Journal of Civil Rights and Economic Development

Volume 32, Spring 2019, Issue 4 Article 2

Striking the Balance: Search Warrants and Encryption Protected Smartphones

Nicholas A. Oliva

STRIKING THE BALANCE: SEARCH WARRANTS AND ENCRYPTION PROTECTED SMARTPHONES

BY NICHOLAS A. OLIVA[1]

INTRODUCTION

Imagine that you are the parent of a dead 15-year-old girl whose life has just been cut short by a stray bullet. You have been up for days now, and you find yourself sitting in the hall of the New York County District Attorney's Office. The door of one of the assistant district attorney's offices opens, and you take a seat in front of her across from a large, mahogany desk.

The attorney tells you she has good news and bad news. The good news: a suspect is being questioned. The bad news: they have not been to access crucial information implicating the suspect in the shooting because the information is being stored on an iPhone 6s, and they could not bypass the privacy protection on the encrypted iPhone.[2] The only way to gain access to the phone is to get suspect to cooperate—but the truth is that simply will not happen. She informs you that without the information on the phone, the attorney will not have enough evidence to prosecute your daughter's murderer. This is exactly the balancing of rights the courts face when approaching smartphone searches: will the interest of the citizen, or of law enforcement prevail? Just as the hypothetical illustrates — "privacy comes at a cost."[3]

[1] J.D. Candidate, St. John's University School of Law, 2018.

[2] *See* Emma Raviv, *Homing in: Technology's Place in Fourth Amendment Jurisprudence,* 28 HARV. J.L. & TECH. 593, 612 (2015) (stating that encryption takes the text contained in the document, and converts it into ciphertext (encrypted text), which can only be converted into plaintext (readable text) with the correct encryption key); *see generally* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding warrantless wiretaps were constitutional because there was neither a physical invasion nor an official search and seizure of a person).

[3] Riley v. California, 573 U.S. 373, 401 (2014) (stating "[w]e cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell

We need not further hypothesize. Manhattan District Attorney Cyrus Vance recently reported that law enforcement was unable to execute search warrants on smartphones in over a hundred instances because the devices were running iOS 8[4] software that encrypts the cell phone's data.[5] More often than not, the information guarded by the smartphone's encryption software is not just useful, but it is often *crucial*.[6] Moreover, these cases do not just concern low-level crimes, but include homicides, attempted murders, sexual abuse of a child, sex trafficking, assault, and robbery.[7] The words of a family who had the life of a loved one stolen by a murderer put the stakes of this issue into perspective:

It hurts us every day to know that the identity of my sister's killer remains sitting inside a phone in an evidence room. As a family, we call on our elected leaders to pass comprehensive legislation to allow law enforcement access to valuable information. We ask this for victims' families like ours, who live in pain every day. We owe this fight to my sister and nephew, and for all of our nation's victims and their family members, as well.[8]

Shortly after Cyrus Vance released that report, the law enforcement crisis with encrypted smartphones made national

phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals.").

4 CYRUS VANCE, JR., REPORT OF MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY, at 1 (2015) (stating "[i]n September 2014, Apple Inc. announced that its new operating system, iOS 8, would be designed such that when a phone or other device running iOS 8 locks, no one but the user or another person with the device's passcode, could open it.").

5 *Id.* at 9.

6 *Id.* (emphasis added).

7 *Id.*

8 *District Attorney Vance, NYPD, Crime Victims' Advocates Call on Congress to #UnlockJustice*, MANHATTANDA.ORG (Apr. 18, 2016), https://www.manhattanda.org/district-attorney-vance-nypd-crime-victims-advocates-call-congress-unlockjustice/16/ (providing statements from Ernie Allen, Founding Chairman, former President, and CEO of the National Center for Missing & Exploited Children, who stated "We need to find the right balance," Joyful Heart Foundation Managing Director Sarah Haacke Byrd, who stated "Leaders, including policymakers, law enforcement, victim advocates, and survivors, must come together to work with technology companies to ensure that law enforcement has the necessary tools at its disposal to fully investigate crimes and to hold violent offenders accountable. Jointly we must examine how current encryption policies, while attempting to preserve privacy, may be diminishing the ability of law enforcement from doing all that they can to seek justice for victims of sexual assault, domestic violence and child abuse, and provide some level of closure for their families.").

headlines with the San Bernardino shooting. On December 2, 2015, Syed Rizwan Farook and his wife, Tashfeen Malik, killed 14 people and wounded another 24 people in an act of domestic terrorism.[9] A crucial piece of information was recovered—Farook's cellphone.[10] The subsequent investigation centered around the cell phone, because the hope was that the phone would provide evidence of the shooters' possible motives, co-conspirators or accomplices, as well as other crucial information that could explain their heinous act of violence.[11] Just as in the hypothetical case described above, law enforcement was unable to access the recovered cell phone because they did not have the necessary passwords, and the terrorists themselves had been shot and killed in a hail of bullets after fleeing the carnage they created.

At the core of the legal dispute between the FBI and Apple lies an issue that has been developing for over a decade with the development of password encryption: what are the consequences when the government's ability to search a private citizen's smartphone is compromised, and thus, there is less access to the extensive information stored on such devices?[12] What grabbed headlines was the fact that the FBI requested the Court to order Apple to "Assist Agents in Search."[13] Essentially, the FBI wanted Apple to provide three things: (1) access to the recovered iPhone by means of bypassing or disabling any function that could wipe out all the information on the phone; (2) unlimited chances to try to crack the iPhone's code by connecting it to a port, or using Bluetooth, Wi-Fi or any other means that would allow such a

9 Richard Pérez-Peña & Adam Goldman, *'It Finally Clicked That This Wasn't an Exercise': Report Recounts San Bernardino Shooting*, N.Y. TIMES (Sept. 9, 2016), http://www.nytimes.com/2016/09/10/us/it-finally-clicked-that-this-wasnt-an-exercise-report-recounts-san-bernardino-shooting.html?_r=0.

10 *Id.*

11 *See* In re Search of an Apple IPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at 1 (C.D. Cal. 2016).

12 *See* Apple Inc's Mot. to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opp'n to Government's Mot. to Compel Assistance, In re Search of an Apple Iphone Seized During the Execution of A Search Warrant on a Black Lexus Is300, California License Plate 35kgd203., 2016 WL 767457 (N.D. Cal. 2016).

13 *See* In re Search of an Apple IPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, *supra* note 11 at 1.

function; and (3) neutralization of function on iPhones that sets a time delay after a number of incorrect passcode attempts.[14]

Apple responded to this demand by recognizing two major considerations that are in tension with one another: the need for law enforcement to be armed with as much information as possible in order to be effective and the rights of private citizens to be secure in their possessions, namely their cell phones.[15] Apple saw this request as the FBI's attempt to compromise its product's security functions, which would allow a password to be input electronically to unlock that device.[16] If Apple was to enable the FBI to use "brute force"[17] tactics in order to unlock the iPhone, it would amount to the government simply "compel[ling] Apple to create a crippled and insecure product." [18] Moreover, Apple feared the promulgation of that product onto the market, because it anticipated it would create privacy concerns for millions of iPhone users who would be now vulnerable not just to government infringement of privacy, as well as "provide[] an avenue for criminals and foreign agents" to access such information.[19] Compliance with such an order would compromise the integrity of their product, and be outright unconstitutional.

This note addresses the various issues presented by the obstacles data encryption has created for law enforcement by placing in tension the American citizen's right to privacy through the use of data encryption, and law enforcement's ability to conduct lawful searches through the use of warrants. Essentially, my proposal sets out to do two things: (1) ensure the protections guaranteed by the Fourth Amendment to United States Citizens;

14 *Id.* The original language of the FBI's request of Apple to "Assist Agent in Search" stated:
(1) it will bypass or disable the auto-erase function whether or not it has been enabled; (2) it will enable the FBI to submit passcodes to the subject device for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol available on the subject device; and (3) it will ensure that when the FBI submits passcodes to the subject device, software running on the device will not purposefully introduce any additional delay between passcode attempts beyond what is incurred by the Apple hardware.

15 Apple Inc's Mot. To Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opp'n to Govt's Mot. To Compel Assistance, *supra* note 12 at 2.

16 *Id.* at 7.

17 *Id.* at 2 ("'[B]rute force' [operates by] trying thousands or millions of passcode combinations with the speed of a modern computer.").

18 *Id.*

19 *Id.*

and (2) give law enforcement a viable avenue to investigate crimes, while simultaneously providing Apple the security that the privacy of its customers will be as protected as it has ever been through carefully tailored legislation.

This note's analysis of searches of encrypted cell phone will be broken down into in three parts. Part I of this note provides context for the balance between individual privacy and law enforcement by reviewing general Fourth Amendment principles and then Supreme Court rulings that apply these principles to cell phones. Part II then details the advancements in cell phone technology, specifically encryption. These new technologies render the data on cell phones inaccessible and lead law enforcement to go beyond search warrants and seek special orders pursuant to the All Writs Act. Part II provides an overview of the All Writs Act and the leading cases that define its scope and concludes that the act does not provide a power to courts to order the decryption of cell phones. Part III then asserts why a judicial response is inadequate to address the issues caused by encryption, and why new legislation is needed that will effectively and lawfully strike the balance between the interests surrounding data encryption on smartphones.

I. THE EVOLUTION OF FOURTH AMENDMENT JURISPRUDENCE WITH THE INTRODUCTION OF SMARTPHONE TECHNOLOGY

A. Fourth Amendment Background

Every citizen of the United States has the right to be free from unreasonable government intrusion.[20] This right is derived from the Fourth Amendment that provides:

The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly

[20] U.S. CONST. AMEND. IV.

describing the place to be searched, and the persons or things to be seized.[21]

Essentially, the government is required to obtain a warrant from a judge and that warrant must be supported by probable cause prior to executing a search or seizure. Moreover, depending on the circumstances of the case, evidence obtained without satisfaction of the Fourth Amendment mandates will be excluded from court proceedings.[22]

In 1928, in *Olmstead* the Court ruled that the rights of a citizen against unreasonable searches and seizures were only violated when there was a physical intrusion into one's property.[23] Thus, it was held that a warrantless wiretap that was placed on the street outside the defendant's home, among other places did not violate the defendant's Fourth Amendment rights because the protections of the Fourth Amendment against unreasonable searches and seizures were not activated.[24]

Four decades later in *Katz*,[25] this Court further clarified when the protections of the Fourth Amendment apply. Once again, the Court wrestled with a wiretap device, but this time it was placed on the outside of a public telephone booth without a warrant and used to eavesdrop on a conversations made with the public telephone.[26] The government contended that because there was "no physical penetration," into the defendant's property, there was no intrusion that triggers the Fourth Amendment.[27] However, the Court agreed with the Petitioner's assertion that notwithstanding the absence of "'technical trespass,'"[28] the government violated the defendant's constitutional rights because "what he sought to

21 *Id.*

22 *See* Segura v. United States, 468 U.S. 796, 796–97, (1984) (quoting Nardone v. United States, 308 U.S. 338, 341 (1939), "The exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or "fruit of the poisonous tree.").

23 *See Raviv*, *supra* note 2 at 595; *see also,* Olmstead v. United States, 277 U.S. 438, 478 (1928).

24 *See Raviv*, *supra* note 2 at 595; *see also,* Olmstead v. United States, 277 U.S. at 478.

25 *See* Katz v. United States, 389 U.S. 347, 347 (1967).

26 *See id*. at 349.

27 *Id.* at 352.

28 *Id.* at 353 (holding that the Fourth Amendment protects not only the seizure of tangible items, but also extends to recordings of oral statements overheard as well, despite the absence of physical intrusion).

exclude . . . was not the intruding eye—it was the uninvited ear."[29] In so deciding, the Court explained that "[t]he Fourth amendment protects people—and not simply 'areas'—against unreasonable searches and seizures."[30] Thus, the Court departed from the narrowly construed principles of *Olmstead* in favor of a more contemporary view that derived from the evolution of the "vital role" the public telephone had come to play in communications.[31]

Therefore, Katz's Fourth Amendment protections were deemed to be activated because: "first[,] [he] exhibited an actual (subjective) expectation of privacy and, second, that the expectation [was] one that society [was] prepared to recognize as 'reasonable.'"[32] This framework has endured the test of time, and continues to inform the application of the Fourth Amendment, even with the continuing advancements in technology in the last few decades.

The Supreme Court of the United States has extended this line of reasoning to encompass the reasonable expectation of privacy that a citizen has in the contents of their cell phone.[33] In *Riley*, the Court held that in order to search an individual's cell phone incident to a lawful arrest, "[a] warrant is generally required."[34] This decision recognized that modern cell phones had an "immense storage capacity" greater than anything ever been encountered by the judiciary before, such as a cigarette pack, a wallet, or a purse.[35]

The *Riley* Court was extremely cognizant of the imminent expansion of the capacity of smartphones.[36] Because of this capacity, tension continues to grow between the private citizen trying to protect their information on smartphones, and law enforcement's interest of being able to access pertinent information relating to law enforcement investigations. While the

29 *Id.* at 352.

30 *Id.* at 353.

31 *See id.* at 352.

32 *Id.* at 361.

33 *See* United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (recognizing that "cell phones contain a wealth of private information," and, as a result, individuals have a "reasonable expectation of privacy" in them).

34 Riley v. California, 573 U.S. 373, 401 (2014).

35 *See id.* at 393.

36 *See id.* at 394 ("We expect that the gulf between physical predictability and digital capacity will only continue to widen in the future").

Riley Court ultimately deemed the contents of a smartphone subject to a reasonable expectation of privacy and a warrant requirement,[37] it fell short of giving the law enforcement guidance on how to approach the execution of warrants on encrypted cell phones.

Investigators soon realized that search warrants, even when granted, did not guarantee access. In the words of FBI director James Comey during his address of a Congressional Committee, "[u]ntil [smartphone encryption], there was no closet in America, no safe in America, no garage in America, no basement in America that could not be entered with a judge's order."[38] However, password encryption changed all that. Accordingly, Comey argued, we have come to a point where the individual privacy interests of a citizen to be secure in the contents of their phone by using data encryption, must give way to the interest of security when law enforcement obtains a valid search warrant to access that very same information.[39]

While a valid search warrant would legally permit the law enforcement to access information on a cell phone,[40] it does not provide physical access. For an encrypted cell phone, only the password will allow law enforcement to access the necessary information. Most of the time criminals do not willingly divulge their passwords; the next step after securing the proper Fourth Amendment search warrant then is judicially compelling the assistance of the producers of the encryption technology. A thorough understanding of how law enforcement traditionally obtained such assistance in similar, earlier circumstances is the logical starting point.

37 *Id.* at 386.

38 Nancy Dillon, *FBI May Have Different Way to Access San Bernardino Shooter's Phone, May Not Need Apple's Hack Help*, N.Y. DAILY NEWS, (Mar. 22, 2016, 8:27 AM), http://www.nydailynews.com/news/national/fbi-access-san-bernardino-shooter-phone-article-1.2572539.

39 *See The Encryption Tightrope: Balancing Americans' Security and Privacy, Hearing Before the Comm. on the Judiciary*, 114th Cong. 79 (2016) (statement of Hon. James B. Comey, Director, Federal Bureau of Investigation).

40 *See* U.S. CONST. amend. IV.

B. Examination of Government Interaction With Third Party Intermediaries, And the Changes Spurred By The Development Of Smartphone Technology

1. Compelling the Assistance of Third-Party Intermediaries

Traditionally, law enforcement was able to circumvent the efforts of targets that were trying to hide information crucial to investigations, because this information would necessarily pass through third-party intermediaries, such as telephone companies or banks.[41] In cases concerning third-party intermediaries, the subject's reasonable expectation of privacy was determined to be lost by virtue of their "voluntarily" turning over, or "knowingly expo[sing]" that information to a third party.[42] Accordingly, the Court has determined the search or seizure of that information would be lawful, as the user of the third-party intermediaries essentially assumed the risk that such data would, in one way or another, not be kept private.

New York Telephone Co. illustrates this concept.[43] There, the FBI suspected that a particular location in a Manhattan neighborhood was home to a gambling operation.[44] Under the authority of a federal statute known as the All Writs Act, the FBI subsequently motioned the United States District Court for the Southern District of New York to order the New York Telephone Company to install a pen register that would record the telephone numbers that were being called or received from that location.[45] The district court judge found there was probable cause to issue an All Writs order to compel New York Telephone to provide the necessary technical assistance required to install the pen

41 *See* Raviv, *supra* note 2, at 595.

42 *See* United States v. Miller, 425 U.S. 435, 442 (1976) (finding no expectation of privacy where documents voluntarily given to bank); *see also* In re U.S. for Historical Cell Site Data, 723 F.3d 600, 610 (5th Cir. 2013) (quoting Reporters Comm. for Freedom of Press v. Am. Tel. &
Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir.1978) "'To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections . . . .'").

43 *See* United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

44 *Id.* at 161-62.

45 *See id.* at 161, 163.

register.[46] New York Telephone complied, but subsequently appealed the order by arguing that the government did not have power to compel such assistance under the All Writs Act.[47]

Ultimately, the Court upheld the decision of the District Court in finding that that the All Writs Act empowered the Court to compel an order of assistance from the telephone company.[48] The Court laid out three elements that are necessary to determine if assistance is warranted: (1) whether the intermediary is too attenuated from the situation; (2) whether compelling assistance is unreasonably burdensome; and (3) whether assistance is necessary to effectuate the warrant.[49] In its analysis, the Court found that the order for assistance was closely related to the controversy as the company had direct control over the medium of communication.[50] Moreover, the court reasoned that the company was not burdened by providing such "meager assistance" to the FBI.[51] Finally, the court order was proven to be necessary because there was "no conceivable way" that the FBI would be able to execute this operation without the help of New York Telephone Co.[52] Accordingly, the Court's order was found to be constitutional, and the order to compel New York Telephone Co.'s assistance, proper. [53]

New York Telephone Co., stands for the broader proposition that law enforcement has always had a reliable way to physically access to even guarded information because of the power granted by the All Writs Act to compel the assistance of third party intermediaries.[54] However, with the introduction of data

46 *Id.* at 162. "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." *Id.* at 161 n.1 A pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached. United States v. Giordano, 416 U.S. 505, 549 n.1 (1974) (Powell, J., concurring in part and dissenting in part).

47 *See N.Y. Tel. Co.*, 434 U.S. at 162-63.

48 *See id.* at 172.

49 *See id.* at 160.

50 *See id.* at 174.

51 *See id.*

52 *See id.* at 175 (1977).

53 *See id.* at 177-78.

54 *See* United States v. Miller, 425 U.S. 435, 443 (1976); *see also* Smith v. Maryland, 442 U.S. 735, 744 (1979); *but see* U.S. v. Taketa, 923 F.2d 665, 676 (9th Cir. 1991) (holding

encryption, the strategy of simply subpoenaing information from third party intermediaries has become essentially obsolete, if not impossible.[55]

2. Default Encryption Has Made The Traditional Methods of Compelling the Assistance of Third Party Intermediaries Outdated

Smartphone encryption is a product of the advancements made by society in the realm of technology. For example, in 2011, smartphone ownership was a mere 35% amongst adults.[56] By 2015, that number had nearly doubled to 68%.[57] This huge growth of smartphone ownership was accompanied by the public's demand to have the strongest possible privacy and security protections.[58] Apple, for example, has been happy to provide just that. Apple has been at the forefront of protecting the privacy of its customers through the use of encryption, which is evident in their privacy policy published online that reads:

Encryption protects trillions of online transactions each day. When you're shopping, paying a bill, or using iMessage or FaceTime, you're using encryption. It turns your data into indecipherable text that can be read only by those with the right key . . . We also refuse to add a backdoor into any of our products.[59]

The use of cell phones has become extremely prevalent in society, so much so "that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy."[60] However, the same impetus for the creation of such

that an area readily open to the public does not create a right of access such that the person's expectation of privacy is automatically compromised).

55 *See* Raviv, *supra* note 2, at 612 ("Once encrypted, an Internet communication is practically impossible to decrypt by guessing—such a process would "occupy a supercomputer for millions of years").

56 *See* David M. Lenz, *Is the Cloud Finally Lifting? Planning for Digital Assets,* ALI CLE EST. PLAN. COURSE MATERIALS J. 35, 35 (Feb. 2017).

57 *Id.*

58 *See Brief of Amicus Curiae Act | the App Association in Support of Apple Inc.'s Motion to Vacate Order Compelling Assistance*, In re Search of an Apple IPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203., 2016 WL 1228636 (C.D. Cal. 2016).

59 *Apple's Privacy Policy*, APPLE, http://www.apple.com/privacy/approach-to-privacy/#safe-device (last visited Feb. 5, 2019).

60 Riley v. California, 573 U.S. 373, 385 (2014).

encryption has created an even greater concern for law enforcement.

Prominent political figures and heads of law enforcement have come forth to voice their concerns regarding the encryption of information contained on cell phones because of the formidable obstacle they present to criminal investigations and prosecutions. President Barrack Obama has addressed the issue of encryption by stating:

[I]f we get into a situation which the technologies do not allow us at all to track somebody we're confident is a terrorist … and despite knowing that information, despite having a phone number or social-media address or email address, that we can't penetrate that, that's a problem.[61]

The director of the FBI, James Comey, has also voiced concerns with regard to tech giants like Apple and Google on "going dark" which creates barriers for law enforcement to gather information to prevent the next terrorist attack.[62]At the State level, District Attorney Cyrus Vance has voiced similar concerns with regard to the cases that enter Manhattan courtrooms each and every day. Vance has stated that hundreds of criminal cases are harmed by encryption software that can be found on the phones of criminals.[63]

Prior to the advancements that software designers made in encryption, law enforcement agencies were able to engage in various methods to try to "crack" the encrypted devices.[64] One such method utilized by law enforcement is called a "brute force attack."[65] This method of code cracking involves a computer trying every key combination in an effort to find the correct password

61 Cody M. Poplin, *President Obama Comments on Back-doors in Encryption*, LAWFARE (Jan. 16, 2015, 5:50 PM), http://bit.ly/1nsk5P1 ("[The President] continued by not[ing] the difficult and sometime tenuous balance between security, liberty, and privacy, and stated that debate with civil libertarians and privacy groups had been "useful.").

62 *See* James Comey, Director, Fed. Bureau Investigations, *Going Dark: Are Technology Privacy, and Public Safety on a Collision Course?,* FBI (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

63 *See* Jamil N. Jaffer & Daniel J. Rosenthal*, Decrypting Our Security: A Bipartisan Argument For a Rational Solution to the Encryption Challenge*, 24 CATH. U. J. L. & TECH. 273, 292 (2016).

64 *See generally* J. Riley Atwood, *The Encryption Problem: Why the Courts and Technology are Creating a Mess For Law Enforcement*, 34 ST. LOUIS U. PUB. L. REV. 407, 411 (2015).

65 *See id.*

that will unlock the encryption.[66] However, the amount of time that this method takes can vary greatly depending on the complexity of the password, and can be anywhere from a few hours, to a few days, or even a few years, thereby causing the "brute force" method obsolete.[67]

With Apple's unwavering advocacy for the privacy rights of its customers, and law enforcement struggling to overcome encryption technology while also abiding by the Fourth Amendment in searches and seizures, former FBI director James Comey poses one simple question that puts the stakes of this issue into focus: "'it's only a matter of time before there's an incident where we say, "Who gave [Apple CEO] Tim Cook the right to decide whether a parent can find a lost child?"'"[68]

II. THE SAN BERNARDINO TERRORIST'S ENCRYPTED SMARTPHONE, AND LAW ENFORCEMENT'S INABILITY TO EXECUTE LAWFUL WARRANTS THEREON

A. The San Bernardino Attack

The intersection between an individual's right to privacy and the need for law enforcement to access encrypted data caught the national spotlight on December 2, 2015,[69] at approximately 11:00 a.m., when a group of co-workers gathered for training at the Inland Regional Center ("IRC"), in San Bernardino, California.[70] Suddenly, a door swung open, and a single masked person wearing all black, and carrying a firearm stepped inside the room.[71] Without a word, he began opening fire.[72] Pandemonium ensued. Pandemonium ensued. A second shooter joined the attack, and

66 *Id.*

67 *Id.*

68 Jaffer & Rosenthal, *supra* note 63, at 293.

69 *See* RICK BRAZIEL, ET. AL., A CRITICAL INCIDENT REVIEW OF THE SAN BERNARDINO PUBLIC SAFETY RESPONSE TO DECEMBER 2, 2016, TERRORIST SHOOTING INCIDENT AT THE INLAND REGIONAL CENTER, 25 (2016). ("The IRC is a frequent training location for county departments because of the conference room's large size and its close proximity to the county office building").

70 *Id.*

71 *Id.* at 26.

72 *Id.*

together they fired over 100 rounds.[73] The attackers then fled in a black SUV, leaving behind death and destruction.[74]

A short time later, officers spotted the same SUV miles away in a neighboring town. A sergeant, as well as undercover police officers that also happened to be in the area, attempted to execute a traffic stop on the SUV.[75] The SUV refused to pull over. After making a turn, the back window of the SUV shattered from within, as gunfire erupted from the vehicle. The gunfire was aimed at the officers trailing close behind.[76] An intense firefight ensued, with the shooters firing 81 rounds at police, and at least 440 shots being returned by police.[77] Both shooters were killed.

Afterwards, police proceeded to process the crime scene and discovered an encrypted iPhone in the shooter's car. Because both perpetrators were killed in the shootout, there was no way to access its contents.[78] The FBI, worried about more attacks, "…promised to explore every investigative avenue in order to learn whether the San Bernardino suspects were working with others, were targeting others, or whether or not they were supported by others."[79] Officials applied for numerous search warrants[80] to search the digital devices and online accounts of Syed Rizwan

73 *Id.*

74 *Id.* at 27.

75 *Id.* at 38.

76 *Id.*

77 *Id.* at 40.

78 Joel Rubin, et al., *FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now*, L.A. TIMES (Mar. 28, 2016, 10:39 PM), http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.

79 *Id.*

80 Richard Winton, *A year after the San Bernardino terror attack, the FBI is still struggling to answer key questions*, L.A. TIMES (Dec. 1, 2016, 2:25 PM), https://www.latimes.com/local/lanow/la-me-san-bernardino-terror-probe-20161130-story.html. Although Farook's phone was owned by his employer, the San Bernardino County Department of Public Health, and despite the employer's consent to execute a search of the phone, officials were unable to bypass the phone's encryption software. The FBI has been unable to make attempts to determine the passcode because Apple has written, or "coded," its operating systems with a user-enabled "auto-erase function" that would, if enabled, result in the permanent destruction of the required encryption key material after 10 erroneous attempts at the passcode (meaning that after 10 failed attempts at inputting the passcode, the information on the device becomes permanently inaccessible). When an Apple iPhone is locked, it is not apparent from the outside whether or not that auto-erase function is enabled; therefore, trying repeated passcodes risks permanently denying all access to the contents. *See* Rubin et al., *supra* note 78.

Farook ("Farook"), and his wife, Tashfeen Malik ("Malik").[81] Thus, the FBI turned to the All Writs Act, and the precedents of *New York Telephone Co.,* and its progeny. These efforts to access the iPhone only bolstered Apple's privacy and business concerns — "th[at] [Apple] must contend with constant attempts by outside parties to worm past [their] security measures."[82]

B. The Order to Compel Apple's Assistance in Accessing the Encrypted iPhone

In order to Compel Apple's assistance, the government relied on the All Writs Act. To understand the framework in which the Government and Apple were arguing, a brief overview and history of the All Writs Act, are necessary at this point.

American courts have long had broad statutory authority to "carry out their duties of an independent judiciary by issuing the orders necessary to do so—even if Congress did not have the foresight to" explicitly proscribe the necessary procedural mechanisms that would effectuate those orders.[83] The All Writs Act was initially enacted by the First Congress in 1789, and provided:

That all the before-mentioned courts of the United States, shall have power to issue writs of *scire facias*, *habeus corpus*, and all other writs not specifically provided for by statute, which may be necessary for the exercise of their respective jurisdictions, and agreeable to the principles and usages of law.[84]

The Act has only been amended twice in the succeeding centuries, but only in form, never in substance.[85] When the Act has been amended, the statute's text was simply modernized. Today, the Act provides "[t]he 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

81 *See* Rubin et al., *supra* note 78.

82 *Id.*

83 In re Apple, Inc., 149 F. Supp. 3d 341, 350 (E.D.N.Y. 2016); Adams v. United States ex rel. McCann, 317 U.S. 269, 273 (1942) (stating "Unless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it.").

84 Judiciary Act of 1789, 1 Stat. 73, § 14 (1789).

85 *See id.*; 28 U.S.C. § 1651(a) (2018).

to the usages and principles of law.[86] The statute confers on all federal courts the authority to issue orders where three requirements are satisfied:

(1) The issuance of the write must be "in aid of" the issuing court's jurisdiction;

(2) The type of writ requested must be "necessary or appropriate" to provide such aid to the issuing jurisdiction; and

(3) The issuance of the write must be "agreeable to the usages and principles of law.[87]

It is important to note that some courts have not reached the *New York Telephone Co.* factors because they conclude that the Government's request to compel assistance does not fall within the reach of the All Writs Act itself.[88] However, in the San Bernardino action, the Government relied heavily on earlier applications of The All Writs Act and analogized facts in those cases, particularly *New York Telephone Co.*, to the facts of their investigation and insisted that their request fell within the statute's authority.[89] Apple disagreed, and in motion practice both sides focused on the three *New York Telephone Co.* factors necessary to allow lawful use of the All Writs Act.[90]

1. Analysis of the Remoteness Factor of *New York Telephone Co.*

The first factor asks whether Apple was "so far removed from the underlying controversy that its assistance could not be permissibly compelled."[91] The core of this issue rests on whether the mere fact that Apple designed, manufactured, and sold the

86 28 U.S.C. § 1651(a).

87 *Id.*

88 *See In re Apple, Inc.*, 149 F. Supp. 3d at 353-54 (holding that an order to compel assistance of the development of software to bypass iPhone encryption fell outside the power of the All Writs Act because "Congress has considered but declined to adopt [such broad power]—albeit without explicitly or implicitly prohibiting it—[and therefore] is not agreeable to the usages and principles of law").

89 Gov't Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search at 6-8, *In re Apple, Inc.,* 149 F. Supp. 3d 341, 353-54 (2016) (No. 15-0451M), 2016 WL 680288, at *1.

90 *Id.*; Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 58, at 15, 20-21, 27, 29.

91 U.S. v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977).

device in question is enough on its own to establish that its connection to the investigation is not too attenuated.[92]

The Government asserted that Apple's development of the device and subsequent placement of it into the stream of commerce was sufficient to establish the first factor of *New York Telephone Co.*[93] The Government reasoned that since Apple wrote and manufactured the software that runs the phone—the same software preventing execution of the warrant—Apple has become uniquely able to modify and control restrictions on the iPhone that were hindering law enforcement's ability to obtain critical information.[94] Accordingly, the Government concluded that since Apple owns the very software that now must be used to enable the search ordered by the warrant, Apple is not too "far removed" from the situation and should be compelled to assist the government.[95]

Conversely, Apple argued that its relationship to the San Bernardino attack is far too attenuated to satisfy the first prong of *New York Telephone Co*.[96] Essential to its argument is the premise that "[t]he All Writs Act does not allow the government to compel a manufacturer's assistance merely because it has placed a good into the stream of commerce."[97] Apple asserted that the All Writs Act, if used in such a way, would "eviscerate the 'remoteness' factor entirely" by allowing any company, no matter how attenuated its connection to criminal activity, to be held accountable and subject to compulsion to assist law enforcement.[98] Accordingly, Apple found that it is too "far removed" and attenuated to compel its assistance.[99]

The first issue to be considered is whether Apple's relationship was sufficiently close to the attack that spurred the conflict between Government and Apple. In *New York Telephone Co.,* the Supreme Court found the remoteness factor to be satisfied where the telephone company's property was "being used to facilitate a

92 *See* Gov't *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search, *supra* note 89, at 6.

93 *See id.*

94 *Id.*

95 *Id.* at 7.

96 Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 12, at 20-21.

97 *Id.* at 16.

98 *Id.*

99 *Id.* at 15.

criminal enterprise on a continuing basis."[100] Ownership of the device used to commit a crime is direct involvement. Unlike *New York Telephone Co.* where the intermediary owned the facility that was being utilized for criminal communications, here, Apple has no ownership interest whatsoever in the phone that was used in the San Bernardino attack.[101]

Even if one was to assume that Apple's financial benefit from the product as a result of the sale of the phone to the consumer establishes some type of involvement, the sale profits alone should not be sufficient to satisfy the first prong of analysis. The fact of the matter is, by the time the consumers were planning and executing the attack, Apple had no direct involvement. Moreover, Apple did not do anything to directly oppose the Government's investigation of the matter; instead it simply decided to take no action.[102] As a result, *New York Telephone Co.,*. would not find that Apple would be so closely related to the underlying crime to make compelling assistance under the All Writs Act appropriate.

2. *Analysis of Whether Compelling Assistance would be Unreasonably Burdensome*

The parties then turned to the second issue, namely, whether compelling assistance is unreasonably burdensome on Apple. The Government argued that compelling Apple to assist in this situation would not require "inordinate effort, and [the Government would even offer] reasonable reimbursement" for its efforts.[103] The Government further emphasized that Apple, in its ordinary course of business, would sometimes be required to write such code in response to subpoenas or other processes.[104] Given

100 U.S. v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977).

101 *See id.*; Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 12, at 15.

102 *See N.Y. Tel. Co.,* 434 U.S. at 174; *In re Apple, Inc.*, 149 F. Supp. 3d 341, 366 (E.D.N.Y. 2016).

("Apple has not conspired with Feng to make the data on his device inaccessible. More importantly, perhaps, it has not even done what the telephone company did in *N.Y. Tel. Co.*—namely, it has not barred the door to its property to prevent law enforcement agents from entering and performing actions they were otherwise competent to undertake in executing the warrant for themselves.").

103 Gov'ts *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search, *supra* note 89, at 7.

104 *See id.*

this fact, the Government argued that Apple could not possibly assert that the order could be overly burdensome.[105] Additionally, Apple's unique ability to develop such a software code would allow it to constrain any software developed for this instance to be "tailored for this particular phone," thus presenting no danger of system malfunctions or disrupting business operations stemming from privacy concerns.[106]

Apple asserted that the FBI's order to compel assistance in this situation would be repugnant to Apple's strong interest in maintaining the level of security that is associated with the brand-value of its product.[107] Essentially, this would impose a crippling burden on the business by destroying the data technology that Apple has spent years developing.[108] As a practical matter, compliance with such an order would require Apple to write a new, previously non-existent code, which would demand engineers to design, create, test, and validate the compromised operating system.[109] After that software was developed, Apple would then have to supervise the operation by the FBI to brute force crack the phone's security.[110] Such processes would also need to be logged and recorded in case Apple's methodology is ever scrutinized.[111] Apple explained how this process of bypassing the passcode security of just one iPhone "diverts man hours and hardware and software from Apple's normal business operations."[112] Apple also expressed its fear that if it was to comply with an order requiring Apple to develop previously non-existent software, it would set dangerous precedent that would require similarly situated technology companies to "do the government's bidding in untold future criminal investigations" that would require the development of new "hacking" departments devoted solely for government purposes. [113]

105 *See id*.

106 *Id*.

107 Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov'ts Motion to Compel Assistance, *supra* note 12, at 16-17.

108 *Id*.

109 *Id*. at 1, 2.

110 *See id*.

111 *Id*.

112 In re Apple, Inc., 149 F. Supp. 3d 341, 370 (E.D.N.Y. 2016).

113 Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 12, at 18.

In considering whether compelling Apple's assistance would be unreasonably burdensome, the crucial consideration is whether the nature of the assistance required is within the day to day operations of Apple's business. Whereas the Court in *New York Telephone Co*., had found that the utilization of a pen register was not offensive to the business operations of the company because it regularly employed pen registers for the use of billing operations, detecting fraud, and preventing violations of law, the measures to break through its encryption technology is not part of the day-to-day business operations of Apple.[114] Moreover, implementation of such measures can substantially threaten Apple's brand which is built on its highly effective security capabilities.

Additionally, meeting the Government's demands would burden Apple, not just with the responsibility of development of completely new software, but also, there would also be a displacement of labor hours that would be required to carry out the necessary development.[115] As such, the Government's contentions that Apple regularly develops software code is not comparable to the type of extensive decryption software that the Government is seeking here. Accordingly, compelling Apple's assistance is also unreasonably burdensome.

3. *Is Compelling Assistance Necessary to Effectuate the Warrant?*

Lastly, the Government asserted that Apple's assistance is necessary to effectuate the search warrant on the subject device. In this case, the iPhone was suspected to have records of who was communicating with Farook up to and during the attacks in San Bernardino. These communications were determined to be critical to law enforcement's investigations, and inaccessible by any other means known to the government or Apple.[116] Consequently, the Government asserted that Apple was the only entity that had the ability to assist the government in unlocking the iPhone, and ensuring the safety of the information contained therein. [117]

114 U.S. v. N.Y. Tel. Co., 434 U.S. 159, 174-75 (1977).

115 *In re Apple, Inc.,* 149 F. Supp. 3d at 370.

116 Gov'ts *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search, *supra* note 58, at 8.

117 *See id.* at 4.

On the other hand, Apple focused on distinguishing the circumstances at issue with those of *New York Telephone Co.* In *New York Telephone Co.*, Apple argued that "there [was] no other conceivable way to effectuate the government's objective." [118] However, in the case at hand, Apple asserted that the Government failed to show that it even sought out or received any technical assistance from alternate avenues with expertise in digital forensics. Consequently, Apple argued failure to obviate the need to compel Apple's assistance should foreclose the endeavor it pursues now.[119] In so concluding, Apple demanded the District Court to view this issue as one in which required the Court to "to preserve certain rights at the expense of burdening law enforcement's interest in investigating crimes and bringing criminals to justice."[120]

Moreover, Apple was opposed to idly accepting any argument that would have far-reaching policy consequences by stretching the All Writs Act for purposes more extensive than it was intended to address.[121] While Apple recognized that the All Writs Act confers the courts the power to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law," here, Apple concluded that the Act simply became the "'issu[uance] [of] ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate'"—which is expressly forbidden by the Act itself.[122] If the courts were allowed to do so, Apple argued, the Government would essentially "short-circuit[] public debate on this controversy, [which is] seem[ingly] fundamentally inconsistent with the proposition that such important policy issues should be determined in the first instance by the legislative branch after public debate—as opposed to having them decided by the judiciary in sealed, *ex parte* proceedings."[123]

118 Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov'ts Motion to Compel Assistance, *supra* note 12, at 15.

119 *See id.* at 19-20.

120 *Id.* at 22.

121 *See id.* at 3.

122 Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov'ts Motion to Compel Assistance, *supra* note 12, at 15.

123 *Id.* at 19.

Consequently, while it is clear that Apple likely has significant ability to develop the necessary software to decrypt smartphones, there is nothing in the record that suggested the Government has sought alternative avenues of relief aside from the All Writs Act. Without such options having been explored, the Government could hardly argue that Apple's assistance is necessary.

III. DEVISING LEGISLATION TO ENSURE THE EXECUTION OF LAWFUL WARRANTS ON SMARTPHONES

Ultimately, Apple was right, and its assistance was not necessary in the FBI investigation. Instead, the FBI's motion to compel Apple to lend its assistance in gaining access to the iPhone belonging to Farook was vacated because law enforcement was able to unlock the encryption software by utilizing third party resources.[124] However, the issue of using the All Writs Act to compel companies to break their own encryption software is still unresolved in the courts. Since October 8, 2015, the Government has submitted requests in nine other matters in the federal courts—in California alone—to compel Apple to bypass the passcode security of numerous devices.[125] There is no easy legal resolution, and the issue is unlikely to be resolved through the All Writs Act. Instead, this Note proposes that the legislature would be best suited to shoulder the load of these weighty issues that have the potential of having widespread social repercussions by approving new legal innovations.

[124] Danny Yadron, *FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone*, GUARDIAN, (Apr. 28, 2016, 7:32 AM), https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino. FBI director James Comey had stated the cost of unlocking the encryption software cost more than what he would be paid during the rest of his tenure—upwards of a million dollars. *Id.*

[125] In re Apple, Inc., 149 F. Supp. 3d 341, 349 (E.D.N.Y. 2016).

A. Existing Laws Are Ill-Equipped To Balance The Security Interests of Law Enforcement and Privacy Interests Of Citizens

Never before has the Court encountered a device with such capacity for "storing and accessing a quantity of information, some highly personal, that no person would ever had on his person in hard-copy form."[126] Even if the judiciary attempted to answer this complex legal issue, the resolution would not achieve a satisfying outcome because a judicial resolution is limited to existing laws. A court can only "mechanically apply . . . rule[s] used in the pre-digital era to a search of a cell phone."[127]

Justice Alito, concurring with the majority's opinion in *Riley*, voiced his opinion on the issue of whether the judiciary was attempting to stretch its powers too far when he asserted that "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."[128] Similarly, a judge presiding over a substantially similar issue regarding the United States' government's motion to compel assistance in the Eastern District of New York, ended his opinion by urging Congress and others in the legislative branch of government to take action in order to force this debate out of the courts, and force the "debate . . . [to] happen today . . . among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive."[129] Thus, a "new balancing of law enforcement and privacy interest" is called for in order to address this issue.[130] The weight of this issue should fall squarely on the shoulders of the"[l]egislatures, elected by the people, [who] are in a better position than [the judiciary is] to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."[131] Even Apple recognized the amicability of such a solution and advocated for a legislative solution in its own brief opposing a motion to

126 Riley v. Cal., 573 U.S. 373, 406-07 (2014) (Alito, J., concurring).
127 *Id.* (Alito, J., concurring).
128 *Id.* at 408 (Alito, J. concurring).
129 *In re Apple, Inc.*, 149 F. Supp. 3d at 376.
130 *Riley v. Cal.*, 573 U.S. at 407 (Alito, J., concurring).
131 *Id.* at 408.

compel assistance that was submitted to the Court by the FBI.[132] There, Apple asserted that instead of the government seeking to compel the creation of a compromised operating system, the FBI would be better served by the "pursu[it] [of] new legislation," which it had not even attempted,[133] rather than "back[ing] away from Congress and turning to the courts."[134] Courts and prominent law enforcement officials have suggested several approaches to analyzing how law enforcement may execute a lawfully obtained search warrant to obtain information thereon.[135] The best course of action would be a bipartisan and cooperatively adapted legislation made by law enforcement and tech giants such as Apple and Google. Such legislation must tend to the concerns of all interested parties—including the consumer—and dispel fears that it would undermine the privacy afforded by smartphone technology.[136] The components of this proposal move to simply "restore the *status quo* before Apple's IOS 8." [137]

A successful solution requires a combination of two key components: (1) cryptographic envelope security and (2) high civil

[132] Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 12, at 2.

[133] James B. Comey, FEDERAL BUREAU OF INVESTIGATION STATEMENT BEFORE THE SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS: *Threats to the Homeland*, (Oct. 8, 2015), https://www.fbi.gov/news/testimony/threats-to-the-homeland (explaining that "[t]he United States government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. However, the administration is not seeking legislation at this time."); Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 12, at 2.

[134] Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 12, at 2.

[135] *See* Compliance with Court Orders Act, S._, 114th Cong., 2d Sess. (2016) (discussion draft available at https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf); Digital Security Commission Act, H.R. 4615, 114th Cong., 2d Sess. (2016) (text available at https://www.govtrack.us/congress/bills/114/hr4651/text/ih). Two pieces of federal legislation have been proposed, but they have not gained traction sufficient to be passed and affect meaningful change. The first bill was made in direct response to the San Bernardino terrorist attack and is named the "Compliance with Court Orders Act of 2016." *See* Compliance with Court Orders Act. The second piece of federal legislation, dubbed the "Digital Security Commission Act," was fashioned in such a way to establish a "National Commission on Security and Technology" challenges in the legislative branch to examine "the intersection of security and digital security and communication technology in a systemic, holistic way." *See* Digital Security Commission Act.

[136] *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ (asserting that "[o]nce created, the . . . [equivalent of a master key] could be used over and over again, on any number of devices").

[137] *See* VANCE, JR., *supra* note 4, at 15.

penalties to be imposed on the consumers of encrypted smartphone technology. Each of these components will be examined in turn in a legislative solution below.

B. A Legislative Solution Would Strike The Balance Between The Competing Interests of Security And Privacy

A legislative solution does not alter all the present Fourth Amendment requirements for ascertaining a warrant—the most important of which requires it to "particularly describe[e] the . . . things to be seized."[138] This particularity requirement creates a safeguard that prevents law enforcement from mistakenly searching a place other than what the magistrate authorized. It minimizes the risk that officers executing search warrants will by mistake search a place other than the place intended by the magistrate.[139] Implicit in these traditional requirements is the answer to Apple's core concern, the center of which suspects the unbridled ability of law enforcement to gain access into iPhones that would open the floodgates, and compromise the privacy of millions. These same rules lend their unwavering stability to the present-day searches justified by a valid search warrant on cell phones or other smart devices and does not change after the implementation of this legislation.

Although Apple has voiced concern about overbroad authority of law enforcement, there is no evidence that the ability of law enforcement to execute *lawful* search warrants would be detrimental in any way. Numerous forensic experts and technologists have concluded that the privacy concern voiced by Apple is unfounded[140] because such software is useless without physical possession of the device that an individual seeks to decrypt.[141] Therefore, naturally, such an option should be explored if it would render answers to these complex legal issues that, so far, have found no solution.

138 U.S. CONST. AMEND. IV.
139 2 Wayne R. LaFave, *Search & Seizure* § 4.5, 5th ed. (2004).
140 *See* Cook, *supra* note 136.
141 *See* Vance, Jr., *supra* note 137, at 15.

1. Cryptographic Envelope Security Would Sufficiently Guard The Privacy Concerns That Encryption Was Meant To Address

The most prominent concern for Tim Cook is the possibility that Apple can be compelled to produce a master key that would fall into the wrong hands, creating the ability for *anyone* to be able to unlock *any* Apple device.[142] This important concern can be met by restrictive control of the process of access, even once the master key is built through a multi-layered system for accessing encrypted private information.

In addition to the Fourth Amendment, additional methods can be used to balance the rights of a citizen with the necessity of law enforcement to be able to access information with execution of a valid warrant.[143] The "cryptographic envelope" method is an integral part of striking the appropriate balance that will address this issue.[144] This method creates "key[s]" that could decrypt data in a series of "nested" envelopes, similar to the concept of "Russian dolls," with one envelope being outside of the next and only accessible through the use of a specific "key" in the possession of independent key-holders. Essentially, such a method would work like this:

Suppose, for example, we put the filesystem key in an envelope sealed with the FBI's public key, and then put that sealed envelope

142 *See* Cook, *supra* note 136.

143 *See* Compliance with Court Orders Act, S._, 114th Cong., 2d Sess. (2016); Digital Security Commission Act, H.R. 4615, 114th Cong., 2d Sess. (2016). *See also* Neema Singh Guliani, *4 Problems with Creating a Commission on Encryption,* ACLU. ORG (Mar. 9, 2016, 4:00 PM), https://www.aclu.org/blog/privacy-technology/internet-privacy/4-problems-creating-commission-encryption; Mark Jaycox, *EFF Opposes McCaul-Warner Encryption Comm'n,* ELEC. FRONTIER FOUND. (Mar. 7, 2016), https://www.eff.org/deeplinks/2016/03/eff-opposes-mccaul-warner-encryption-commission. The second piece of federal legislation, dubbed the "Digital Security Commission Act," was fashioned in such a way to establish a "National Commission on Security and Technology challenges in the legislative branch to examine "the intersection of security and digital security and communication technology in a systemic, holistic way." *See* Digital Security Commission Act. Essentially, this legislation was aimed only at examining the issues we already know to exist by appointing various individuals to man each position of the board who were knowledgeable in various fields relevant to the issue of search and seizure of data encryption. *See id.* After further examination of the issue, the Commission would prepare several reports that would be used for tackling the issue in the future. *See id.* While the Act garnered bipartisan support from both the Senate and the House, there has been sharp criticism asserting that the commission's mission was "overly broad." *Id.* Moreover, the Commission would simply "prolong the encryption conversation," in a time where the American people need answers.

144 *See* VANCE, JR., *supra* note 4, at 16.

inside another envelope, this time sealed with the manufacturer's public key . . . To start with, the drive can no longer be decrypted unilaterally by the FBI. The FBI doesn't have the manufacturer's private key, it can't open the outer envelope. The drive also can't be unilaterally decrypted by the manufacturer. Although the manufacturer can open the outer envelope, only the FBI can open the inner one to retrieve the filesystem key. Decryption of the drive (at least, without knowledge of the user's password) now cryptographically requires both organizations to work with each other—all but eliminating the possibility of criminal misuse by insiders, or institutional misuse. [145]

The "cryptographic envelope" method would ensure that consumer's privacy would be thoroughly protected.

Another simpler way of thinking about this cryptographic envelope method is to analogize to a safety box at a bank. A safety lock box requires two keys to be accessed: one belonging to the owner of the contents of the box and the other belonging to the bank where the box is stored and protected. The two key system means that the owner of the box is required to go to the bank and ask for access to their lock box. When the person's credentials are verified, the employee of the bank will bring them to their lock box and insert their key. At that time, the owner of the contents of the lock box will insert their own key, and with both keys in place, the box is unlocked.

The safeguards afforded by the cryptographic method balance the right of citizens to be secure in their private information stored on cell phones and the need for law enforcement's ability to appropriately, and with only with the requisite authorization, access information that is suspected to be used in furtherance of criminal investigations.[146]

145 *See* Matt Tait, *An Approach to Jim Comey's Technical Challenge,* LAWFARE INST. (Apr. 27, 2016, 7:00 AM), https://www.lawfareblog.com/approach-james-comeys-technical-challenge.

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

2. Civil Sanctions Are Also Necessary To Incentivize Companies to Comply With Law Enforcement

Indeed, "privacy comes at a cost," but the burden of such cost should be borne by those best situated to carry the weight.[147] The burden falls rightfully on the shoulders of those manufacturing the products that dangerously hinder the ability of law enforcement to investigate and prosecute criminal activities. Accordingly, an obligation to build a bypass for encryption for all devices along with civil sanctions for the failure to meet the obligation would be another integral part of the proposed legislation. Essentially, this "would be no different conceptually than legislation that requires products to be safe, buildings to be constructed with exits and egresses that satisfy specific requirements, and roads to have maximum speed limits."[148] In fact, various states and agencies have proposed the use of civil sanctions in helping to find a solution to the production of encrypted technology.[149] New York State, in particular, has seen some serious consideration.

All of the district attorneys in New York have proposed a specific provision that would mandate that "[a]ny smartphone that is manufactured on or after . . . [a certain date], and sold or leased in New York, shall be capable of being decrypted and unlocked by its manufacturer or its operating system provider."[150] New York Assembly Bill A.8093A proposed an amendment to the New York General Business Laws to require that any seller or lessor of a "smartphone . . . that is not capable of being decrypted and unlocked *by its* manufacturer or its operating system provider . . . [be] subject . . . to a civil penalty of . . . [$2,500 per] smartphone . . . if it . . . [can be] demonstrated that the seller or lessor . . . knew at the time of the sale or lease that the smartphone was not capable of being decrypted and unlocked . . . ."[151] Violations of this law would be enforced either by the district attorney of the county in which the sale or lease occurred or by the state Attorney

147 Riley v. Cal., 573 U.S. 373, 401 (2014).

148 SMARTPHONE ENCRYPTION & PUBLIC SAFETY, *supra* note 4, at 15.

149 *See id.* at 24-26 (describing proposals from several states). *See, e.g.* Assemb. A.8093A, 2015 Leg., Reg. Sess. (N.Y. 2015); Assemb. 1681, 2016 Leg., Reg. Sess. (Cal. 2016); H.R. 1040, 2016 Leg., Reg. Sess. (La. 2016).

150 VANCE, JR., *supra* note 4, at Appendix I.

151 N.Y. Assemb. A.8093A.

General.[152] Essentially, this would cause the profit from producing and selling iPhones with default encryption to be dwarfed by the penalty that would need to be paid for violation of the encryption provisions.

California Assembly Bill 1681 is, for all intents and purposes, the same as New York Assembly Bill A.8093A,[153] but it was amended to prohibit any manufacturer or operating system provider who pays the civil penalty from passing on any portion of it to smartphone purchasers, so that companies cannot shift the financial burdens to the consumers.[154] Essentially, the California bill would give law enforcement the authority to penalize the manufacturers, like Apple and Google, who are directly responsible for marketing a product with default-encryption.[155]

One important distinguishing feature of the California bill from its New York counterpart is the fact that the California bill would only impose a penalty for each instance in which a smartphone could not be decrypted pursuant to a court order decreasing the number of situations where the civil penalty would be imposed.[156] As a result, the financial burden that would be borne by the manufacturer would be as small or severe as the number of instances where the government required assistance to enter into the phone's encryption.[157]

The imposition of civil sanctions would incentivize tech companies to manufacture products that may be decrypted by simply changing their cost-benefit analyses. Whereas it is still profitable to manufacture and sell encrypted devices, by imposing a civil sanction, the production of the same phone may result in a loss of profit. The new proposal would lead to a situation where the manufacturer would be incentivized to cooperate in the balance between the interests of private citizens and law enforcement.

The adoption of the aforementioned safeguards would restrict the scope of law enforcement's ability to access private information and incentivize companies, like Apple and Google, to manufacture

152 *Id.*
153 *See id.*; Cal. Assemb. 1681.
154 Cal. Assemb. 1681.
155 *See id.*
156 *See id.*
157 *See id.*

products that would promise both the privacy and security of their customers. The adoption of legislation with these components serves the interests of all parties, which would enable companies, like Apple and Google, to find solace in the fact that society has asserted its will by a fair congressional vote.[158]

CONCLUSION

Law enforcement and companies, like Apple, must take the lead on this issue that touches the lives of just about every single American citizen. While there are competing interests on both sides, those interests do not have to be dichotomous. While it is clear that there is no way to find a solution where one side will not have to compromise or to create a system without unintentional vulnerabilities,[159] in the end, the effort set forth will aid in upholding the rights and freedoms that our government has protected for centuries.

While criminal or even national security interests are not enough, on their own, to justify the judicial orders originally sought by law enforcement, the Framers of the Constitution envisioned a legislative means of confronting this issue. These highly divisive issues must be tried in the appropriate arena—Congress—and not left to the judiciary to "fill in gaps in the law" by forcing such political discussion to be decided by the Court.[160] Legislation tapping into cryptographic envelope technology would account for all of the aforementioned competing interests and would strike the necessary balance between the citizen's right to

158 *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 58, at 3 ("If this order is permitted to stand, it will only be a matter of days before some other prosecutor, in some other important case, before some other judge, seeks a similar order using this case as precedent. Once the floodgates open, they cannot be closed, and the device security that Apple has worked so tirelessly to achieve will be unwound without so much as a congressional vote.").

159 Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security*, WASH. POST (Apr. 10, 2015), https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html?tid=a_inl.

160 Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Gov't's Motion to Compel Assistance, *supra* note 58, at 14.

privacy and law enforcement's duty to provide security to its citizens.