—none of which is particularly helpful.

1. Law Enforcement Likely Cannot Force Defendants to Unlock Their Smartphones

Under the Fifth Amendment, "[n]o person shall be . . . compelled in any criminal case to be a witness against himself."[99] There are three elements an individual must establish in order to invoke this privilege: (1) compulsion; (2) a testimonial communication; and (3) incrimination.[100]

Caselaw indicates that the government violates a defendant's Fifth Amendment right against self-incrimination when it compels the defendant to *tell* his numerical or alphanumerical passcode.[101] Al-

---

96 *Id.*

97 There are a number of reported cases in which suspects refused to surrender their passwords, *see, e.g.*, United States v. Diermyer, No. 3:10-cr-071-HRH-JDR, 2010 WL 4683550, at *2 (D. Alaska Nov. 12, 2010); Griffin-El v. Beard, No. 06-2719, 2009 WL 2929802, at *2 (E.D. Pa. Sept. 8, 2009); United States v. Horton, No. 4:08CR3005, 2009 WL 1872612, at *7 (D. Neb. June 30, 2009), or conveniently "forgot" them, *see* Matt Apuzzo et al., *Apple's Line in the Sand Was Over a Year in the Making*, N.Y. TIMES (Feb. 18, 2016), http://www.nytimes.com/2016/02/19/technology/a-yearlong-road-to-a-standoff-with-the-fbi.html.

98 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 4.

99 U.S. CONST. amend. V. The Fifth Amendment's privilege from compulsory self-incrimination has been "incorporated" by the Fourteenth Amendment so that the privilege applies to state criminal proceedings as well as federal. *See* Griffin v. California, 380 U.S. 609, 615 (1965); Malloy v. Hogan, 378 U.S. 1, 6 (1964).

100 *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1341 (11th Cir. 2012).

101 *See, e.g.*, *id.* at 1346 (compelling an individual's passcode constitutes a violation of his Fifth Amendment self-incrimination privilege); SEC v. Huang, No. 15-269, 2015 WL 5611644, at

though the Supreme Court has not yet ruled on this precise issue, dicta in *Doe v. United States*[102] strongly suggests that the Court would find that requiring a defendant to disclose his passcode would violate the Fifth Amendment right against compulsory self-incrimination.[103] Indeed, lower courts are mostly in agreement that disclosing a passcode is "incriminating" within Supreme Court jurisprudence.[104]

Although the government cannot compel an individual to disclose his passcode, it may be able to require a defendant to unlock his phone using his fingerprint if the smartphone has a biometric fingerprint scanner.[105] At first blush, the solution seems promising. However, because "biometric authentication cannot be set up without first creating a passcode" (thus directly linking authentication to a passcode), commentators contend that a fingerprint scan still constitutes a Fifth Amendment violation.[106] Additionally, not all smartphones have fingerprint authentication technology.[107] Even for smartphones that

---

*2–3 (E.D. Pa. Sept. 23, 2015) (same); United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010) (same); United States v. Rogozin, No. 09-CR-379(S)(M), 2010 WL 4628520, at *6 (W.D.N.Y. Nov. 16, 2010) (same); Virginia v. Baust, No. CR14-1439, 2014 WL 6709960, at *3 (Va. Cir. Ct. 2014) (same).

102 487 U.S. 201 (1988).

103 The Court declared that "be[ing] forced to surrender a key to a strongbox containing incriminating documents" is non-testimonial, while "be[ing] compelled to reveal the combination to [a] wall safe" is. *Id.* at 210 n.9 (quoting *id.* at 219 (Stevens, J., dissenting)). In sum, a defendant cannot be forced to disclose the contents of his mind. *Id.*

104 *See* Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L. HEIGHTENED SCRUTINY 11, 24 (2012) ("Courts generally agree that divulging a password constitutes a testimonial act.").

105 *See Baust*, 2014 WL 6709960, at *3 (holding that a "[d]efendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same," because his "fingerprint, like a key . . . does not require the witness to divulge anything through his mental processes").

106 Erin M. Sales, Note, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, 69 U. MIAMI L. REV. 193, 227 (2014). A defendant forced to unlock his smartphone using his fingerprint was arguably compelled to indirectly disclose knowledge of the passcode because the fingerprint is connected to the passcode:

> Thus, unlike the cases where the Supreme Court has held that compelling the suspect to be the source of physical evidence did not violate the self-incrimination privilege, a court may consider biometric authentication differently. In those cases, the physical evidence was not linked to any knowledge. The blood analysis in *Schmerber*, the blouse modeling in *Holt*, the speech in *Wade*, and the handwriting exemplar in *Gilbert*, all occurred without the defendant creating a passcode committed to his and only his memory.

Id. at 228 (footnotes omitted).

107 On certain iPhones, the user can enable Touch ID, a fingerprint sensing system that requires the user's fingerprint to unlock the device. *See* APPLE INC., IOS SECURITY 7 (Sept. 2014) [hereinafter IOS SECURITY GUIDE]. Some Android devices have fingerprint scanners, which allow the user to unlock the device with their fingerprint. *See* Google Store, *Android 6.0 Marsh-*

have such technology, the user is not required to enable it.[108] In other words, the user could choose to only have a numerical or alphanumerical passcode.[109] Thus, a defendant looking to keep the contents of his smartphone from law enforcement will simply not enable the biometric authentication function.

The "forgone conclusion" exception, which applies if the government learns "little or nothing" from the information conveyed by the defendant's act of production,[110] may allow the government to require the defendant to unlock his smartphone *using* his passcode[111] or to provide its decrypted contents.[112] In either circumstance, only the data on the smartphone, not the passcode itself, would be revealed.[113] It is "difficult" for the government to "clear the 'foregone conclusion' hurdle."[114] The Eleventh Circuit is currently the only federal appeals court to have ruled on the standard the government must meet to satisfy the foregone conclusion exception.[115] In *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*,[116] law enforcement believed the defendant was using a specific Youtube.com account to share sexually explicit material of underage girls.[117] Investigators were able to seize several of the defendant's laptops and external hard drives, however, forensic examiners were unable to access parts of the encrypted drives.[118] A grand jury subpoena required the defendant to produce the "unencrypted contents" of the digital media.[119] A forensic

---

mallow. S'more to Love, GOOGLE, https://store.google.com/magazine/android_6_platform_story (last visited Jan. 18, 2017). However, due to the variety of OEMs making Android devices, not all Android devices can be unlocked using the user's fingerprint. MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 3.

108 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 2–3.

109 *See id.* at 3.

110 Fisher v. United States, 425 U.S. 391, 411 (1976) ("The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.").

111 *See* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614 (Mass. 2014); Orin Kerr, *Apple's Dangerous Game*, WASH. POST: THE VOLOKH CONSPIRACY (Sept. 19, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/.

112 *See, e.g.*, United States v. Fricosu, 841 F. Supp. 2d 1232, 1235, 1238 (D. Colo. 2012) (directing the defendant to provide a decrypted copy of her computer's hard drive where its contents were accessible only by entry of a passcode); *In re* Grand Jury Subpoena to Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1, *4 (D. Vt. Feb. 19, 2009) (same).

113 *See supra* notes 111–112.

114 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 5.

115 *See generally In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335 (11th Cir. 2012).

116 670 F.3d 1335 (11th Cir. 2012).

117 *Id.* at 1339.

118 *Id.*

119 *Id.*

examiner for the government testified that they believed data existed on the encrypted parts of the hard drive because the still-encrypted parts contained nonsensical characters and numbers.[120] The examiner believed that these characters and numbers suggested the presence of an encrypted form of data.[121]

The Eleventh Circuit rejected the government's contention that the existence of evidence on the hard drive was a foregone conclusion.[122] The court noted that while the government showed that "the drives *could* contain files," the government did not meet its burden to show that "the drives *actually* contain any files."[123] It does not appear that the requisite probable cause standard for a search warrant would satisfy the foregone conclusion exception. The "substance" of probable cause only requires a "reasonable ground" for belief that a phone contains evidence of a crime;[124] the standard "does not demand any showing that such a belief be correct or [even] more likely true than false."[125] Additionally, the "foregone conclusion" exception does not apply to situations where the defendant denies ownership or control of the smartphone.[126]

2. *Law Enforcement Cannot Use Brute Force to Unlock Smartphones*

Smartphones protected by full-disk encryption can theoretically be unlocked using "brute force," which is a trial and error method that involves running through all possible passcode combinations (e.g., "1,1,1,1," "1,1,1,2," "1,1,1,3").[127] However, brute force extraction of data from smartphones is highly unavailing for two reasons.

First, brute force extractions are so time-intensive that they are frequently considered an unviable extraction alternative.[128] This is be-

120 *Id.* at 1340.

121 *Id.*

122 *See id.* at 1346.

123 *Id.* at 1347–48 ("*Fisher* and *Hubbell* . . . require that the Government show its knowledge *that the files exist*."); *see also* SEC v. Huang, No. 15-269, 2015 WL 5611644, at *4 (E.D. Pa. Sept. 23, 2015) ("Here, the SEC has no evidence any documents it seeks are actually located on the work-issued smartphones, or that they exist at all. Thus, the foregone conclusion doctrine is not applicable.").

124 Brinegar v. United States, 338 U.S. 160, 175 (1949).

125 Texas v. Brown, 460 U.S. 730, 742 (1983).

126 *See* Fisher v. United States, 425 U.S. 391, 410, 412 (1976).

127 Martin Kaste, *Your Smartphone Is a Crucial Police Tool, If They Can Crack It*, NPR: ALL TECH CONSIDERED (Mar. 25, 2014, 2:54 PM), http://www.npr.org/sections/alltechconsidered/2014/03/25/291925559/your-smartphone-is-a-crucial-police-tool-if-they-can-crack-it; MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 4.

128 *See, e.g.*, *Encryption and Technology Issues Hearing*, *supra* note 24, at 4; Lily Hay New-

cause iOS and Android discourage passcode attacks with escalating time delays that trigger after an invalid passcode is entered at the lock screen.[129] Time delays dramatically limit the efficacy of brute force attempts; according to Apple, "it would take more than 5½ years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers."[130] Four-digit numerical passcodes may require less time, but they still could take up to 10,000 guesses.[131] In regards to iPhones, passcodes (otherwise known as Personal Identification Numbers ("PINs")) must be entered by hand on the physical device, one at a time.[132]

Second, brute force could result in a complete data wipe once a maximum number of incorrect passcodes is entered. For iOS, "[u]sers can choose to have the device automatically wiped if the passcode is entered incorrectly after 10 consecutive attempts."[133] Similarly, for Android, the data may become permanently inaccessible if a user enters an incorrect passcode a certain number of times in a row.[134]

3. The Recent Unlocking of the San Bernardino iPhone Does Not Create a Viable Method to Access a Smartphone's Contents

Although an anonymous hacker was able to access data on the San Bernardino iPhone for the FBI, this one-time unlocking is not a permanent or viable solution. As mentioned above, the FBI is un-

---

man, *Federal Judge Says Law Enforcement Can't Make You Hand Over Your Smartphone Passcode*, SLATE: FUTURE TENSE (Sept. 25, 2015, 2:41 PM), http://www.slate.com/blogs/future_tense/2015/09/25/court_rules_that_defendants_don_t_have_to_provide_smartphone_passcodes.html.

129 *See* APPLE, iOS SECURITY, iOS 9.0 OR LATER 12 (Sept. 2015).

130 *Id.* For iPhones, iOS 9 and higher now ask for a six-digit passcode by default. Jason Cipriani, *Secure Your iOS Device With a Six-Digit Passcode on iOS 9*, CNET (Sept. 11, 2015, 10:58 AM), http://www.cnet.com/how-to/secure-your-ios-device-with-a-six-digit-passcode-on-ios-9/. However, users can manually switch to a four-digit numeric code, a custom numeric code, or a custom alphanumeric code. *See* iOS SECURITY, iOS 9.0 OR LATER, *supra* note 129, at 12. For Android-powered smartphones operating on Froyo 2.2 and higher, the phone offers the ability to lock the device using a numeric or alphanumeric passcode. *See* Phil Nickinson, *Password Protect Your Phone*, ANDROID CENTRAL (Aug. 6, 2010, 11:16 AM), http://www.androidcentral.com/password-protect-your-phone.

131 Martin Kaste, *The Security Cracks In Your Smartphone*, NPR: ALL TECH CONSIDERED (Mar. 25, 2014, 2:49 PM), http://www.npr.org/sections/alltechconsidered/2014/03/25/291942703/the-security-cracks-in-your-smartphone.

132 Chris Smith, *Does Apple Even Have the Ability to Hack the iPhone Like the FBI Wants?*, BGR (Feb. 17, 2016, 12:33 PM), http://bgr.com/2016/02/17/apple-iphone-security-backdoors/.

133 iOS SECURITY GUIDE, *supra* note 107, at 11; *see also* iOS SECURITY, iOS 9.0 OR LATER, *supra* note 129, at 12.

134 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 3.

likely to share the method in every single case that involves smartphone encryption.[135] Because Apple is proactively trying to isolate and mitigate this security vulnerability,[136] the FBI has chosen to selectively use its newly-found "key" in order to protect its secrecy.[137] This fear is not unfounded; in the past, Apple has developed new security measures to close weaknesses exposed by hackers.[138] Moreover, many technology experts have speculated on the method used by the anonymous hacker—increasing the likelihood that Apple will uncover the vulnerability.[139] Apple may even pursue legal measures to force the government to disclose the vulnerability.[140] Regardless of whether Apple uncovers the actual method used, Apple engineers are continually strengthening the security of iPhones and their corresponding encryption technology.[141] For example, on March 21, 2016, Apple released iOS 9.3 which corrected an encryption flaw in iMessage.[142]

Even assuming the FBI does share its "key" before Apple can close the vulnerability, technology experts note that it may not work on every iPhone.[143] Additionally, iOS and Android are distinct mobile operating systems (with, by extension, distinct vulnerabilities) and a hack that works for one will likely not work for the other.[144]

Finally, the government's continued, ad hoc reliance on anonymous, third-party hackers disservices the public. A hacking service that only one—or at most, a few—can perform creates a hacker-controlled monopoly. A hacker who can successfully extract data from a full-disk encrypted smartphone can demand a very high price for his services.[145] Assuming future mobile operating systems have unique se-

---

135 *See* Learmonth, *supra* note 16.

136 *See supra* notes 13–15 and accompanying text.

137 *See* Learmonth, *supra* note 16.

138 *See* Apuzzo & Benner, *supra* note 15 ("Apple regularly publishes security updates and gives credit to researchers who hunt for bugs in the company's software.").

139 *See* Benner et al., *supra* note 15; Alina Selyukh, *The Apple-FBI Whodunit: Who Is Helping The Feds Crack The Locked iPhone?*, NPR: ALL TECH CONSIDERED (Mar. 23, 2016, 5:58 PM), http://www.npr.org/sections/alltechconsidered/2016/03/23/470573608/the-apple-fbi-whodunit-whos-helping-the-feds-crack-the-locked-iphone.

140 *See* Selyukh, *supra* note 13; Strohm et al., *supra* note 14.

141 *See* Apuzzo & Benner, *supra* note 15.

142 *See* Tim Moynihan, *Apple iOS 9.3 Is Available Today. Here's Why You Want It*, WIRED (Mar. 21, 2016, 1:56 PM), http://www.wired.com/2016/03/ios-9-3-is-available/.

143 *See* Richard Winton & James Queally, *Will the FBI Share Its iPhone-Cracking Method with Police? Probably Not*, L.A. TIMES (Mar. 29, 2016, 4:59 PM) http://www.latimes.com/local/lanow/la-me-ln-police-phone-access-san-bernardino-20160329-story.html.

144 *See id.*

145 Rewards can total in the millions for hackers able to demonstrate critical security vulnerabilities: Google has paid outside hackers more than $6 million for finding security flaws. *See*

curity flaws that allow a hacker to access the smartphone's contents, the government will continually have to use taxpayer dollars to pay substantial bounties for each updated system.[146] Alternatively, hackers could stop performing data extractions altogether for future mobile operating systems.[147]

4. Apple and Google Refuse to Comply with Government Search Warrants

In cases where a passcode is withheld or unable to be obtained, a prosecutor can apply to a court for a search warrant.[148] Law enforcement agencies used to be able to obtain search warrants and orders (often referred to as "unlock orders") that required tech companies to assist in data extraction procedures.[149] After obtaining an unlock order,

> [t]he prosecutor . . . then sends . . . a copy of the warrant, the unlock order, the device, and a blank external hard drive. [The mobile operating system provider] 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.[150]

However, in several recent cases, Apple has challenged the legal validity of unlock orders.[151] Many technology companies, including

---

Nicole Perlroth & Katie Benner, *Apple Policy on Bugs May Explain Why Hackers Would Help F.B.I.*, N.Y. TIMES (Mar. 22, 2016), http://www.nytimes.com/2016/03/23/technology/apple-policy-on-bugs-may-explain-why-hackers-might-help-fbi.html.

146 Cellebrite, an Israeli data forensics firm, is rumored to be the anonymous hacker that unlocked the iPhone 5c in the San Bernardino case. *See, e.g.*, Mikey Campbell, *Cellebrite Again Rumored to Have Accessed San Bernardino iPhone 5c for FBI*, APPLEINSIDER (Apr. 1, 2016, 3:54 PM), http://appleinsider.com/articles/16/04/01/-cellebrite-again-rumored-to-have-accessed-san-bernardino-iphone-5c-for-fbi. Cellebrite signed a $218,000 contract with the FBI the same day DOJ announced it unlocked the iPhone. *Id.* Over the last seven years, the FBI purchased forensic tools from Cellebrite averaging $10,883 each. *Id.* The $218,000 is the largest to date. *Id.*

147 *See* Paresh Dave, *Why Few Hackers Are Lining Up to Help FBI Crack iPhone Encryption*, L.A. TIMES (Mar. 23, 2016, 6:17 PM), http://www.latimes.com/business/technology/la-fi-tn-apple-hackers-20160323-snap-htmlstory.html (noting that the stigma of assisting the FBI with an investigation could deter potential hackers).

148 The Supreme Court held that warrants based on probable cause are required for searches of smartphone data, absent an exception. Riley v. California, 134 S. Ct. 2473, 2485 (2014).

149 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 4.

150 *Id.*

151 *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist in Search, and Opposition to Government's Motion to Compel Assistance, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (SP), 2016 WL 618401 (C.D. Cal. Feb. 25, 2016) [hereinafter Apple Inc.'s Motion to Vacate Order]; Apple Inc.'s Supplemental Response to Court's October 9, 2015 Order and Opinion, *In re* Apple, Inc., No. 15 MISC 1902 (JO) (E.D.N.Y. Oct. 23, 2015).

Google, have filed amicus briefs in support of Apple.[152] Unlock orders, thus, are no longer an effective way of compelling tech companies to extract data from full-disk encrypted smartphones.[153]

III. Critique of Other Proposals

There have been attempts to remedy this problem before. A judicial approach through the use of the All Writs Act and several legislative approaches, both on the federal and state levels, have been put forth. Taking each proposal in turn, this Part demonstrates why they are not sufficient.

A. The All Writs Act

In two highly publicized cases, the DOJ tried to use the All Writs Act to get a court order requiring Apple to help the government access data on locked, encrypted iPhones.[154] The All Writs Act says that courts have broad statutory authority to issue orders necessary to effectively carry out the duties of an independent judiciary.[155] Thus, courts may issue orders when three requirements are satisfied: (1) the issuance of the writ is "in aid of" the issuing court's jurisdiction; (2) the type of writ requested is "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and (3) the issuance of the writ is "agreeable to the usages and principles of law."[156] Apple's public statements and court filings demonstrate its opposition to writ-based unlock orders.[157] The government's use of the All Writs Act is problematic for three primary reasons.

---

152 *See, e.g.*, Brief for Amazon.com et al. as Amici Curiae Supporting Apple, Inc., *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED CM 16-10 (SP) (Mar. 4, 2016); Brief for Airbnb, Inc. et al. as Amici Curiae Supporting Apple, Inc., *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED CM 16-10 (SP) (Mar. 3, 2016).

153 *See infra* Section III.A.

154 *See In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016); *In re* Apple, Inc., 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016).

155 The All Writs Act states: "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a) (2012).

156 *In re Apple, Inc.*, 149 F. Supp. 3d at 350; *see, e.g.*, United States v. Williams, 400 F.3d 277, 280–81 (5th Cir. 2005) (quoting *In re* United States, 397 F.3d 274, 282 (5th Cir. 2005)).

157 *See The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 100 (2016) (statement of Bruce Sewell, Senior Vice President & General Counsel, Apple, Inc.); Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 14–15; Customer Letter, *supra* note 8.

First, numerous critics argue that the All Writs Act cannot be extended to compel private companies, like Apple and Google, to assist the government in unlocking encrypted smartphones.[158] Currently the only legal precedent on the issue of whether a court has the power to issue such an order is in Apple's favor.[159] In *In re Apple, Inc.*,[160] Judge Orenstein based his denial to extend the All Writs Act partly on the fact that Congress has yet to pass a law explicitly requiring tech companies to provide assistance to law enforcement.[161] Both the DOJ and Apple agreed that the CALEA[162] currently does not compel a private company to help law enforcement agencies unlock encrypted smartphones.[163] Judge Orenstein held that this omission reflects a legislative choice to exempt tech companies from complying with unlock orders for encrypted smartphones.[164] He also found that, alternatively, Apple was an "information service provider" and thus expressly exempted under the CALEA from providing the governmental assistance sought.[165]

Second, some critics argue that the government's use of the All Writs Act adds to the loss of confidence in oversight of the American national security establishment.[166] Numerous technology companies, including Apple and Google, redesigned their products to include encryption in direct response to Edward Snowden's infamous disclosure regarding the U.S. government's mass surveillance.[167] The DOJ's current reliance on the All Writs Act reignites fears tied to governmental circumvention of democratic and legal processes for investigatory purposes—"invoking 'terrorism' and moving *ex parte* behind closed courtroom doors, the government sought to cut off debate and circumvent thoughtful analysis."[168] Indeed, opponents view the government's application of the All Writs Act as an "unlimited" and

158 *See, e.g.*, Brief for Airbnb, Inc. et al., *supra* note 152; Brief for Amazon.com et al., *supra* note 152; Brief for AT&T Mobility LLC as Amici Curiae Supporting Apple, Inc. at 4–6, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED CM 16-10 (SP) (C.D. Cal. Mar. 3, 2016).

159 *See In re* Apple, Inc., 149 F. Supp. 3d at 344, 351.

160 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

161 *See id.* at 355–59.

162 For a discussion on the CALEA, see *infra* Part IV.

163 *In re Apple, Inc*., 149 F. Supp. 3d at 355.

164 *See id.* at 355–59.

165 *See id.* at 356–57.

166 *See, e.g.*, Yochai Benkler, *We Cannot Trust Our Government, So We Must Trust the Technology*, GUARDIAN (Feb. 22, 2016, 8:00 AM), http://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi.

167 *See* Apuzzo & Benner, *supra* note 15.

168 Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 2, 5.

"sweeping use of the judicial process."[169] Critics believe that the All Writs Act does not sufficiently hold the government accountable and guard privacy interests. They warn that this precedent could be extended to access data from other products and unwilling private companies (e.g., microphones on televisions, computers, and even children's toys).[170]

Third, reliance on the All Writs Act would produce inconsistent results. Even if a subsequent court were to grant the government's order, the All Writs Act is discretionary and judges are not required to grant orders even if all three statutory requirements are met.[171] Moreover, historically, legislatures have prescribed mandatory law enforcement assistance requirements that involve technological changes on the part of private companies.[172] The "information environment of legislative rulemaking is superior to that of judicial rulemaking in the context of developing technologies."[173] Unlike Congress,[174] "[j]udges decide cases based primarily on a brief factual record, narrowly argued legal briefs, and a short oral argument. They must decide their cases in a timely fashion, and can put only so much effort into any one case."[175] Legislation, as opposed to a judicially-issued writ, is the only feasible solution to this problem.

---

169 *Id.* at 1; *see* Benkler, *supra* note 166.

170 *See, e.g.*, Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 25–26; OLSEN ET AL., *supra* note 75, at 13–15.

171 *See, e.g.*, 28 U.S.C. § 1651(a) (2012) ("The Supreme Court and all courts . . . *may* issue all writs . . . ." (emphasis added)); Morrow v. District of Columbia, 417 F.2d 728, 736 (D.C. Cir. 1969); Paramount Film Distrib. Corp. v. Civic Ctr. Theatre, Inc., 333 F.2d 358, 360 (10th Cir. 1964).

172 *See, e.g.*, 18 U.S.C. § 2703(f)(1) (2012) (requiring providers "of wire or electronic communication services" to assist law enforcement by preserving specified evidence); 47 U.S.C. § 1007(a) (2012) (providing authority for court-issued orders to communications carriers requiring carriers to assist law enforcement).

173 Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 881 (2004).

174 On February 29, 2016, Senator Mark Warner introduced in the Senate a bipartisan bill to establish in the legislative branch the National Commission on Security and Technology Challenges. The purpose of the Commission is:

> To bring together leading experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community . . . and the national security community to examine the intersection of security and digital security and communications technology . . . and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace.

Digital Security Commission Act of 2016, S. 2604, 114th Cong. § 3(b)(1) (2016).

175 *See* Kerr, *supra* note 173, at 875 (footnote omitted).

B. The Manhattan District Attorney's Office's White Report

In November 2015, the Manhattan District Attorney's Office released a report calling for a legislative solution to full-disk encryption on smartphones.[176] The report called for state and federal legislation that would require "that any smartphone manufactured, leased, or sold in the U.S. must be able to be unlocked" pursuant to a lawful search warrant and unlock order.[177]

Critics argue that the proposed legislation takes an "absolutist" approach and, as such, does not adequately take into consideration Apple and Google's interests.[178] But what if full-disk encryption is not as "impossible" to crack as the government asserts? What if it does not frustrate as many investigations and prosecutions as previously suggested? Regardless, under the proposed legislation, Apple and Google will still have to produce smartphones with "weakened" encryption.[179] As discussed above, the government has already successfully unlocked an iPhone 5c running iOS 9 with the assistance of a third party hacker,[180] and Zerodium, a firm that sells security vulnerabilities to the U.S. government and private corporations, reported that a team of hackers had successfully exploited a flaw in iOS 9.[181] Apple and Google do have an interest in the quality of their products and their company brands. These brands are, in fact, built on privacy and security.[182] It may negatively impact the companies' brands if the public perceives the companies as "weakening" security and assisting the government to extract "private" data.[183] This is a distinct possibility given that both companies (particularly Apple) have heavily marketed their opposition to any government-imposed changes in their mobile operating systems.[184]

---

176 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 13.

177 *Id.*

178 Benner & Perlroth, *supra* note 8.

179 *See id.*

180 *See* Benner & Lichtblau, *supra* note 3.

181 *See* Perlroth & Benner, *supra* note 145.

182 *See* Katie Benner & Paul Mozur, *Apple Sees Value in Its Stand to Protect Security*, N.Y. TIMES (Feb. 20, 2016), http://www.nytimes.com/2016/02/21/technology/apple-sees-value-in-privacy-vow.html.

183 *Cf.* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html (discussing the loss to American tech companies in foreign markets after Snowden's revelations).

184 *See, e.g.*, Benner & Mozur, *supra* note 182; Benner & Perlroth, *supra* note 8; Customer Letter, *supra* note 8.

The proposal could also be seen as deputizing private corporations without providing just compensation. This is because the proposed legislation does not contemplate a reimbursement scheme.[185] According to Apple, it would take a team of six to ten Apple engineers and employees between two to four weeks to develop a decryptable mobile operating system.[186] The proposed legislation would force Apple to bear the entire cost of development.

C. Legislative Solutions at the State Level

Currently two states—New York and California—have introduced bills that would require smartphones sold in the state to be amenable to search warrants. New York Assemblyman Matthew Titone (D-Staten Island) introduced legislation, bill A8093, that would require any smartphone manufactured, sold, or leased in New York to be "capable of being decrypted and unlocked by its manufacturer or its operating system provider."[187] Any smartphone that cannot be decrypted and unlocked will subject its seller or lessor to a $2500 fine. California Assemblyman Jim Cooper (D-Elk Grove) introduced legislation, bill AB 1681,[188] that would subject a manufacturer or operating system provider to "a civil penalty of $2500 for each instance in which the smartphone is unable to be decrypted," if decryption is ordered by a state court.[189] Neither bill proposes a compensation scheme to reimburse companies for the costs of reengineering smartphones to be amenable to search warrants and unlocking them pursuant to a court order.[190] Additionally, neither bill states what the funds from the civil penalty will be used for.[191]

---

185 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 13.

186 *See* Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 13.

187 A8093A, 2016 Leg., 239th Sess. (N.Y. 2016). Assemblyman Titone introduced the bill on June 8, 2015, *see id.*, and it was referred to committee in January 2016 following publicity around DA Vance's white report. *See* Tom Risen, *New York Bill Aims to Ban Encrypted Phones*, U.S. NEWS (Jan. 15, 2016, 5:46 PM), http://www.usnews.com/news/articles/2016-01-15/new-york-bill-aims-to-ban-encrypted-phones.

188 AB-1681, 2016 Leg., 2015–2016 Sess. (Cal. 2016). Assemblyman Copper introduced the bill on January 20, 2016, and the bill was amended in assembly on March 28, 2016, after this Note had been substantially drafted. *See id.* The bill as first introduced was nearly identical to the pending New York bill, however, the stated rationale was to fight human trafficking rather than terrorism. *See* Cyrus Farivar, *Yet Another Bill Seeks to Weaken Encryption-by-Default on Smartphones*, ARS TECHNICA (Jan. 21, 2016, 5:00 AM), http://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones/; *see also* N.Y. A8093A § 1.

189 Cal. AB-1681.

190 *See* Cal. AB-1681; N.Y. A8093A.

191 *See* Cal. AB-1681; N.Y. A8093A.

Opponents criticize New York and California's pending bills in part because they are state legislation.[192] If the New York and California bills passed, a tech company (like Apple or Google) that sells encrypted-by-default smartphones would have four options. One, a tech company could stop including full-disk encryption on its smartphones. For companies like Apple and Google, this would contradict almost two years of outspoken statements on encryption technology and its corresponding privacy and security benefits.[193] Indeed, Apple has a built a "global marketing strategy" around privacy and security (particularly against government intrusion).[194] Two, a tech company could cease selling smartphones in two of the richest states in the United States.[195] It would be ironic if California-based Apple and Google could not sell smartphones in the Silicon Valley state. Three, a tech company could create decryptable smartphones for those states to abide by their anti-encryption laws. This third option would most likely result in New York or California residents purchasing full-disk encrypted smartphones from neighboring states.[196] Differences in products across states create incentives for secondary market sales.[197] Additionally, the California bill only imposes a fine for each instance that a smartphone cannot be decrypted pursuant to a "state court order."[198] The bill would do nothing to further federal investigations and prosecutions in the state. Thus, the state legislation ultimately would not further law enforcement investigations because criminals and future victims could still obtain a full-disk encrypted smartphone with a quick trip across the state border. Moreover, the pending bills would

192 *See* Brian Barrett, *New Bill Aims to Stop State-Level Decryption Before It Starts*, WIRED (Feb. 10, 2016, 3:27 PM), http://www.wired.com/2016/02/encrypt-act-2016/.

193 *See* Benner & Perlroth, *supra* note 8; Customer Letter, *supra* note 8.

194 Apuzzo & Benner, *supra* note 15; *see also* Benner & Mozur, *supra* note 182.

195 *See* U.S. CENSUS BUREAU, MEDIAN HOUSEHOLD INCOME (IN 2013 INFLATION-ADJUSTED DOLLARS) BY STATE RANKED FROM HIGHEST TO LOWEST USING 3-YEAR AVERAGE: 2011-2013; Megan Willett, *The Wealthiest People in America Live in These States*, BUS. INSIDER (Mar. 24, 2015, 2:05 PM), http://www.businessinsider.com/us-states-with-the-wealthiest-residents-2015-3.

196 *See* Barrett, *supra* note 192.

197 For example, immediately after New York City and State cigarette tax increased in April 2002, there was a "'flood' of cigarette smuggling into NYC and a rise in illegal sales of untaxed cigarettes." Donna Shelley et al., *The $5 Man: The Underground Economic Response to a Large Cigarette Tax Increase in New York City*, 97 AM. J. PUB. HEALTH 1483, 1483 (2007). A New York City Department of Health and Mental Hygiene's Community Health Survey reported that eighty-nine percent of cigarettes in New York City were purchased through alternative sales channels (i.e., not through New York City retailers). *Id.*

198 AB-1681, 2016 Leg., 2015–2016 Sess. (Cal. 2016).

negatively impact the economy in those states by driving away business from New York and California smartphone retailers.[199]

And finally, four, in regard to the California bill, tech companies would likely continue to sell encrypted smartphones in the state. The state legislation would not have "the clout to affect multinational corporations like Apple and Google."[200] Over the course of one year, the Manhattan District Attorney's Office reported that it had 175 smartphones that it could not decrypt.[201] Covering a population of approximately 1.644 million,[202] that is roughly one inaccessible smartphone per every 9394 individuals. Presuming that this ratio is constant, there will be approximately 4167 smartphones that California law enforcement cannot decrypt every year.[203] This would result in the imposition of a $10.417 million civil penalty each year to be shared amongst the manufacturers and mobile operating system providers of those inaccessible smartphones. However, this penalty would be unlikely to compel tech companies to reengineer their smartphones to be decryptable pursuant to a court order. In just the third quarter of fiscal year 2015, Apple had a quarterly net profit of $10.7 billion,[204] while Google had a quarterly net profit of $3.979 billion.[205] Even if each respective company were to pay the entire estimated yearly penalty, it would only constitute 0.097% of Apple's quarterly net profit and 0.261% of Google's.[206] Moreover, the civil penalty would likely not be shouldered by one company (or even two). The California bill fines the "manufacturer or operating system provider,"[207] and there are presently at least ten distinct companies that manufacture

199 *See* Barrett, *supra* note 192.

200 Ellen Nakashima, *Officials Seizing the Moment of Paris Attacks to Rekindle Encryption Debate*, WASH. POST (Nov. 18, 2015), https://www.washingtonpost.com/world/national-security/officials-seizing-the-moment-of-paris-attacks-to-rekindle-encryption-debate/2015/11/18/cdb89400-8d5c-11e5-acff-673ae92ddd2b_story.html.

201 *See* Benner & Apuzzo, *supra* note 64.

202 This information is current as of July 1, 2015. U.S. CENSUS BUREAU, QUICKFACTS: NEW YORK COUNTY (MANHATTAN BOROUGH), NEW YORK, http://www.census.gov/quickfacts/table/PST045215/36061,36 [https://perma.cc/GE79-ZFRE] (last visited Feb. 6, 2017).

203 As of July 1, 2015, California has a population of approximately 39,144,818. U.S. CENSUS BUREAU, QUICKFACTS: CALIFORNIA, http://www.census.gov/quickfacts/table/PST045215/06,00 [https://perma.cc/PSQ3-W7SZ] (last visited Feb. 6, 2017).

204 Press Release, *Apple Reports Third Quarter Results*, APPLE (July 21, 2015), http://www.apple.com/pr/library/2015/07/21Apple-Reports-Record-Third-Quarter-Results.html?sr=hotnews.rss [https://perma.cc/H77Z-Z3LK].

205 Jared Dipane, *Google Announces Q3 2015 Results: $18.7 Billion in Revenue, $3.97 Billion Net Income*, ANDROID CENTRAL (Oct. 22, 2015, 4:19 PM), http://www.androidcentral.com/google-announces-q3-2015-results-187-billion-revenue-397-billion-net-income.

206 *See supra* notes 203–05 and accompanying text.

207 AB-1681, 2016 Leg., 2015–2016 Sess. (Cal. 2016).

smartphones or engineer mobile operating systems in the United States.[208] In sum, this solitary bill would not motivate companies to reengineer their encryption technology; the bill's effectiveness depends on other states adopting congruent legislation. Because there are no other pending state bills similar to California's, the absence of extrajurisdictional penalties diminishes the proposed scheme's effectiveness.

Critics of the pending bills argue that state legislation concerning smartphone encryption would be illegal under the Dormant Commerce Clause.[209] The Dormant Commerce Clause is a constitutional doctrine that forbids states from enacting legislation that imposes undue burdens on interstate commerce.[210] Opponents argue that the pending bills would place undue burdens on interstate commerce for many of the reasons discussed above (e.g., forcing companies to create substantially different mobile operating systems for each state).[211]

On February 11, 2016, due to concerns associated with the impracticality of state-by-state encryption laws, a bipartisan group of legislators in the U.S. Congress introduced the ENCRYPT Act of 2016. The Act would prevent states and localities from passing laws banning encryption on smartphones sold in the United States.[212] The Act is specifically aimed at the pending legislation in New York and California.[213]

Additionally, nothing in the New York bill prevents Apple and Google from making the fully encryption-enabled version of its mobile operating system available to anyone who, after purchasing the smartphone, can get the encryption technology through a software update. Under the pending bill, the seller or lessor is only subject to the $2500 civil penalty if the retailer knew "at the time of the sale or lease that the smartphone was not capable of being decrypted and unlocked

---

208 *See* Victor H., *Top 10 Smartphone Makers in Q1 2015: Sony and Microsoft Drop Out of the Picture, Chinese Phone Makers Take Over*, PHONE ARENA (May 25, 2015, 4:46 AM), http://www.phonearena.com/news/Top-10-smartphone-makers-in-Q1-2015-Sony-and-Microsoft-drop-out-of-the-picture-Chinese-phone-makers-take-over_id69643.

209 *See* Farivar, *supra* note 188.

210 The Dormant Commerce Clause is inferred from the Commerce Clause in Article I of the United States Constitution. *See, e.g.*, McBurney v. Young, 133 S. Ct. 1709, 1719 (2013); United States v. Lopez, 514 U.S. 549, 579 (1995). The Commerce Clause expressly grants Congress the power to regulate commerce "among the several states." U.S. CONST. art. I, § 8, cl. 3. This grant of power implies a negative converse.

211 *See* Barrett, *supra* note 192.

212 Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016, H.R. 4528, 114th Cong. § 2 (2016).

213 *See id.*

by its manufacturer or its operating system provider."[214] Thus, criminals and future victims could frustrate New York investigations and prosecutions with a trivial software update.

Further, the New York bill exclusively punishes retailers.[215] Manufacturers and mobile operating system providers are not subject to any civil penalty.[216] It is inherently unfair to punish the retailer for an encryption technology that it had no hand in creating.[217] The New York bill works indirectly to achieve its goal: it imposes a civil penalty on retailers to discourage the sale of full-disk encrypted smartphones in order to ultimately force manufacturers and mobile operating system providers to reengineer their products.

The California bill is silent on how the government would determine whether to fine the "manufacturer or [the] operating system provider."[218] Sometimes the manufacturer and the mobile operating system provider are the same company, like for Apple's iPhones.[219] However, for the majority of smartphones running Android, the manufacturer and mobile operating system provider are two separate companies.[220] The bill's silence could easily lead to arbitrary and inconsistent results. For example, the state government could fine Google for one instance of an inaccessible LG G5 (a smartphone made by LG Electronics ("LG") that runs Android) and then LG for the next five.

IV. Background on the CALEA

Having now explored various judicial and legislative solutions, this Part discusses a pertinent federal legislative Act that will form the basis of this Note's proposal.

Beginning in the 1990s, emerging digital and wireless technologies have increasingly frustrated law enforcement efforts to facilitate court-authorized surveillance.[221] In response, Congress, concerned about the efficacy of modern law enforcement, prompted the Govern-

214 A8093A, 2016 Leg., 239th Sess. (N.Y. 2016).

215 *See id.*

216 *See id.*

217 In fact, the California bill, when it was first introduced, subjected only the seller or lessor to the civil penalty. However, the state legislature explicitly amended the bill to state that the "inability of a smartphone manufacturer or its operating system provider to decrypt the contents of the smartphone . . . shall not result in liability to the seller or lessor." AB-1681, 2016 Leg., 2015–2016 Sess. (Cal. 2016).

218 *Id.*

219 *See supra* note 44 and accompanying text.

220 *See supra* note 51 and accompanying text.

221 *See* King, *supra* note 26, at 178.

ment Accountability Office to examine the growing application of digital technology in public telephone systems.[222] Their investigation found that digitalization could potentially inhibit the FBI's ability to effectively wiretap and surveil suspects.[223] Unfortunately, this concern manifested as more than just a hypothetical impediment: a 1992 FBI survey indicated that advanced telecommunications technologies prevented law enforcement from carrying out court-authorized electronic surveillance in ninety-one instances.[224] Congress felt compelled to rectify this burgeoning problem and ultimately enacted in 1994 the Communications Assistance for Law Enforcement Act.[225] This Act ensures that court-authorized surveillance investigations could survive contemporary technological advancements.[226]

A. Requirements

"The primary purpose of the CALEA is to clarify a telecommunications carrier's duty to assist law enforcement agencies with the lawful interception of communications and the acquisition of call-identifying information in an ever-changing telecommunications environment."[227] The CALEA requires that telecommunications carriers meet the assistance capability requirements in section 1002.[228] Generally, section 1002 requires that telecommunication carriers ensure their equipment, facilities, and services are capable of enabling the government, pursuant to a court order, to effectively intercept communications within the carrier's service area, to or from its equipment, concurrently with the transmission.[229] The carriers must assist law enforcement, even "to the exclusion of any other communications."[230] Telecommunications carriers must also allow law enforcement access

222 *See* U.S. Gov't Accountability Office, FBI: Advanced Communications Technologies Pose Wiretapping Challenges (July 1992).

223 *See id.* at 2 ("[S]ince 1986, the FBI has become increasingly aware of the potential loss of wiretapping capability due to the rapid deployment of new technologies, such as cellular and integrated voice and data services, and the emergence of new technologies such as Personal Communication Services, satellites, and Personal Communication Numbers.").

224 *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearing Before the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil & Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 36 (1994) (statement of Louis J. Freeh, Director, FBI).

225 Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (2012).

226 *See* Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Reg. 53643 (Oct. 16, 1995).

227 *Id.*

228 *See* 47 U.S.C. § 1002.

229 *See id.* § 1002(a)(1).

230 *Id.*

to "call-identifying information that is reasonably available to the carrier . . . before, during, or immediately after the transmission."[231]

B. Reimbursement

At the outset, the CALEA dedicated $500 million to reimburse telecommunications carriers for upgrades and modifications that were made during fiscal years 1995 through 1998.[232] The affected industries raised concerns that the $500 million would be insufficient to compensate telecommunications carriers for their start-up costs.[233] For this reason, if compliance is not reasonably achievable, and the Attorney General does not agree to reimburse, the telecommunications carrier will be deemed in compliance without having to perform the modifications required under section 1003.[234] The carrier will continue to be deemed in compliance unless it notably modifies the relevant equipment, facility, or service.[235] After the initial four-year period,[236] the government will no longer reimburse telecommunications carriers, and the affected companies will bear "reasonable costs of compliance," to be determined by the FCC.[237]

C. Enforcement

A court may impose a civil penalty against a telecommunications carrier of up to $10,000 per day for its failure to comply with the CALEA.[238] A court can impose a civil penalty only if: (1) it finds that law enforcement has no other reasonably available alternatives (such as another carrier) to implement interception; and (2) compliance with the CALEA would have been "reasonably achievable" on the

---

231 *Id.* § 1002(a)(2).

232 *Id.* § 1009. The Act provides that the Attorney General may reimburse telecommunications carriers for "all reasonable costs directly associated" with modifications to equipment, facilities, and services installed on or before January 1, 1995. *Id.* § 1008(a). The Federal Communications Commission ("FCC") determines, on petition, whether a telecommunications carrier will be compensated/receive funds for such changes after January 1, 1995. *Id.* § 1008(b)(1).

233 *See* 140 CONG. REC. H27,707 (daily ed. Oct. 4, 1994) (statement of Rep. Hyde).

234 The telecommunications carrier may petition the FCC to determine whether compliance would impose significant difficulty or expense. *See* 47 U.S.C. § 1008(b)(1). The FCC bases its decision on ten enumerated factors, including public safety and national security, and one catchall factor. *Id.* § 1008(b)(1)(A)–(K).

235 *See id.* § 1008(d).

236 The FCC may extend the transition period up to two additional years. 140 CONG. REC. H27,707 (daily ed. Oct. 4, 1994) (statement of Rep. Hyde).

237 *See id.*

238 18 U.S.C. § 2522(c)(1).

part of the offending carrier.[239] A court can mandate that the offending carrier perform the required upgrades and modifications to bring it into compliance with the CALEA, so long as the directed upgrades and modifications do not result in unreasonable costs that will not be reimbursed by the Attorney General.[240]

D. Inapplicability to Smartphone Data

Since the introduction of the first widely adopted smartphone in 2007,[241] it has been quickly noted that the CALEA does not apply to data on these smartphone devices.[242] This has sparked a "great deal of debate" about expanding the Act.[243] In 2009, the FBI voiced concerns about the CALEA's inability to reach smartphone data.[244] In the following years, the agency spoke before Congress on the "Going Dark" problem[245] and drafted amendments to the CALEA that would encompass smartphone data.[246] The Justice Department approved the draft legislation, but the White House never sent the proposed CALEA amendments to Congress.[247]

V. Congress Must Amend the CALEA to Address Full-Disk Encryption on Smartphones

As Justice Alito observed, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public

---

239 47 U.S.C. § 1007(a).

240 *See id.* § 1007(c).

241 King, *supra* note 26, at 178.

242 *Id.*

243 *Id.*; *see In re* Apple, Inc., 149 F. Supp. 3d 341, 355 (E.D.N.Y. 2016) (noting that both the government and Apple agree that the CALEA does not compel a private company, such as Apple, to help the government access an encrypted phone's data).

244 King, *supra* note 26, at 178.

245 Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people are not always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.

James Comey, Dir., Fed. Bureau of Investigation, Speech at the Brookings Institution, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014) (transcript available at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course).

246 *See* King, *supra* note 26, at 178.

247 *Id.* at 179.

safety in a comprehensive way."[248] By enacting legislation, "the United States could make clear that the era of 'secret cooperation' [between the government and U.S. tech companies] is over."[249]

This Note proposes an amendment to the CALEA that gives manufacturers and mobile operating system providers a choice to either make smartphones amenable to search warrants or pay a civil penalty each time a smartphone cannot be decrypted pursuant to a court order. Under the proposed amendment, manufacturers and mobile operating system providers would be liable for $127,500[250] for each instance that law enforcement cannot unlock or otherwise access the data on a smartphone it has the legal authority to search.[251] This civil penalty scheme is similar to that being considered by the California legislature in the bill described in Section IV.B.[252] However, this Note's proposed amendment effectively responds to the criticisms and failings raised by other proposals (including the pending California bill).[253]

Under this Note's proposed amendment, the law enforcement agency must obtain a search warrant and unlock order from the court with proper jurisdiction. In order for the court to issue an unlock order, it must first find that the moving law enforcement agency exhausted its technological capabilities. This will help safeguard against a deputization of Apple and Google as the IT department of the state and U.S. governments,[254] and prevent (quite literally) unwarranted intrusions into citizens' privacy.

---

248 United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) (citation omitted); *see, e.g.*, Kerr, *supra* note 173.

249 Reema Shah, Comment, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, 125 YALE L.J. 543, 558 (2015).

250 This number constitutes the medium payment made to hackers by the U.S. government. *See* Jayesh Limaye, *$250,000 Paid To Reveal iOS Exploit*, TECHTREE (July 3, 2012, 8:51 PM), http://www.techtree.com/content/news/879/250000-paid-to-reveal-ios-exploit.html. However, this number serves more as a placeholder and is by no means the exact number that should be adopted. This Note argues that open debate in Congress would lead to the optimal civil penalty. *See supra* notes 173–75 and accompanying text.

251 In cases where the same company is both the manufacturer and the mobile operating system provider, the company will have to pay a total of $255,000. There are two distinct wrongs given the two different capacities that the manufacturer and mobile operating system provider serve.

252 *See* AB-1681, 2016 Leg., 2015–2016 Sess. § 2(b) (Cal. 2016) ("A manufacturer or operating system provider of a smartphone sold or leased in California on or after January 1, 2017, shall be subject to a civil penalty . . . for each instance in which the manufacturer or operating system provider of the smartphone is unable to decrypt the contents of the smartphone pursuant to a state court order.").

253 *See supra* Part IV.

254 *See supra* notes 184–86 and accompanying text.

Companies that make their smartphones amenable to search warrants (by either giving law enforcement a method to access the data or accessing the data for law enforcement) will avoid civil penalties and be reimbursed for the costs of their compliance with the proposed statutory scheme. Similar to CALEA sections 1008 and 1009, the amendment authorizes $500 million[255] to reimburse manufacturers and operating system providers for the costs associated with reengineering their smartphones.[256] The funds will be available until exhausted or four fiscal years have passed since the amendment's enactment.[257] To quell potential concerns about insufficient compensation, the amendment contains a provision similar to section 1008(b)(1) and (d) of the CALEA: if a manufacturer or mobile operating system provider cannot "reasonably achieve" compliance, and the Attorney General does not agree to reimburse, the company will be deemed compliant and thus exempt from the civil penalty.[258] After the initial four-year period, the government will no longer reimburse manufacturers and mobile operating system providers, and the affected companies will bear "reasonable costs of compliance."[259] This part of the reimbursement scheme is limited to four years in order to encourage companies to immediately make smartphones amenable to search warrants. Additionally, under the proposed amendment, the government will compensate the manufacturer or mobile operating system provider for each smartphone that needs to be unlocked using a proprietary method that only the company possesses. Reimbursement for data extractions of specific smartphones will continue indefinitely.

Under this Note's proposed legislation, manufacturers and mobile operating system providers do not have to make smartphones amenable to search warrants. If a company elected not to make its smartphones amendable to a search warrant, investigators could bring a civil suit against it. For federal investigations and prosecutions, a U.S. Attorney may bring civil suit in federal court for any inaccessible, legally searchable smartphone in his district. Similarly, for state investigations and prosecutions, the Attorney General of that state or the

255 This is the same amount that the CALEA allotted to reimburse telecommunications carriers. *See* 47 U.S.C. § 1009 (2012). However, this Note recognizes that open debate is necessary to achieve the correct reimbursement amount to be set aside for manufacturers and mobile operating system providers wanting to make their products amenable to search warrants. *See supra* notes 173–75 and accompanying text.

256 *See supra* note 232 and accompanying text.

257 *See supra* note 236 and accompanying text.

258 *See supra* notes 234–37 and accompanying text.

259 *See supra* notes 236–37 and accompanying text.

District Attorney of that jurisdiction may bring civil suit in federal court for any inaccessible, legally searchable smartphone. The court would then have the ability to impose the $127,500 civil penalty only if law enforcement has no "reasonable alternative" to access the phone's data. A reasonable alternative is limited to one of the following: (1) the user consents; (2) law enforcement obtains a court order requiring the user to unlock his smartphone or provide its contents; or (3) law enforcement has in its possession the technological capability to safely unlock the smartphone at issue. Regarding the third reasonable alternative, law enforcement must actually possess the technology—the fact that law enforcement can pay a third-party hacker will not exempt the companies from the civil penalty. The amendment will prohibit the manufacturer and mobile operating system provider from passing on any portion of the costs associated with compliance or the civil penalty.

Rather than go into the state or U.S. Treasury (as most civil penalties do),[260] the civil penalties here will be paid directly to the respective state or federal investigative agency that obtained the search warrant and unlock order. With the money going to these agencies, the fine will more directly further investigative and prosecutorial efforts. The civil penalties can be used to create specialized investigative teams, training programs to respond to changing technology, or to recoup the costs of paying a third-party hacker. For example, state governments and the DOJ could create both entry-level and advanced onsite training courses for law enforcement that are aimed at improving the investigation of electronic crimes and the collecting and examining of technology-based evidence.[261] Jurisdictions can partner with the private high-tech industry to develop a joint task force or can create an onsite high-tech task force that is trained to investigate electronic crimes and examine technology-based evidence.

This Note's proposed amendment puts the decision in the hands of the affected private companies. The statute imposes a civil penalty to force tech companies to engage in a more balanced weighing of the

---

260 Kathleen Pender, *When Government Fines Companies, Who Gets Cash?*, SFGATE (May 6, 2010, 4:00 AM), http://www.sfgate.com/business/networth/article/When-government-fines-companies-who-gets-cash-3189724.php.

261 The FBI "lost a chance to capture data" from the iPhone in the San Bernardino case when FBI personnel mistakenly believed that resetting the iCloud passcode would grant access to the data on the iPhone. Kang & Lichtblau, *supra* note 4. Instead, "the change had the opposite effect—locking [the FBI] out and eliminating other means of getting in." *Id.* Perhaps this mistake (and subsequent litigation) could have been avoided if federal investigative agencies had specialized training programs focused exclusively on investigating and using technology.

costs and benefits. Companies currently have no incentive to make smartphones amenable to search warrants. As mentioned, Apple and Google publicly advocated against altering current full-disk encryption technology on their mobile operating systems.[262] They have created a brand based on privacy and security, particularly against government intrusion.[263]

This Note's proposed amendment takes a balanced approach to remedying the encryption problem. The civil penalty is attached to only those smartphones that the government has the legal authority to search but cannot decrypt. The civil penalty should be substantial enough to "highly encourage" manufacturers and mobile operating system providers to elect to make their smartphones amenable to search warrants; however, the penalty should not be so substantial as to unequivocally prevent companies from selling full-disk encrypted smartphones.

The amendment can adapt to the nebulous intersection of tech and law enforcement; for example, the government may only infrequently encounter inaccessible smartphones. If this highly unlikely supposition becomes a reality,[264] then forcing private companies to reengineer their mobile operating systems for every smartphone sold in the United States would be an excessive response. If most defendants voluntarily disclose their passcodes or are made to provide their smartphone's data or physically unlock it using their passcode or fingerprint, then there is no harm to law enforcement investigations and thus no civil penalty imposed on tech companies. If law enforcement possesses the technology, then companies will not have to pay the civil penalty.[265] This Note's proposed amendment limits the imposition of a civil penalty (or private companies' assistance) to those few cases that are truly detrimental to the public interest. The investigative agency will receive $127,500 to offset the costs of paying a hacker or pursue other investigatory avenues in cases where the smartphone is indisputably inaccessible.

---

262 *See, e.g.*, Brief for Amazon.com et al. as Amici Curiae, *supra* note 152; Benner & Perlroth, *supra* note 8; Customer Letter, *supra* note 8.

263 *See supra* notes 182–84 and accompanying text.

264 *See supra* Part II.

265 For instance, the FBI currently has the technology to unlock some iPhones running iOS 9 and older versions. *See* Benner & Lichtblau, *supra* note 3. An anonymous third-party hacker gave the FBI a previously unknown tool that could access the data on at least one iPhone, *see id.*, which may potentially be used to unlock others, *see* McCallister, *supra* note 21.

On the other hand, if—as current evidence suggests[266]—smartphone encryption is consistently an impediment to law enforcement investigations, then companies will be persuaded by the frequently-imposed civil penalty to make smartphones amenable to search warrants.

VI. Responses to Counterarguments

This Part addresses and refutes the three biggest counterarguments to this Note's proposal. These three arguments include: (A) that making smartphones amenable to search warrants would weaken the phone's security; (B) that the technology industry would be overly financially burdened; and (C) that authoritarian governments would be able to harm their citizens through this technology.

A. Any Loss in Personal Security and Privacy Would Be Insignificant

Opponents argue that any effort to make smartphones amenable to search warrants would necessarily weaken the smartphone's security and "thus increase the possibility of a bad actor unlawfully accessing device data."[267] However, any loss in personal security and privacy would be insignificant for at least four reasons.

First, the high-profile security breaches that fueled a nationwide desire for heightened data security and privacy did not involve data at rest[268] on smartphones.[269] Many opponents conflate the concerns regarding compromised end-to-end encryption (data in transit) with full-disk encryption (data at rest).[270] End-to-end encryption involves encryption at the end points of live data transfers or communication

---

266 *See supra* Part II.

267 Manhattan Dist. Attorney's Office, *supra* note 71, at 14; *see, e.g.*, Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 7; Olsen et al., *supra* note 75, at 1; *Answers to Your Questions About Apple and Security*, Apple, http://www.apple.com/customer-letter/answers/ [https://perma.cc/L2PZ-48FL] (last visited Feb. 6, 2017); Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, Wash. Post (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html.

268 Data at rest (also known as device encryption), "in which the keys exist only on locked devices[,] prevents the contents from being read by anyone who does not possess the keys." Olsen et al., *supra* note 75, at 4.

269 *See* Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. Times (Aug. 15, 2015), http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html (discussing the NSA wire-tapping event); Blistein, *supra* note 89 (discussing the hacker who leaked the personal contents of information stored in celebrities' cloud accounts).

270 *See* Olsen et al., *supra* note 75, at 4; Brad Reed, *The FBI Has Laid a Clever Trap for*

channels, and "only the original sender and intended recipient possess the keys necessary to decrypt the message."[271] Thus, "the information is (in theory, and as advertised) not capable of being read by anyone who sees it traverse a network between the sender and the receiver, including an intermediary service provider, such as Apple."[272] The ability of law enforcement to "decrypt data in transit presents unique risks that are simply not presented by the ability to decrypt data at rest."[273] Notably, "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."[274] At least in regard to Apple, the company's passcode-bypass process cannot be used remotely.[275] Even if a maligned hacker were to learn Apple's decryption process, he would still need the physical iPhone to be able to decrypt and access its data.[276]

Second, an individual's privacy still receives the protection of the Fourth Amendment. In *Riley v. California*,[277] the Supreme Court held that the Fourth Amendment requires warrants for searches of smartphone data.[278] A judge may only issue a search warrant for a smartphone if there is probable cause to believe that it contains evidence or proceeds of a crime.[279] The *Riley* Court acknowledged that cellphones keep "a digital record of nearly every aspect of their lives—from the mundane to the intimate"; however, it ultimately held that the Fourth Amendment and its search warrant requirement are sufficient privacy safeguards.[280] Indeed, Apple and Google seek to unilaterally alter Supreme Court jurisprudence that affords the home the highest level of privacy protection.[281] If "[e]very home can be en-

---

Apple, BGR (Feb. 17, 2016, 4:24 PM), http://bgr.com/2016/02/17/fbi-vs-apple-smartphone-encryption/.

271 OLSEN ET AL., *supra* note 75, at 4.

272 *Id.*

273 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 14.

274 *Id.*

275 *Id.*; *see* Customer Letter, *supra* note 8 ("[T]his software . . . would have the potential to unlock any iPhone in someone's *physical possession*." (emphasis added)).

276 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 14.

277 134 S. Ct. 2473 (2014).

278 *Id.* at 2485.

279 U.S. CONST. amend. IV.

280 *Riley*, 134 S. Ct. at 2490, 2493.

281 *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("But when it comes to the Fourth Amendment, the home is first among equals. At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).

tered with a search warrant," then "[t]he same should be true of [smartphone] devices."[282]

Third, smartphones have additional security features (beyond encryption) to protect one's data if a user's smartphone were to be stolen. For example, if the user had previously enabled the Find My iPhone App or a certain setting in Android Device Manager, he could remotely wipe the smartphone's data.[283]

Fourth, the privacy and security argument advanced by opponents presumes and depends on the encryption technology being absolutely uncrackable. Critics claim that the tool or software the government asked Apple to build in the San Bernardino case—and presumably the same tool or software that the government eventually got from a third-party hacker—would "[o]nce created . . . be used over and over again, on any number of devices" and thus "expose [Apple's and Google's] customers to a greater risk of attack."[284] Opponents argue that the mere existence of such a decryption tool or software—whether it be held by the mobile operating system provider itself or the government—would invariably "get out" to bad actors.[285] But this argument assumes that such a tool is impossible to create and that Apple's and Google's security is otherwise impenetrable. As mentioned, the government currently has access to an unknown tool or software created by a third-party hacker that can at least access iPhones running iOS 9.[286] And other hackers have been able to "crack" the supposedly inaccessible iOS software.[287] Under this Note's proposed legislation,[288] Apple and Google could save themselves from the imposition of a fine (along with saving the government time in time-sensitive investigations) by constructing the decryption tool or software themselves before the government has to enlist a third-party hacker. Additionally, Apple and Google—companies which have both stated that customer privacy security is important to them[289]—would be able to control the creation and distribution of the tool or software,

---

282 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 15.

283 *See* APPLE, IOS SECURITY, IOS 9.0 OR LATER, *supra* note 129, at 55; *Remotely Ring, Lock, or Erase a Lost Device*, GOOGLE, https://support.google.com/accounts/answer/6160500 [https://perma.cc/MCV3-ZLNX] (last visited Feb. 6, 2017).

284 Customer Letter, *supra* note 8.

285 *See, e.g.*, Brief for Amazon.com et al. as Amici Curiae, *supra* note 152, at 20; Customer Letter, *supra* note 8.

286 *See* Benner & Lichtblau, *supra* note 3.

287 *See* Perlroth & Benner, *supra* note 145.

288 *See supra* Part V.

289 *See* Brief for Amazon.com et al. as Amici Curiae, *supra* note 152, at 13–14; Customer Letter, *supra* note 8.

rather than have the government outsource decryption to an unknown, third-party hacker.

Endeavoring to create an entirely impenetrable smartphone is against Apple's and Google's business interests. Additional or enhanced security features often make the smartphone "slower" or "clunkier," while companies want to sell and market smartphones that are "sleek" and "intuitive."[290] Further, companies want to sell products to the public at-large and a security feature that frustrates consumers is unworkable.[291] Apple's and Google's full-disk encryption technology is thus more burden than benefit; it only provides, at best, minimal enhanced data protection at the expense of severely weakening Americans' safety from criminal enterprise.

Additionally, under this Note's proposed legislation, the affected companies themselves will ultimately decide whether or not to make smartphones amenable to search warrants.[292] The companies could choose not to reengineer their smartphones to make them amenable to governmental search warrants—completely negating any security or privacy concerns.[293]

B. The Burden Imposed on Technology Companies Would Be Minimal

Opponents contend that legislation requiring companies to make their smartphones amenable to search warrants would impose an undue burden.[294] Manufacturers and mobile operating system providers would have to expend resources reengineering their smartphones to allow for backdoor access as well as unlocking such phones in response to search warrants.[295] Yet, this argument, in part, presumes that tech companies are, and should be, free from any government-imposed burdens designed to advance societal interests. Countless industries in the United States have to expend resources to comply with laws and regulations issued to remedy a societal problem.[296] The tech industry should be no exception.

---

290 Apuzzo & Benner, *supra* note 15.

291 *See id.*

292 *See supra* Part V.

293 *See supra* Part V.

294 *See* Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 23–24; Brief for Amazon.com et al. as Amici Curiae, *supra* note 152, at 15–18.

295 *See* Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 13–14; Apuzzo & Benner, *supra* note 15.

296 *See* Mitchell Holt, *Five Areas of Government Regulation of Business*, HOUSTON CHRON.: SMALL BUS., http://smallbusiness.chron.com/five-areas-government-regulation-business-701.html

The real downfall of this argument is, however, that it completely ignores the possibility that legislation would contain a reimbursement provision. This Note proposes a reimbursement scheme that would compensate companies for the initial start-up costs of compliance and for costs associated with unlocking or extracting data from smartphones in response to a search warrant.[297] Although, admittedly, this proposal may not reimburse companies fully, as stated, companies are expected to bear reasonable costs of compliance with laws and regulations enacted for the public interest.[298]

Apple and Google regularly reengineer their mobile operating systems. Apple released iOS 9 on September 16, 2015.[299] In the six and a half months following its release, there were numerous updates (e.g., iOS 9.0.1, iOS 9.0.2, iOS 9.1, iOS 9.2, iOS 9.2.1, iOS 9.3, iOS 9.3.1).[300] Android released its newest operating system (Nougat 7.0) in October 2016, and its first major update in December of that same year.[301] The constant development of new and updated mobile operating systems belies the notion that this Note's proposal would be overly burdensome. The amendment would not be prompting entirely new development; it would simply be inserting a requirement into a process the companies already undertake.

Additionally, this Note's proposal is not forcing companies to invent novel technology. Apple and Google have the capability to either unlock or extract data from locked iPhones and Android-powered smartphones running "older" mobile operating systems.[302] Furthermore, the proposed amendment also does not require companies to

---

(last visited Feb. 6, 2017) (listing privacy and safety and health as two areas where the U.S. government has "many business regulations in place").

297 *See supra* Part V.

298 *See supra* Part V.

299 Press Release, *iOS 9 Available as a Free Update for iPhone, iPad & iPod Touch Users September 16*, APPLE (Sept. 9, 2015).

300 *See* Gordon Kelly, *Apple iOS 9.3.1: Should You Upgrade?*, FORBES (Apr. 1, 2016, 10:40 AM), http://www.forbes.com/sites/gordonkelly/2016/04/01/apple-ios-9-3-1-should-you-upgrade/#2bf38d51facf.

301 *See* Matt Swider & James Peckham, *Android Nougat Release Date: When You'll Get It and Everything You Need to Know*, TECHRADAR (Jan. 19, 2017), http://www.techradar.com/news/phone-and-communications/mobile-phones/android-7-what-we-want-to-see-1311290.

302 *See* Declan McCullagh, *How Apple and Google Help Police Bypass iPhone, Android Lock Screens*, CNET (Apr. 2, 2012, 5:19 PM), https://www.cnet.com/news/how-apple-and-google-help-police-bypass-iphone-android-lock-screens/ ("Apple has for at least three years helped police to bypass the lock code, typically four digits long, on iPhones seized during criminal investigations."); *Legal Process Guidelines*, *supra* note 47 (providing that Apple will no longer perform data extractions on devices running iOS 8.0 or later versions).

make any changes to their mobile operating systems.[303] They could elect to pay the civil penalty instead.[304]

C. *Individuals Living Under Authoritarian Governments Would Not Be Harmed*

Opponents argue that any effort to legislate a government backdoor into encrypted smartphones would create a precedent for authoritarian governments demanding similar access.[305] The argument continues that if an authoritarian 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."[306] These fears, however, are unfounded.

Again, as stated, mass surveillance by an authoritarian government would prove difficult—if not impossible—as the government must have the physical smartphone to access its contents.[307] Additionally, a foreign nation's government wanting information from an American company would have to go through lawful process in the U.S., either pursuant to a Mutual Legal Assistance Treaty ("MLAT") or a letter rogatory.[308] If the foreign government used the MLAT process, the executive branch of the federal government would decide whether, in its discretion, the foreign government's request was proper. If the foreign government used a letter rogatory, a federal court would make that determination. In either case, the request could be refused if the information was sought for use in a proceeding that would violate human rights.[309] "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.'"[310]

Additionally, Apple and Google could choose to not do business in, or only sell full-disk encrypted smartphones in, countries that have

---

303 *See supra* Part V.

304 *See supra* Part V.

305 S*ee, e.g.*, OLSEN ET AL., *supra* note 75, at 9; Bruce Schneier, *Security or Surveillance?*, BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. U. app. A.1–2 (2016); Apuzzo & Benner, *supra* note 15; Benner & Mozur, *supra* note 182.

306 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 18.

307 *See supra* notes 275–76 and accompanying text.

308 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 19.

309 *Id.*

310 *In re* 840 140th Ave. NE, 634 F.3d 557, 572 (9th Cir. 2011) (quoting *In re* Request for Judicial Assistance from Seoul Dist. Criminal Court, 555 F.2d 720, 724 (9th Cir. 1977)).

repressive governments and no laws banning such encryption technology.[311]

Conclusion

Investigating and prosecuting in the twenty-first century requires that the government have the tools necessary to crack cases. Without crucial evidence available only on the smartphone itself, cases could go unsolved. However, any legislative remedy to full-disk encryption must balance the interests of law enforcement, tech companies, and consumers. This Note's proposed amendment to the CALEA achieves such balance by subjecting the manufacturer and mobile operating system provider to a civil penalty for each instance that law enforcement cannot decrypt a smartphone it has the legal authority to search.

311 Manhattan Dist. Attorney's Office, *supra* note 71, at 18–19.

APPENDIX

TABLE. COMPARISON OF DATA SOURCES[312]

	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[313]	No	No	Perhaps(2)	Perhaps(4)
Historical other cell tower-related data[314]	Perhaps(5), (6)	No	Perhaps(7)	No
Historical Wi-Fi network data	Perhaps(6)	Yes	Perhaps(7)	No
Historical GPS or other satellite data[315]	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

312 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 7 (table and following information taken directly from report).

313 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.

314 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.

315 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.

(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. [In Apple's September 2014 Security Guide, the company states it "does not log messages or attachments [sent through iMessage], and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them."[316]]
(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. . . .
(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 than [sic] 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).

316 iOS Security Guide, *supra* note 107, at 23.