# CALLING A TRUCE TO THE CRYPTO WARS: WHY CONGRESS AND TECH COMPANIES MUST WORK TOGETHER TO INTRODUCE NEW SOLUTIONS AND LEGISLATION TO REGULATE ENCRYPTION

*Liz Kaminski*[*]

## I. INTRODUCTION

On December 2, 2015 at 10:59 A.M., Syed Rizwan Farook and his wife, Tashfeen Malik, entered a conference room at the Inland Regional Center in San Bernardino, California and opened fire.[1] By the end of the attack, Farook and his wife murdered fourteen people and left twenty-two people seriously injured.[2] Both attackers died during a gunfight with authorities after being pursued for the brutal assault.[3] Then considered "the third deadliest attack on U.S. soil since Sept. 11, 2001," law enforcement, unsurprisingly, began an immediate investigation into the mass shooting.[4]

During the course of the investigation, law enforcement recovered three cellphones used by the assailants.[5] Only one cellphone remained intact, an Apple iPhone 5C provided to Farook from his employer, the San Bernardino County Department of Health.[6] Apple's encryption technology, however,

* J.D. Candidate, 2018, Seton Hall University School of Law; B.A., St. Thomas Aquinas College. I would like to thank my adviser to this comment Professor David Opderbeck, and the entire *Seton Hall Law Review* editorial team for their feedback and comments.

[1] Sari Horwitz & Joel Achenbach, *Report Offers New Details on San Bernardino Terrorist Attack*, WASH. POST (Sept. 9, 2016), https://www.washingtonpost.com/world/national-security/report-offers-new-details-on-san-bernardino-terrorist-attack/2016/09/09/599ea266-76be-11e6-b786-19d0cb1ed06c_story.html.

[2] *Id.*

[3] *Id.*

[4] *Id.* Unfortunately, terrorism and mass shootings have continued since the writing of this article. Therefore, the ranking of the San Bernardino shooting may not be accurate considering recent events. *See, e.g.*, Geoffrey Mohan, *The Trigonometry of Terror: Why the Las Vegas Shooting Was so Deadly*, L.A. TIMES (Oct. 4, 2017), http://www.latimes.com/nation/la-las-vegas-shooting-live-updates-the-trigonometry-of-terror-why-the-las-1507085772-htmlstory.html.

[5] *Apple-FBI Battle over San Bernardino Terror Attack Investigation: All the Details*, L.A. TIMES (Feb. 19, 2016), http://www.latimes.com/business/technology/la-fi-tn-apple-fbi-20160219-htmlstory.html.

[6] *Id.*

protected the information contained in the iPhone.[7] Unable to circumvent the security measures protecting Farook's iPhone, the Federal Bureau of Investigations (FBI) turned to Apple for assistance in unlocking the phone.[8] After about a month of meetings, discussions between Apple and the FBI broke down.[9] Once talks between the two parties collapsed, Magistrate Judge Sheri Pym of the District of Central California ordered Apple to assist the FBI in unlocking the phone on February 16, 2016.[10] Judge Pym issued the order pursuant to the All Writs Act (AWA).[11] This Act allows federal courts to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[12] Specifically, the order detailed that Apple should provide the FBI with "reasonable technical assistance" to bypass Farook's encrypted iPhone.[13]

Apple issued a letter in response to Judge Pym's order that very same day.[14] Apple openly opposed the order claiming that forced compliance would set a "dangerous precedent" for data security.[15] Referring to "technical assistance," Apple stated, "[b]uilding a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control."[16]

---

[7] Raoul Rañoa & Paresh Dave, *How the iPhone's Security Measures Work*, L.A. TIMES (Feb. 24, 2016, 1:40 PM), http://www.latimes.com/business/la-g-how-the-iphone-s-security-measures-work-20160219-htmlstory.html.

[8] 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?_r=1.

[9] *Id.*

[10] 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.

[11] 28 U.S.C. § 1651(a) (2012).

[12] *See In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016).

[13] The Central District of California ordered Apple's reasonable technical assistance in three respects: (1) bypassing the auto-erase function on the iPhone; (2) enabling the FBI to submit passcodes to the iPhone; and (3) ensuring that the FBI would not be delayed by any wait times between submitting passcodes. *In re* An Apple iPhone, 2016 U.S. Dist. LEXIS 20543, at *2–3.

[14] *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ (last visited Jan. 13, 2017).

[15] *Id.*

[16] *Id.*

Apple's opposition reignited a debate within the United States regarding encryption.[17] On the one hand, law enforcement faces increasing investigative challenges due to sophisticated encryption protections. On the other, private tech companies feel a responsibility to their users to provide security in addition to privacy. This innate conflict between law enforcement's ability to investigate and tech companies' promises of user privacy has led to a standoff between law enforcement and private tech companies.

This Comment will discuss the renewed "crypto war"—the debate surrounding technology companies' role in aiding law enforcement to obtain information from encrypted devices.[18] Part II will begin by exploring the recent legal battles between Apple and the FBI as a case study of this conflict between private, third-party companies that produce encryption and United States law enforcement. Part III will then discuss the background of cryptology (or cryptography) and the controversy that has continuously surrounded private use of cryptology within the United States. Next, Part IV will consider the current legislation relied upon by tech companies and the government, and will analyze its applicability to today's encryption technology. Part V will then propose a possible solution—a commission comprised of tech industry specialists, law enforcement, and other government officials. Further, this Comment will present Israel as a case study that the United States could possibly use as a model for encryption regulations. Finally, this Comment concludes that a compromise between law enforcement and private tech companies must be fostered in order to end the "crypto wars" and create new legislation to regulate encryption.

## II. APPLE VS. FBI: LEGAL BATTLES OVER COMPELLING PRIVATE, THIRD PARTIES TO DECRYPT PRIVATE DEVICES

The recent legal battles between the FBI and Apple demonstrate the struggles that the courts face in balancing law enforcement's need for information and the private tech industry's need for ever-increasing encryption security for individuals. For instance, Apple's refusal to comply with Judge Pym's order to unlock Farook's iPhone made news headlines

[17] For an introductory discussion of the United States's earlier "crypto wars," see Andrea Peterson, *The 'Crypto Wars' of the 1990s Are Brewing Again in Washington*, WASH. POST (Sept. 10, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/10/the-crypto-wars-of-the-1990s-are-brewing-again-in-washington/.

[18] The Fifth Amendment controversy surrounding law enforcement compelling individual defendants to provide their password to decrypt protected information is beyond the scope of this Comment. For a discussion involving the Fifth Amendment implications in requiring defendants to provide their passwords for decryption, see, J. Riley Atwood, Comment, *The Encryption Problem: Why the Courts and Technology Are Creating a Mess for Law Enforcement*, 34 ST. LOUIS U. PUB. L. REV. 407 (2015).

during February 2016.[19] Apple insisted that the court-compelled technical assistance would create a "backdoor" in all Apple devices running similar software.[20] To comply with Judge Pym's order, Apple needed to create and install new "bad" code on Farook's iPhone to override the phone's current "good" code.[21] The "good" code improves security measures on the device while the "bad" code diminishes or creates vulnerabilities in the security measures on a device.[22] By updating the iPhone's operating system with "bad" code, the current security system[23] would become vulnerable, allowing the FBI to successfully retrieve information from Farook's encrypted iPhone.[24] Under this premise, Apple appealed Judge Pym's order compelling technical assistance on the high-profile Farook matter.[25]

Another Apple legal battle also grabbed headlines during winter 2016.[26] On February 29, 2016, Judge Orenstein in the Eastern District of New York ruled against the government's motion to force Apple to extract information from a drug dealer's encrypted iPhone 5S, protected with a passcode.[27] Judge Orenstein, who issued the ruling *In re Order Requiring Apple, Inc. to Assist*, agreed with Apple's argument that the AWA improperly applied to

---

[19] *See, e.g.*, *Apple-FBI Battle over San Bernardino Terror Attack Investigation: All the Details*, *supra* note 5.

[20] *See A Message to Our Customers*, *supra* note 14. Although Apple referred to the San Bernardino technical assistance order as forcing the company to create a "backdoor," this in a technical sense is not correct. A technical backdoor is when a manufacturer pre-equips software or hardware with code that allows the manufacturer to access the information from the device without the user's permission. *See* Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What it Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599, 609–10 (2016).

[21] *See* Pell, *supra* note 20, at 613.

[22] *Id.*

[23] Apple's passcode feature provides iPhone users with the ability to protect information using 256-bit encryption. *See* Rañoa & Dave, *supra* note 7. This encryption method produces trillions of possible patterns. *Id.* Further, Apple provides users with a choice to completely erase information found on the iPhone after several failed attempts to unlock the passcode. *Id.*

[24] iPhones have the inability to distinguish between "good code" and "bad code." *See* Pell, *supra* note 20, at 613.

[25] Jonathan Chew, *This Is Apple's Next Move in its Fight with the FBI*, FORTUNE (Mar. 2, 2016, 10:53 AM), http://fortune.com/2016/03/02/apple-appeal-fbi-iphone/.

[26] *See, e.g.*, Sarah Jeong, *Judge James Orenstein Has Something to Say About the US Government's Decryption of iPhones*, VICE: NEWS (Mar. 1, 2016, 3:30 PM), https://news.vice.com/article/judge-james-orenstein-has-something-to-say-about-the-us-governments-decryption-of-iphones.

[27] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 354–55 (E.D.N.Y. 2016) [hereinafter, *N.Y. Apple iPhone Case*]. Katie Benner & Joseph Goldstein, *Apple Wins Ruling in New York iPhone Hacking Order*, N.Y. TIMES (Feb. 29, 2016), http://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html?_r=1. As of July 2016, the DOJ is appealing Judge Orenstein's decision. *DOJ Continues Appeal for iPhone Data Case in New York*, FORTUNE (Apr. 8, 2016), EBSCOhost (last visited Sept. 16, 2016).

compelling a private tech company in assisting law enforcement.[28] Apple, therefore, could not be compelled under this Act to provide technical assistance in unlocking the device.[29] This decision marked a major divergence from earlier decisions because no other court had ruled in favor of Apple over law enforcement's use of the AWA.[30]

The facts in both the San Bernardino case and the New York case bore two major similarities. First, the New York case, like the San Bernardino case, involved an encrypted iPhone.[31] Second, the government in both cases used the AWA as its legal basis for compelling Apple to unlock the iPhone.[32] This made *In re Order Requiring Apple, Inc. to Assist* a foremost victory for Apple, and made the FBI's argument to compel Apple to unlock Farook's iPhone under the AWA vulnerable to attack on appeal.[33]

Apple, however, did not get the opportunity to attack the validity of the FBI's use of the AWA regarding Farook's iPhone. Ultimately, the FBI withdrew its motion to compel Apple's technical assistance on March 28, 2016.[34] Instead, the FBI figured out a way to circumvent the encryption protecting Farook's iPhone with the help of anonymous third-party hackers and no longer needed Apple's assistance.[35]

The FBI revealed little information regarding the flaws in the iOS 9 software's security measures to Apple or the public.[36] The hack used for the San Bernardino matter only unlocked iPhone 5Cs running the iOS 9.[37]

---

[28] *See* Benner & Goldstein, *supra* note 27; *see also infra* Part IV.B and accompanying text.

[29] *See* Benner & Goldstein, *supra* note 27; *see also infra* Part IV.B and accompanying text.

[30] Previously, at least seventy orders compelling Apple to unlock phones had been issued. *See* Benner, *supra* note 27.

[31] Sarah Jeong, *The Convoluted Logic Behind Apple's 'Obstruction' of Law Enforcement*, VICE: MOTHERBOARD (Mar. 8, 2016, 6:00 AM), http://motherboard.vice.com/en_au/read/doj-seeks-to-overturn-new-york-iphone-case.

[32] *Id.*

[33] *Id.*

[34] Kate Sheehy, *FBI Breaks into San Bernardino Gunman's iPhone, Ending Court Case*, N.Y. POST (Mar. 28, 2016), http://nypost.com/2016/03/28/fbi-breaks-into-san-bernardino-gunmans-iphone-ending-court-case/.

[35] *Id.*

[36] In January 2017, the FBI released heavily redacted documents in response to a lawsuit from USA TODAY and two other news organizations seeking information about the FBI's ability to circumvent Farook's iPhone security measures. *See* Elizabeth Weise, *FBI Blacks out Most Details on Hack of Terrorist's iPhone*, USA TODAY (Jan. 7, 2017 10:48 A.M.), http://www.usatoday.com/story/tech/news/2017/01/07/fbi-iphone-terrorist-san-bernardino-syed-rizwan-farook-foia-lawsuit-ap-vice-usa-today/96280458/. These documents showed little besides boilerplate language. *Id.* The documents did not reveal how much the FBI paid outside sources to hack into the iPhone or the sources. *Id.*

[37] Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (Apr. 12, 2016), https://www.washingtonpost.com/world/

Nonetheless, some critics and Apple itself claimed that the FBI should release the information regarding the vulnerability so the security issue can be fixed.[38] In April of 2016, the FBI maintained that it needed the vulnerability in the software for a few more months before it would publicly disclose the system's issues.[39]

While the San Bernardino battle may be over, the war over encryption between tech companies and law enforcement persists. In Fall 2017, Apple introduced the iPhone 8 and iPhone X equipped with iOS 11, which is expected to make seizing data from an iPhone far more difficult.[40] Encrypted data on Apple devices will, therefore, continue to cause difficulties for law enforcement.[41]

As encryption technology advances to protect users' privacy, law enforcement continues to struggle with obtaining encrypted information and courts continue to grapple with outdated legislation. Congress must create new laws to provide law enforcement with the ability to obtain encrypted information to strike the balance between two competing ideas of security: (1) the security that strong encryption affords to private individuals, the government, and industries such as the financial or healthcare sectors, and (2) the security of the United States against threats such as terrorist attacks and criminal enterprises.

## III. CRYPTOLOGY AND ITS DEVELOPMENT WITHIN THE UNITED STATES

### A. *Primer on Cryptology*

While encryption and decryption methods have drastically changed over time, the idea behind cryptography[42] remains substantially the same.[43] In the classic example, Alice wants to send Bob a message that only Bob can

national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.ebd9df8ccee8.

[38] *Id.*

[39] *Id.*

[40] Andy Greenberg, *Apple's iOS 11 Will Make it Even Harder for Cops to Extract Your Data*, WIRED (Sept. 11, 2017), https://www.wired.com/story/apples-ios-11-will-make-it-even-harder-for-cops-to-extract-your-data/. Even Siri now comes equipped with end-to-end encryption. *iOS 11*, APPLE.COM, https://www.apple.com/ios/ios-11/.

[41] *See* Greenberg, *supra* note 40.

[42] Throughout this Comment, the words "cryptography" and "cryptology" are used interchangeably.

[43] This idea of using a "secret language" can be traced back to the Roman Empire. BERT-JAAP KOOPS, THE CRYPTO CONTROVERSY: A KEY CONFLICT IN THE INFORMATION SOCIETY 34 (1999). By using a substitution method, Julius Caesar allegedly used a Caesar cipher, which used a key of three—meaning that to encrypt a message one would use the letter that occurs three letters after the actual letter (A would be D). *Id.*

read.[44] Alice, the sender, transforms her message into a different, secret language that turns the message into jumble so that any interceptors are unable to read the message—this is encryption.[45] When Bob receives Alice's message, he uses his cipher or key to translate the jumbled message back into an understandable one—this is decryption.[46]

While cryptography was originally done by hand, by World War I machines were being used to encrypt and decrypt messages using the "substitution method" of encryption.[47] During World War II, cryptography became extremely important for the military.[48] For instance, United States cryptologists managed to build a replica of the Japanese cryptograph machine and used it to break the Japanese's coded messages throughout the war.[49] After World War II, the military and United States intelligence agencies continued to research cryptography.[50] The United States established the secret National Security Agency a.k.a. "No Such Agency" (NSA),[51] which concentrated on developing cryptography.[52] The NSA primarily focused on two areas of research: (1) creating encryption codes that could not be broken to maintain the security of government information and (2) gathering and decoding foreign intelligence.[53] By the 1970s, however, researchers outside the NSA were making headway in the field of cryptology and were using computers to encrypt and decrypt data.[54] IBM introduced a "symmetric system" for encryption that allowed encryption and decryption to use the same key.[55]

Encryption methods have continued to develop and uses have expanded into the private sector, like Apple's encryption technology. Apple uses a

---

[44] *See* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT–SAVING PRIVACY IN THE DIGITAL AGE 5–6 (2001).

[45] *Id.*

[46] *Id.*

[47] The machines developed would automatically *substitute* letters for numbers and symbols and be able to transpose encrypted messages. *See* Koops, *supra* note 43, at 34.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] The NSA was created in 1952 under President Truman with the purpose of gathering intelligence and securing government information. *See* LEVY, *supra* note 44, at 13–14. The agency was known for being very secretive and rarely discussed research publicly, so by the early 1970s, some who were in the know would refer to the agency as "No Such Agency." *Id.*

[52] *See* Koops, *supra* note 43, at 35.

[53] The NSA organized itself into two major divisions. *See* LEVY, *supra* note 44, at 14. Communication Security, or COMSEC, created encryption codes while Communications Intelligence, or COMINT, intercepted foreign electronic information and decoded that information. *Id.*

[54] *See* Koops, *supra* note 43, at 35–36.

[55] *Id.* at 35–36, 42–43.

"bit" encryption method for its devices.[56] For instance, the security measures installed on Farook's iPhone used a 256-bit encryption method.[57] This method substitutes data on the iPhone and stores the data as a series of "o's" and "1's".[58] The smartphone then uses a unique number 256 bits long as the key to encrypt the data.[59] The more bits there are, the more possible keys there are to unlock the phone so a 256-bit encryption provides for trillions of patterns that could be the key to decrypting the data.[60] Apple does not keep a copy of the "key" for each iPhone, and without this key, not even Apple can unscramble the data.[61]

By setting a passcode on the iPhone, the iPhone's data can only be decrypted and accessed by entering the passcode.[62] The passcode has additional security features that force a wait time after several failed attempts at opening the iPhone and provides users with the ability to permanently delete information after ten failed passcode attempts.[63] These security measures prevented the FBI from using a "brute force attack" to unlock Farook's iPhone.[64] A brute force attack on encrypted data occurs when a program runs every possible combination for the key until it finds the combination used to decrypt the data.[65] Since the FBI could not use a brute force program, the key to an iPhone would likely not be ascertained unless some other security measure in the iPhone was exploited.[66]

### B. *The "Original" Crypto Wars*

Long before Apple's 256-bit encryption method, United States law enforcement had concerns about encryption technology and its ability to retrieve encrypted information.[67] During the 1990s, two major encryption issues developed in the United States.[68] Concerned with national security, law enforcement pursued regulations regarding: (1) the exportation of encryption products and (2) the ability to aid law enforcement in recovering

---

[56] *See* Rañoa, *supra* note 7.
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *See* Rañoa, *supra* note 7.
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *See id.*
[67] Jack Karsten & Darrell M. West, *A Brief History of U.S. Encryption Policy*, BROOKINGS (Apr. 19, 2016), https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/.
[68] *Id.*

encrypted information.[69]

With the rise of the Internet, the United States felt as if it had to control encryption technology exports to keep them out of the hands of possible foreign enemies.[70] Through legislation already in place,[71] Clinton's Administration classified encryption products under the Commerce Control List giving the United States Department of Commerce's Bureau of Export Control the ability to regulate encryption exports.[72] Today, the Department of Commerce continues to regulate encryption; however, the Bureau of Industry and Security (BIS) now oversees export controls.[73] As domestic regulations regarding encryption products do not exist within the United States, the BIS remains mainly responsible for regulating encryption products exported on an international level.[74] For instance, the encryption regulations prohibit exporting encryption products to terrorist-supporting countries.[75]

While the United States has international export regulations, regulating encryption within the United States has presented unique difficulties. Law enforcement agencies wanted to establish legal procedures to receive third-party assistance in decrypting information.[76] In the early 1990s, law enforcement approached this issue by introducing the concept of a "key escrow."[77] The NSA initially proposed that tech companies voluntarily install a "Clipper chip" into the technological network for phones.[78] The installed chip would encrypt data installed on the phones for its users and would make a copy of the user's key.[79] The two parts of the "key" would then be held in an "escrow" by two agencies, the National Institute of Standards and Technology and the Treasury Department's Automated Systems Division, until law enforcement obtained a valid court order to

---

69 *Id.*

70 *Id.*

71 For example see, the International Emergency Economic Power Act, 50 U.S.C. § 1701 (2012), the National Emergencies Act, 50 U.S.C. § 1601 (2012), and the Export Administration Act, 50 U.S.C. § 2410 (2012). MARTIN CHARLES GOLUMBIC, FIGHTING TERROR ONLINE: THE CONVERGENCE OF SECURITY, TECHNOLOGY, AND THE LAW 80–81, n.67 (2008).

72 GOLUMBIC, *supra* note 71, at 81.

73 *Policy Guidance*, BUREAU OF INDUS. & SECURITY, https://www.bis.doc.gov/index.php/policy-guidance/. (last visited Nov. 2, 2017).

74 GOLUMBIC, *supra* note 71, at 81–82.

75 *See* 15 C.F.R. § 740 Supp. 1 (2016). Currently, there are four countries the United States deemed terrorist-supporting countries: Iran, North Korea, Sudan, and Syria. *See* 15 C.F.R. § 740 Supp. 1 (2016).

76 *See generally*, Karsten & West, *supra* note 67.

77 *Id.*

78 *See id.; see also* KOOPS, *supra* note 43, at 109.

79 *See* KOOPS, *supra* note 43, at 109.

acquire the information contained on the encrypted phone.[80] After obtaining the court order to acquire the information, the key's two parts would be released to law enforcement.[81]

In 1993, President Clinton introduced the "Clipper chip" concept to the public through the voluntary Escrowed Encryption Standard (EES).[82] The EES faced heavy criticism from privacy advocates who believed a key escrow would ultimately become a mandatory control, meaning that the voluntary installation would one day become a mandatory installation.[83] Further, technologists believed that a key escrow would create vulnerabilities in encryption security that hackers could exploit.[84] By 1997, the NSA abandoned pursuing the EES system.[85]

Congress, however, continued to attempt to address law enforcement's concerns over obtaining encrypted information. Both the Senate and the House drafted competing bills that dealt with regulating encryption domestically in the 1990s—many included some type of key escrow or key recovery policy.[86] Although discussed and drafted, Congress never adopted the various proposals due to the key escrow policies that many bills contained.[87] The hesitation to adopt a full-blown key escrow derived from the fact that these systems create major security risks for encryption.[88] In addition, the inherent complexity and astronomical costs of building a key escrow system made employing the escrow system difficult.[89]

---

80 *Id.*

81 *Id.*

82 *Id.*

83 *Id.* Documents showed that federal agencies contemplated that there would be a point that a voluntary system would not be viable, and a mandatory policy would need to be implicated. *Id.*

84 *See generally* Peterson, *supra* note 17 ("[I]f the government has a secret backdoor into a technical system, what's to stop a malicious hacker from finding it?"). For a discussion of the vulnerabilities found within the EES, see Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard,* CRYPTO.COM, http://www.crypto.com/papers/eesproto.pdf. (last visited Jan. 13, 2017).

85 *See* KOOPS, *supra* note 43, at 109.

86 *See id.* at 111–12. The bills included: the Secure Public Networks Act introduced by Senators Kerrey, McCain, and Hollings, which promoted the use of a key escrow policy that law enforcement would have the ability to access; the Security and Freedom through Encryption Act (SAFE) introduced in the House by Representative Goodlatte, and later amended by the House Permanent Select Committee on Intelligence to include a key escrow policy (a competing version of this bill, amended by the House Commerce Committee, mandated that the government may not impose a key escrow policy; however, these two conflicting versions of the bill made it "unfit for voting."); and the E-Privacy Act that would create a National Electronic Technologies (NET) Center to assist law enforcement. *Id.*

87 *See id.*

88 Peter Swire, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 436 (2012).

89 *Id.* at 437.

The United States examined alternative encryption control methods to a key escrow such as installing encryption products with technical "backdoors" or, rather, pre-installed software that allows the manufacturer to access encrypted information without the user's permission.[90] Yet, backdoors also faced criticism because the encryption producers have no way to ensure that only "good guys"—law enforcement enforcing a search warrant—maintain an exclusive entrance.[91] "Bad guys," including hackers intending to steal information, could exploit the intentional vulnerability.[92] After the mounting disapproval over domestic encryption regulations to aid law enforcement, the United States government abandoned the endeavor.[93] Consequently, an open question remains regarding encryption producers' role in aiding law enforcement within the United States.

### C. *"Going Dark": Challenges Faced by Today's Law Enforcement*

While law enforcement had no legal means tailored to compel assistance from encryption producers, other agencies within the United States' government continued programs aimed at weakening strong encryption products such as the NSA.[94] When Edward Snowden, a former NSA contractor, defected in 2013, he revealed to the world documents that showed the NSA conducted a secret program called "Bullrun" to decrypt data within the United States.[95] Until Snowden revealed this information, the NSA kept its capabilities to decrypt digital information a closely guarded secret.[96]

Once the secret leaked that the NSA had decryption spying capabilities in 2013, tech companies like Apple started pushing the bounds of encryption by pre-installing its products with "end-to-end encryption."[97] End-to-end encryption gives only the sender and recipient the key to unlock the data

---

[90] Parker Higgins, *On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures*, ELEC. FRONTIER FOUND. (Apr. 16, 2015, 1:07 PM), https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures; *see also* Pell, *supra* note 20.

[91] Swire, *supra* note 88, at 433.

[92] *Id.*

[93] *See* Higgins, *supra* note 90.

[94] Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=2&_r=3.

[95] *Id.* A key feature of the Bullrun program was that Internet companies voluntarily cooperated with the NSA. *Id.* For instance, the NSA uses the Sigint Enabling Project to incentivize tech companies to "covertly influence and/or overtly leverage" designs to make them "exploitable" and had spent more than $250 million a year on the program. *Id.* The NSA had capabilities including having an American manufacturer actually install a backdoor onto a computer being shipped to a foreign intelligence target. *Id.*

[96] *Id.*

[97] *See* Peterson, *supra* note 17.

making it highly secure.[98] In its approach to privacy statement, Apple emphasized that end-to-end encryption does not allow the company to decrypt a user's message when in transit between devices.[99] Apple has also stated that regarding "all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key."[100] Since end-to-end encryption has been introduced, law enforcement has become increasingly nervous that this encryption technology will shelter criminals and terrorists, thus putting the United States's public safety and national security at risk.[101]

Stronger end-to-end encryption products mean challenges for law enforcement; however, advances in this type of encryption technology also have many benefits.[102] Strong encryption benefits every private individual—not just criminals or terrorists—as encryption is used to protect financial information, healthcare information, government information, military data, and data from intelligence agencies.[103] For instance, with more than fifty-one percent of United States adults using online banking today,[104] powerful encryption helps protect this sensitive information from being hacked or stolen.[105] Without powerful encryption, many online banking or financial transfers might be vulnerable to fraudulent transactions or cyber-attacks.[106]

While the public reaps benefits from encryption, strong encryption hinders law enforcement investigations, and even prosecuting criminal behavior. When bad actors, such as terrorists, use encryption to hide activities and conceal evidence of criminal activity, a "digital crime scene"

---

98 *Id.*

99 *Our Approach to Privacy*, APPLE, http://www.apple.com/privacy/approach-to-privacy/ (last visited Nov. 2, 2017).

100 LEGAL PROCESS GUIDELINES, APPLE 10 (June 23, 2017), https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

101 *See* HOUSE HOMELAND SEC. COMM. MAJORITY STAFF REP., GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE 10 (2016), https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf [hereinafter HOMELAND SEC. REP.].

102 A dual use product, such as encryption, can be used for both military and peaceful, civil purposes. *See* KOOPS, *supra* note 43, at 98.

103 *See* HOMELAND SEC. REP., *supra* note 101 at 7.

104 *Id.* at 8.

105 *Id.* at 8–9.

106 *Id.* For example, seven Iranian hackers were indicted in March 2016 for systematically attacking targets including Bank of America, the New York Stock Exchange, Capital One and ING, and PNC Bank, which "stopped hundreds of thousands of customers from accessing their accounts and cost the businesses millions of dollars as they raced to protect their servers." Tom Winters & Tracy Connor, *Iranians Charged with Cyber Attacks on U.S. Banks, Dam*, NBC NEWS (Mar. 24, 2016, 10:56 AM), http://www.nbcnews.com/news/us-news/iranians-charged-hacking-attacks-u-s-banks-dam-n544801.

is created, but is unreachable by law enforcement investigators and prosecutors.[107] For example, the Office of the District Attorney for New York County cited 175 cases between September 2014 and March 2016 in which the office struggled to obtain evidence because the investigators could not access digital information from encrypted devices.[108] Law enforcement agencies like the FBI cannot access the "digital crime scene" so they face "going dark."[109]

Former FBI Director James Comey described "going dark" as the "phenomenon in which law enforcement personnel have the 'legal authority to intercept and access communication and information pursuant to court order,' but 'lack the technical ability to do so.'"[110] Director Comey also understands the competing interests at stake:

> We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public. One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds reason to believe that certain private communications contain evidence of a crime, then the government can conduct a limited search for that evidence. For example, by having a neutral arbiter—the judge—evaluate whether the government's evidence satisfies the appropriate standard, we have been able to protect the public and safeguard citizens' constitutional rights. . . . We would like to emphasize that the Going Dark problem is, at base, one of technological choices and capability.[111]

Comey insists that law enforcement is not looking to expand surveillance capabilities.[112] Law enforcement merely wants the opportunity to obtain encrypted information for investigations pursuant to a legal authority.[113]

Others in law enforcement have acknowledged similar "going dark" problems with obtaining encrypted information. Former New York Police Department ("NYPD") Police Commissioner Bill Bratton found that Apple's refusal to unlock Farook's iPhone was a display of "corporate irresponsibility."[114] During a press conference with Bratton, Manhattan's

---

107 *See* HOMELAND SEC. REP., *supra* note 101, at 10.

108 *Id*.

109 *See infra* note 110 and accompanying text.

110 HOMELAND SEC. REP., *supra* note 101, at 5 (quoting former FBI Director James Comey).

111 *The Encryption Tightrope: Balancing Americans' Security and Privacy Before H. Comm. on the Judiciary*, 114th Cong. 11–12 (2016) (statement of James B. Comey, Director, Federal Bureau of Investigations).

112 *Id.* at 12.

113 *Id.*

114 Graham Rayman & Leonard Greene, *NYPD Commissioner Bill Bratton, Manhattan*

District Attorney, Cyrus Vance, displayed numerous inaccessible, encrypted iPhones on a table to reporters and expressed frustration over the dilemma by stating, "[i]t's very difficult to explain to a victim of crime that we can''t get evidence because of cellphone technology."[115] NYPD Deputy Commissioner, John Miller, agreed, stating, "now totally encrypted devices like the Apple iPhone, cannot be penetrated even with a search warrant from a judge."[116] Similarly, Los Angeles County Sheriff's Captain Chris Cahhal asserted that an encrypted iPhone makes a "nice paperweight," because the department has no way to access the information encrypted on those devices.[117] Hillar C. Moore, III, the District Attorney for East Baton Rouge, acknowledges that not all encrypted phone data may lead to an arrest or prosecution; however, he believes that law enforcement should have the capability to look for clues.[118] These statements demonstrate that both federal law enforcement, like the FBI, and local law enforcement are facing a massive "going dark" problem.

Despite this "going dark" problem, Apple continues to resist assisting law enforcement. Apple requires the government to present a warrant or subpoena for information requests.[119] Apple also specifically stated that it cannot perform data extractions on iOS 8 and newer software as it does not have the encryption key.[120]

A study conducted by the Berkman Center for Internet & Society at Harvard University supports the theory that law enforcement can obtain

*DA Cyrus Vance Blast Apple's Unwillingness to Unlock Criminals' iPhones*, NY DAILY NEWS (Feb. 18, 2016, 3:43 PM), http://www.nydailynews.com/new-york/bill-bratton-blasts-apple-encryption-stance-article-1.2536506.

115 *Id.* For example, the Manhattan District Attorney's office has been stalled in collecting any evidence from the main suspect's encrypted iPhone for the murder of a Hofstra graduate student due to the phone's password protection despite the existence of a search warrant. Shayna Jacobs, *iPhone of Suspect in Hofstra Grad Student Murder Inaccessible to Prosecutors*, N.Y. DAILY NEWS, http://www.nydailynews.com/new-york/iphone-suspect-hofstra-grad-student-murder-locked-da-article-1.3492123 (last updated Sept. 14, 2017, 4:49 AM).

116 Eric Geller, *Top NYPD Official Says Apple's Encryption Helps Murderers and Kidnappers*, DAILY DOT (Mar. 7, 2016, 9:35 AM), http://www.dailydot.com/layer8/apple-iphone-encryption-nypd-john-miller-kidnappers-murderers/.

117 Kate Mather & James Queally, *The Federal Government Is Fighting Apple for Something the Police Want Too*, L.A. TIMES (Feb. 26, 2016, 11:15 AM), http://www.latimes.com/business/technology/la-me-apple-police-20160226-story.html.

118 Mather, *supra* note 117. Moore hit a dead end in an open murder investigation due to an encrypted iPhone. *Id.* In April 2015, an unknown assailant murdered an eight-months pregnant woman named Brittney Mills in her Baton Rouge home. *Id.* Investigators obtained a warrant for Mills' iPhone, but Mills' iPhone ran iOS 8 or later version of software. *Id*. Apple, therefore, refused to crack the device. *Id.*

119 *Government Information Requests,* APPLE, http://www.apple.com/privacy/government-information-requests/ (last visited Jan. 13, 2017).

120 *See Legal Process Guidelines*, *supra* note 100.

information in ways other than compelling assistance from non-government tech companies like Apple.[121] Law enforcement may use methods involving metadata to mine for information[122] or malware to catch data before encryption.[123] Despite these alternative methods for law enforcement surveillance,[124] law enforcement still faces enormous challenges in obtaining information from the "digital crime scene"[125] without a proper legal foundation.

## IV. THE CURRENT LEGAL FRAMEWORK FOR COMPELLING THIRD PARTIES TO BYPASS ENCRYPTION

Without any guidance from Congress, courts have struggled to apply an appropriate legal framework to compel third party encryption producers to assist law enforcement in obtaining information related to open investigations. Courts, like the District Court for the Central District of California, have used existing wiretapping legislation and extraordinary writ measures to compel aid from non-governmental third parties like Apple;[126] however, neither existing wiretapping legislation nor extraordinary writ measures are appropriate in compelling a completely private encryption producer to decrypt a user's encrypted information for law enforcement.[127]

---

[121] *See* MATT OLSEN ET AL., DON'T PANIC. MAKING PROGRESS ON THE "GOING DARK" DEBATE 2–3 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [hereinafter BERKMAN STUDY] (noting that the "going dark" metaphor does not accurately describe current law enforcement conditions). *See also* Pell, *supra* note 20, at 625–27.

[122] *See id.* at 3, 9. Metadata is not encrypted, and not likely to become encrypted. *Id.* Metadata can reveal information such as email addresses and mobile device location. *Id.* Since metadata is plaintext, this is a source surveillance information for law enforcement. *Id.*

[123] *See* Pell, *supra* note 20, 635 n.130, 641–42. (citing Matt Apuzzo, *F.B.I. Used Hacking Software Decade Before iPhone Fight,* N.Y. TIMES (April 13, 2016), http://mobile.nytimes.com/2016/04/14/technology/fbi-tried-to-defeat-encryption-10-years-ago-files-show.html?_r=2 (discussing how the FBI remotely installed malware on a computer as a part of criminal wiretap in order to circumvent encryption)). In order to gain access to encrypted information, law enforcement may hack a smartphone and install malware designed to catch voice communications and keystrokes before encryption. *Id.*

[124] Since law enforcement has new alternatives for surveying criminal activity, Peter Swire believes that today is the "golden age for surveillance." Swire, *supra* note 88, at 460–73. The phrase "golden age for surveillance" refers to the idea that law enforcement's surveillance activities are greatly enhanced compared to earlier periods of time. *Id.* For a discussion on the idea that technology has advanced to provide law enforcement with more means to survey the population, see Swire, *supra* note 88, at 460–73.

[125] *See supra* text accompanying note 107.

[126] *See In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016).

[127] *See infra* Part IV.A–B.

### A. *The Communications Assistance for Law Enforcement Act Cannot Reasonably Be Applied to Today's Encryption Products*

Law enforcement has considered Communications Assistance for Law Enforcement Act (CALEA) as one avenue of fitting today's encryption producers within a legislative framework.[128] Congress enacted CALEA so that law enforcement authorities with a proper court order could "intercept . . . communications."[129] Under CALEA, telecommunication carriers, telephone companies, and telecommunication manufacturers must have built-in surveillance systems that law enforcement can access and monitor. [130]

The capability requirements under CALEA are subject to exceptions. For instance, "information services" are exempt from CALEA's assistance requirements.[131] This Act defines "information services" as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[132] Further, CALEA carves out special measures for encryption stating that "*telecommunication carriers*"[133] are not required to decrypt any information or communication unless the carrier provided the encryption and has the information available to decrypt the data.[134] CALEA remains silent on whether "information service[s]" have any role in aiding law enforcement with encryption.

*American Council on Education v. FCC* solidifies the interpretation that CALEA's statutory language exempts information services from assisting law enforcement.[135] In *American Council*, the D.C. Circuit emphasized that CALEA's language clearly limits law enforcement from compelling information services to comply with controls such as installing monitoring devices.[136] The D.C. Circuit ultimately concluded that broadband providers fell within CALEA's scope because broadband providers fit the definition of

128 *See* 47 U.S.C. §§ 1001–10 (2012).

129 *See id.* § 1002(a)(1).

130 Swire, *supra* note 88, at 421–22.

131 47 U.S.C. § 1002(b)(2)(A) (2012).

132 *Id.* § 1001(6).

133 *Id.* § 1001(8)(A) (emphasis added). "The term 'telecommunications carrier' (A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." *Id.*

134 *Id.* § 1002(b)(3).

135 *See* Am. Council on Educ. v. FCC, 451 F.3d 226, 228 (D.C. Cir. 2006).

136 *Id.* (citing 47 U.S.C. § 1001(8)(C)(i)).

"telecommunication carrier" rather than "information service."[137] Although the D.C. Circuit broadened CALEA's scope to include broadband providers, companies like Apple remain outside CALEA's purview.[138]

Apple deals in convergence technology,[139] and cannot be considered either a broadband provider or a telecommunication carrier. Judge Orenstein, the presiding judge for *In re Order Requiring Apple, Inc. to Assist*, reasoned that CALEA applies only to "telecommunication carriers," and specifically exempts certain areas within the technology industry.[140] Judge Orenstein concluded that Apple falls within the technology industry exemption and would not be considered a telecommunication carrier because Apple produces convergence technology.[141]

Therefore, law enforcement cannot rely on CALEA to compel Apple to unlock iPhones and override security devices. Nor could CALEA compel any other encryption producer that does not fit the statutory definition of "telecommunication carrier" to assist in obtaining encrypted information. In addition, CALEA has not been updated in over twenty years to reflect modern technology.[142] Without some type of amendment to CALEA, devices with encryption protections, like the iPhone, will remain out of law enforcement's reach.[143]

### B. *The AWA Is an Extraordinary Measure to Use Against Private Third-Party Companies*

Law enforcement has also utilized the "AWA" to compel third party encryption producers to assist with decrypting information. While

---

137 *See id.* at 232–36 (emphasizing that the standard of review was extremely deferential to the FCC's "reasonable" interpretation of the phrase "telecommunications carrier" in the CALEA).

138 "CALEA is not viewed as applying to data contained on smart phones. . . ." *See* Peter T. King, *Remembering the Lessons of 9/11: Preserving Tools and Authorities in the Fight Against Terrorism*, 41 J. LEGIS. 173, 178 (2015).

139 *See* Christy Roland, *The Complete and Modern Guide to Technology Convergence*, AT&T DEVELOPER PROGRAM (May 15, 2017, 11:48 AM), https://developer.att.com/blog/technology-convergence ("[A]n example of technology convergence is smartphones, which combine the functionality of a telephone, a camera, a music player, and a digital personal assistant."). Convergence technology is when a single device contains two or more different technological capabilities, i.e., a cell phone that can also be used as a camera. *See* Bill Ward, *The Impact of Technology Convergence*, DIGITILIST MAG. (Aug. 6, 2014), http://www.digitalistmag.com/innovation/2014/08/06/impact-of-technology-convergence-01257734. ""

140 *N.Y. Apple iPhone Case*, 149 F. Supp. 3d at 354–55.

141 *Id.* at 356–57.

142 *See* Matthew Braga, *The FBI Is at War with Apple Because it Couldn't Change Wiretap Law*, VICE: MOTHERBOARD (Mar. 1, 2016), https://motherboard.vice.com/en_us/article/z434z4/calea-my-old-friend.. Congress passed CALEA in 1994. *Id. '*

143 Around 2009, the FBI and the Department of Justice discussed amending CALEA to encompass technology like smartphones and e-mail. *See* King, *supra* note 138, at 178–79. These proposed amendments, however, were never sent to Congress. *Id.*

considered an extraordinary writ, the AWA has been invoked at least sixty times since 2008 to compel Apple and Google to provide assistance in obtaining information from devices.[144] While law enforcement has successfully compelled private third party assistance under the AWA,[145] law enforcement cannot use the AWA to properly compel Apple to undermine its own security features.

Passed in 1789, the AWA permits federal courts to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[146] The AWA can be used to compel private third parties to provide technical assistance in certain situations.[147] In *United States v. New York Telephone Company*, the New York Telephone Company resisted an order to provide technical assistance to the FBI to install pen registers[148] by refusing to lease the telephones lines the FBI needed to install pen registers.[149] The Supreme Court found that the AWA may be applied to third parties as an auxiliary measure when that third party is "in a position to frustrate the implementation of a court order or the proper administration of justice."[150] According to the FBI, the New York Telephone Company's own property, the physical telephone lines, were likely being used to further criminal activity.[151] The Court ruled that the FBI properly invoked the AWA because the New York Telephone Company was closely related to the matter being investigated by the FBI.[152] Further, the Court concluded that the technical assistance the order required—to install pen registers—was in no way burdensome to the New York Telephone Company because the company simply had to provide the FBI with access to the lines.[153] Finally, the Court found that the New York Telephone's Company assistance was necessary because the court order to tap the lines could not

144 Eliza Sweren-Becker, *This Map Shows How the Apple-FBI Fight Was About Much More Than One Phone*, ACLU BLOG (Mar. 30, 2016, 9:00 AM), https://www.aclu.org/blog/privacy-technology/internet-privacy/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone?redirect=blog/speak-freely/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone.

145 Lorenzo Franceschi-Bicchierai, *Feds Say Apple Has Unlocked Suspects'' iPhones "At Least" 70 Times in the Past*, VICE: MOTHERBOARD (Oct. 26, 2015), https://motherboard.vice.com/en_us/article/4xagvq/feds-say-apple-has-unlocked-suspects-iphones-at-least-70-times-in-the-past.

146 All Writs Act, 28 U.S.C. § 1651(a) (2012).

147 The Act itself does not identify examples; however, case law has identified situations when courts may issue this extraordinary writ. *See, e.g.*, United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

148 Pen registers are a type of wiretapping device. *Id.* at n.1.

149 *N.Y. Tel. Co.*, 434 U.S. at 161–63.

150 *Id.* at 174–75.

151 *Id.* at 174–78.

152 *Id.*

153 *Id.* at 174–75.

be carried out without access to the physical lines.[154]

Under *New York Telephone Company*'s reasoning, law enforcement has attempted to leverage the AWA in a similar manner against companies like Apple. In *In re Order Requiring Apple, Inc. to Assist*, law enforcement tried to use the AWA as an auxiliary measure to CALEA to compel Apple's technical assistance in circumventing security measures in an encrypted iPhone.[155] This argument, however, initially failed on its face because Apple is a technology company that falls outside the scope of CALEA.[156] Therefore, ordering Apple's assistance to decrypt an iPhone could not be a proper auxiliary measure to CALEA.[157] In addition, Judge Orenstein concluded that the AWA could not be used as a "gap filler"[158] for holes in CALEA because CALEA's legislative scheme is so comprehensive that it implicitly prevents imposing orders onto private third parties like Apple.[159] The executive branch cannot use the AWA "to achieve a legislative goal that Congress has considered and rejected."[160]

Judge Orenstein also distinguished the facts of *In re Order Requiring Apple, Inc. to Assist* from those presented in *New York Telephone Company*.[161] First, unlike a telephone carrier that owns telephone lines, Apple's property was not used in the commission of a crime; rather, the

---

154 *Id.*

155 *See N.Y. Apple iPhone Case*, 149 F. Supp. 3d at 352–57.

156 *See supra* note 138, and accompanying text.

157 *See N.Y. Apple iPhone Case*, 149 F. Supp. 3d at 354, 360–64. Arguably, CALEA absolves a company like Apple from having any responsibility to assist law enforcement. *See id.*

158 *Id.* at 353, 357–58. "Gap filler" refers to the fact that Congress cannot anticipate every circumstance a court may act to "properly . . . vindicate the rights of parties before it." *Id.* Therefore, the AWA acts as a piece of legislation for courts to perform their duty even when there is gap within legislation as long as that gap is "agreeable to the usages and principles of law." *Id.* The AWA's statutory language of "usages" and "principles" compels the conclusion that the order must not merely be consistent with the law, but be "consonant with both the manner in which the laws were developed . . . and the manner in which the laws have been interpreted and implemented." *Id.*

159 *Id.* at 354.

160 *N.Y. Apple iPhone Case*, 149 F. Supp. 3d at 360; CALEA's history reveals that Congress considered whether the CALEA should be expanded to cover technology such as the iPhone, but have yet to reach a consensus. *See id*. n.25*; see also In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 15-mc-01902, 2015 WL 5920207, at *2 (E.D.N.Y. Oct. 9, 2015).

Further, the FBI has not sought to use the legislature as a means to deal with the issue of encryption. *See* James B. Comey, Dir., FBI, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, (Oct. 8, 2015), https://www.fbi.gov/news/testimony/threats-to-the-homeland ("The 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.").

161 *N.Y. Apple iPhone Case*, 149 F. Supp. 3d at 364.

criminal used his own property, which distanced Apple's role from the matter.[162] Further, while the telecommunication industry, such as phone companies, is a heavily regulated utility "with a duty to serve the public,"[163] Apple remains a private business and, like any other private entity, has no duty to serve the public.[164]

Unlike the New York Telephone Company, Apple would also bear a much larger burden by having an order of compelled technical assistance enforced against it. Apple is a private company that owes a duty to its shareholders—not the United States government or law enforcement.[165] The technical assistance the FBI requested would require Apple to undermine its own security measures, which would tarnish the Apple brand.[166] Further, Apple is not in the line of work to bypass its own security measures and this act would be offensive to the business.[167] Apple would also have to dedicate many hours to unlocking the device.[168] Thus, if the government continued with requests to compel Apple to unlock iPhones on a massive scale, Apple's productivity would be significantly impacted.[169]

Finally, "necessity" also failed to support the argument that an extraordinary writ should be issued to compel Apple to bypass its own software.[170] The FBI contradicted itself throughout the case by arguing that it could only decrypt the iPhone with Apple's help, while later claiming that there were circumstances when law enforcement had the capabilities to decrypt a specific phone without the help of private third parties.[171] Therefore, Judge Orenstein concluded that the government did not present the pressing necessity needed to issue an extraordinary writ.[172]

Not all courts have followed *In re Order Requiring Apple, Inc. to Assist*'s reasoning;[173] however, Judge Orenstein's opinion provides

---

162 *Id.* at 364–65.

163 United States v. N.Y., Tel. Co., 434 U.S. 159, 174 (1977).

164 *N.Y. Apple iPhone Case*, 149 F. Supp. 3d at 364–65.

165 *Id.* at 369.

166 *Id.*

167 *Id.* Apple prides itself as being a producer of secure products and Apple is "committed to keeping [] personal information safe." *See Our Approach to Privacy,* APPLE, http://www.apple.com/privacy/approach-to-privacy/ (last visited Jan. 11, 2017).

168 *N.Y. Apple iPhone Case*, 149 F. Supp. 3d at 370–71.

169 *Id.*

170 *Id.* at 375.

171 *Id.*

172 *Id.*

173 *See In re* Order Requiring [XXX], Inc., No. 14 Mag. 2258, 2014 U.S. Dist. LEXIS 154743, at *1–6 (S.D.N.Y. Oct. 31, 2014). Compared to Judge Orenstein's reasoning, *In re Order Requiring XXX, Inc*. reasons that the AWA does apply in compelling third-party tech companies to decrypt devices for law enforcement. *See id.* This decision, made prior to Judge Orenstein's ruling, simply concluded a tech company must assist in unlocking a cellphone as it was required in *N.Y. Tel. Co. See id.*

ammunition for Apple in future litigation. As made obvious by *In re Order Requiring Apple, Inc. to Assist*, compelling a private tech company to decrypt a device is not analogous to compelling a phone company to provide access to phone lines so the FBI can install wiretapping devices.[174] Therefore, law enforcement will likely have much more difficulty in utilizing the AWA to compel assistance from encryption producers in the future.

## V. CONGRESS MUST ADDRESS A TECHNOLOGICAL COMPANY'S ROLE IN WORKING WITH LAW ENFORCEMENT

### A. *Prior to Legislating, Congress Must First Better Understand Encryption Today*

Congress must be proactive by introducing new legislation or updating current legislation to ensure that law enforcement has the capability to receive assistance from encryption producers.[175] On February 29, 2016, two Senators introduced the Digital Security Commission Act of 2016.[176] Proposed by House Homeland Security Chairman Michael McCaul and Senator Mark Warner, the bill called to form a bipartisan[177] National

---

174 *See supra* Part IV.A–B.

175 Michael McCaul & Mark Warner, Opinion, *How to Unite Privacy and Security—Before the Next Terrorist Attack*, WASH. POST (Dec. 27, 2015), https://www.washingtonpost.com/opinions/how-to-unite-privacy-and-security—before-the-next-terrorist-attack/2015/12/27/628537c4-a9b3-11e5-9b92-dea7cd4b1a4d_story.html?utm_term=.1be00f88e00c.

176 HOMELAND SEC. REP., *supra* note 101, at 17. Although the bill passed the House in 2016, the Senate did not vote on the bill so it is possible that this legislation will be re-visited under the Trump administration. Mintz Levin Cohn Ferris Glovsky & Popeo PC, *Federal Cybersecurity Landscape for 2017*, LEXOLOGY (Jan. 3, 2017), https://www.lexology.com/library/detail.aspx?g=045e64ca-81b2-4a05-ad9a-c493fe88d105. Another bill regarding encryption was also introduced by Senators Burr and Feinstein around the same time; however, this bill was highly criticized as it was considered essentially mandating tech companies to compromise their own products for law enforcement and did not gain any traction. *See, e.g.*, Rainy Reitman, *Security Win: Burr-Feinstein Proposal Declared "Dead" for This Year*, ELEC. FRONTIER FOUND. (May 27, 2016), https://www.eff.org/deeplinks/2016/05/win-one-security-burr-feinstein-proposal-declared-dead-year.

177 The legislation is co-sponsored in the Senate by Senators Cory Gardner (R-CO), Brian Schatz (D-HI), Susan Collins (R-ME), Michael Bennet (D-CO), Shelley Moore Capito (R-WV), Angus King (I-ME), Dean Heller (R-NV), Bill Nelson (D-FL), Steve Daines (R-MT), Michael Bennet (D-CO), Jeff Flake (R-AZ), Martin Heinrich (D-NM), Rob Portman (R-OH), Mike Rounds (R-SD), Thomas Carper (D-DE) and Gary Peters (D-MI). *Sen. Warner Leads Bipartisan Coalition to Create a National Commission on Digital Security,* MARK R. WARNER, http://www.warner.senate.gov/public/index.cfm?p=sen-warner-leads-bipartisan-coalition-to-create-a-national-commission-on-digital-security_7 (last visited Jan. 13, 2017). In addition to Chairman McCaul, House co-sponsors are Representatives Jim Langevin (R-RI), Patrick Meehan (R-PA), Mike Bishop (R-MI), Ted Lieu (D-CA), Will Hurd (R-TX), Kathleen Rice (D-NY), Blake Farenthold (R-TX), Eric Swalwell (D-CA), Dan Donovan (R-NY), Jerry McNerney (D-CA), Barbara Comstock (R-VA), Mimi Walters (R-CA), Ryan Costello (R-PA), Dave Reichert (R-WA), Earl ""Buddy"" Carter (R-GA), Peter King (R-NY), Candice Miller (R-MI), John Katko (R-NY), Lamar Smith (R-TX), Barry Loudermilk

Commission on Security and Technology Challenges ("the Commission") comprised of cryptologists, law enforcement, intelligence agencies, and others in the tech sector to propose solutions to the encryption challenges presently faced by law enforcement.[178]

Senator Warner stated that the Commission would "strike an appropriate balance that protects Americans' privacy, American security, and American competitiveness."[179] The Commission would achieve this balance by: (1) assembling the brightest minds in the industry; (2) creating an open national dialogue on the topic; and (3) moving quickly.[180] The Commission would also issue an interim report within six months after it convened and then make recommendations to Congress within twelve months.[181]

Although the Commission presents a possible compromise between the tech industry and law enforcement, some civil liberty advocates vehemently oppose the idea of the United States government meeting with technological companies.[182] The Electronic Frontier Foundation ("EFF")[183] believes that a commission like that proposed by the Digital Security Commission Act would simply continue an unnecessary conversation that was already hashed out during the crypto wars of the 1990s.[184] During the 1990s, Congress took

(R-GA), Martha McSally (R-AZ), Mike Rogers (R-AL), Jeff Duncan (R-SC), Susan Brooks (R-IN), Mark Walker (R-NC), John Ratcliffe (R-TX), Betty and McCollum (D-MN). *Id.*

178 HOMELAND SEC. REP., *supra* note 101, at 17.

179 *See Sen. Warner Leads Bipartisan Coalition to Create a National Commission on Digital Security, supra* note 177. FBI Director Christopher Wray has also discussed achieving a "balance" between law enforcement and technology companies though Wray was not yet able to articulate a solution for the issue. Christopher Wray, Dir., FBI, Statement Before the House Judiciary Committee, ( July 12, 2017), https://www.hatch.senate.gov/public/index.cfm/releases?ID=C41F131A-D1E7-4E50-8E2B-1548A7EDCF17.

180 *McCaul-Warner Commission on Digital Security*, HOMELAND SECURITY COMM., https://homeland.house.gov/wp-content/uploads/2016/02/McCaul-Warner-Commission-One-pager-1.pdf (last visited Jan. 13, 2017).

181 *Id.*

182 *See, e.g.*, Erin Kelly, *Electronic Privacy Advocates Split Over Encryption Commission in New Bill*, USA TODAY (Mar. 11, 2016), http://www.usatoday.com/story/news/2016/03/11/electronic-privacy-advocates-split-over-encryption-commission-new-bill/81600870/. Similarly, FBI Director Wray's comments on achieving a balance have also be criticized. *See* Kevin Collier, *The Encryption 'Balance' Trump's FBI Candidate Wants Is Mathematically Impossible*, NY MAG. (July 12, 2017), http://nymag.com/selectall/2017/07/the-encryption-balance-fbi-nominee-wants-is-impossible.html.

183 *About EFF,* ELEC. FRONTIER FOUND., https://www.eff.org/about (last visited Jan. 13, 2017). The Electron Frontier Foundation ("EFF") is a nonprofit organization that defends civil liberties within the digital world including privacy, free expression, and innovation. *Id.* Technologist, activists, and attorneys at EFF "defend free speech online, fight illegal surveillance, advocate for users and innovators, and support freedom-enhancing technologies." *Id.*

184 Mark Jaycox, *EFF Opposes McCaul-Warner Encryption Commission*, ELEC. FRONTIER FOUND. (Mar. 7, 2016), https://www.eff.org/deeplinks/2016/03/eff-opposes-

similar attempts to reconcile law enforcement's ability to obtain information with protecting the private tech industry, which led to no solutions.[185] EFF imagines that the Commission's solution will merely be to create a key escrow, which has already been a heavily rejected solution.[186] Despite opposition from the EFF, Apple has shown support for having a commission between the tech industry and the federal government in an effort to foster a national dialogue about encryption.[187]

The EFF also fails to consider the alternatives if a new encryption discussion fails to occur between the tech industry and the federal government in the United States. The American public will face an ongoing controversy surrounding encryption without a dialogue, especially if another domestic terrorist attack occurs.[188] The Commission, or a similar commission, will help establish that encryption technology is not the problem, but the system that does not afford law enforcement a remedy is the problem. The Commission will focus on fixing a broken system that has public safety at odds with personal privacy.[189] Further, Congress has limited expertise in this new area of technology so a panel of experts within the matter can better facilitate a more informed discussion to create a system of regulatory oversight.[190] As the *Wall Street Journal* Editorial Board stated,

> A mature democracy—if America still is one—ought to be able to work out these crucial matters of national security through legislative deliberation. The public interest on encryption is best served with a rational debate, not the ad hoc nuclear legal exchange that the Administration is inviting.[191]

After meeting with experts in the field and better understanding the technology, Congress would have a better path forward to knowledgably adopt legislation and regulations. The Commission may even consider new methods for law enforcement to access information on encrypted devices. One approach could be a legal hacking regime.[192] Another strategy that the Commission may look to for regulating encryption domestically could be a

mccaul-warner-encryption-commission.

185 *Id*; *see also supra* Part III.B and accompanying text.

186 *See* Jaycox *supra* note 184; *see also supra* Part III.B and accompanying text.

187 Brian Bennett, *Apple Backs Idea for Panel to Study Technology and National Security*, L.A. TIMES (Feb. 23, 2016), http://www.latimes.com/nation/la-na-apple-commission-2-20160223-story.html.

188 *See* McCaul & Warner, *supra* note 175.

189 *See* Ryan Hagemann, *The Path Forward on Encryption: The McCaul-Warner Commission,* LAWFARE BLOG (June 24, 2016, 2:10 PM), https://www.lawfareblog.com/path-forward-encryption-mccaul-warner-commission.

190 *Id.*

191 Joe Rago, Editorial, *The FBI vs. Apple*, WALL ST. J. (Feb. 19, 2016), http://www.wsj.com/articles/the-fbi-vs-apple-1455840721.

192 *Id.*

licensing scheme like the one implemented in Israel.[193]

### B. *Israel Strikes a Regulatory Balance Between National Security and Individual Liberty for Encryption*

The Israeli government needs highly secure encryption codes to protect information within their own national agencies, but the Israeli government also needs to incept and decrypt information regarding terroristic threats.[194] The Israeli government decided to solve its own "crypto wars" by implementing specific domestic encryption licensing methods.[195] Under Israel's 1957 Control of Commodities and Services Law, the Israeli Minister of Defense created an encryption-control licensing regime in 1974.[196] Under this encryption policy, Israel "aims to balance between national security interests on the one hand and preserving competitive Hi-tech Industry on the other, whilst enabling users to engage in encryption without over-burdening restrictions."[197]

The licensing scheme has three levels: a general license, a restricted license, and a special license.[198] Each level has its own requirements that an applicant must meet to receive the license.[199] When a company wants to produce a new encryption product, the company must submit an application

---

193 *See infra* Part V.B.

194 Matthew Waxman & Doron Hindin, *How Does Israel Regulate Encryption?*, LAWFARE BLOG (Nov. 30, 2015, 9:11 AM), https://www.lawfareblog.com/how-does-israel-regulate-encryption.

195 *Id.*

196 *Id.*

197 *Encryption Policy*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/Encryption_Policy.aspx (last visited Sept. 26, 2017).

198 *See* GOLUMBIC, *supra* note 71, at 130–31; *see also Encryption Control in Israel*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx (last visited Sept. 26, 2017). The general license is granted for all types of encryption engagements, "with the exceptions of modification and integration." GOLUMBIC, *supra* note 71, at 131; *see also Encryption Control in Israel*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx (last visited Sept. 26, 2017). A general license has no time limit. *See also Encryption Control in Israel*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx (last visited Sept. 26, 2017). Limited licenses, or restricted licenses, are more restricted and granted only for "certain types of encryption measures and for certain destination countries, based on criteria such as type of user." GOLUMBIC, *supra* note 71, at 131; *see also Encryption Control in Israel*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx (last visited Sept. 26, 2017). Restricted licenses are valid only for one year. *Encryption Control in Israel*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx (last visited Sept. 26, 2017). Special licenses are issued only for a certain form of encryption engagement and are also valid only for one year. *See* GOLUMBIC, *supra* note 71, at 131; *see also Encryption Control in Israel*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx (last visited Sept. 26, 2017).

199 *Encryption Control in Israel*, *supra* note 198.

to the Supervisor of Military Export Controls in the Ministry of Defense to receive the necessary license for the development of the encryption measures.[200] Once the encryption measures have been developed, an applicant must also apply for an additional license for the production, export, or sale of the encryption product.[201] Throughout this process, the Ministry may request information from the applicant, including a "working" version of the product.[202] The product is then either approved or rejected for a license.[203] Further, the license may not be infinite and when it expires, the encryption developer must apply for a renewal.[204]

Israel's current licensing system was updated in 1998, and the amended language allows Israel to incorporate modern technology.[205] The amended language also contains a "Free Means" exemption, which allows for certain encryption products to be decontrolled.[206] Further, an "Internal Use" rule allows for a company or individual to use encryption products without a license for intra-company purposes.[207] The Ministry of Defense also issued a policy update in 2001, which relaxed some policy requirements such as exempting certain license holders from saving sales data.[208]

By having this flexible system, Israel fosters open communication between the private and public sectors.[209] The Israeli government and its law enforcement are constantly apprised of encryption advances.[210] If the government identifies new encryption technology that may threaten national security or law enforcement, the program's information-sharing scheme allows the tech companies and the government to cooperate and reach possible solutions and compromises.[211] To date, no known law enforcement action has taken place concerning violations of the encryption controls.[212] Yet, this system seems to work since major technology companies, including

200 *See* GOLUMBIC, *supra* note 71, at 132.

201 *Id.*

202 *Id*; *see also Encryption Policy, supra* note 197 ("[T]he applicant will be required to submit to the Ministry of Defense the necessary technical information and/or a sample of the product and/or any necessary additional information for completing the technical review.").

203 *See* GOLUMBIC, *supra* note 71, at 132.

204 *Id.*

205 *Id.* at 128.

206 Waxman & Hindin, *supra* note 194. *See also Free Means,* MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/FreeMeans.aspx (last visited Sept. 26, 2017) ("Any Encryption Item that has received a general licence [sic] is declared a '"Free means"', and as such requires no further licence [sic].").

207 Waxman & Hindin, *supra* note 194.

208 *Encryption Policy*, *supra* note 197.

209 Waxman & Hindin, *supra* note 194.

210 *Id.*

211 *Id.*

212 *Id.*

Apple, continue to comply and submit to the Israeli licensing system.[213] According to available statistics, denials of licenses for encryption in Israel are also rare and the average time for processing an application is a few days, which further demonstrates the cooperation between the Israeli government and technology companies.[214] Israel's encryption regulation reflects encryption's dual use nature[215] by balancing between individual privacy and national security.[216]

Israel faces similar threats of terrorism[217] and public safety, but also values user privacy. Israel's regulation provides a good example of how to balance competing interests within the United States. A study of Israel's encryption regulations may help the Commission and Congress develop their own plans to develop encryption regulation within the United States. A commission like that proposed by the Digital Security Commission Act is the first step to foster a dialogue between tech companies and the United States government. Commissions, however, are limited in duration.[218] On the other hand, if Congress legislated a licensing scheme similar to Israel's, the federal government could continue the open dialogue between the tech industry and law enforcement.[219] This persistent engagement would not only lead to less animosity between the two entities, but would also create solutions that would allow law enforcement to receive assistance regarding encrypted information.

## VI. CONCLUSION

Although Farook's iPhone has faded from the spotlight, the controversy surrounding stronger private encryption products remains, and the FBI and Apple continue to face legal battles.[220] The American public and Congress

213 *Id.*

214 *Statistics*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/Statistics.aspx (last visited Sept. 26, 2017).

215 *See supra* note 102, and accompanying text.

216 GOLUMBIC, *supra* note 71, at 130.

217 Waxman & Hindin, *supra* note 194.

218 The Commission was projected to be a year long. *See* HOMELAND SEC. REP., *supra* note 101, at 4.

219 Similarly, in India, the Observer Research Foundation, a public policy think-tank, proposed a licensing scheme like Israel's as an encryption policy due to the cooperative exchange of information such a scheme offers. Bedavyasa Mohanty, *Encryption Policy 2.0: Securing India''s Digital Economy*, ORF SPECIAL REPORT 4 (2017), http://cf.orfonline.org/wp-content/uploads/2017/05/ORF_SpecialReport_35.pdf.

220 The FBI recently sought to unlock an iPhone used by Dahir Ada, a terrorist that committed a mass stabbing in a Minnesota Shopping Mall. Joe Uchill, *FBI, Apple Eye New Fight over Encryption,* THE HILL (Oct. 10, 2016, 6:00 AM), http://thehill.com/policy/cybersecurity/299853-fbi-apple-eye-new-fight-over-encryption; Amy Forliti, *FBI Still Trying to Establish Motive in St. Cloud Mall Stabbing*, TWIN CITIES (Feb. 17, 2017), http://www.twincities.com/2017/02/17/fbi-still-trying-to-establish-motive-in-st-cloud-mall-stabbing/.

must not forget the dueling interests that are at stake with encryption: individual privacy and security, and national security and law enforcement investigations. Instead of fighting a war, the federal government and private sector companies should call a truce. By following a model like that currently employed in Israel, an open discussion between the technology sector and law enforcement can produce new solutions to old problems faced by law enforcement.[221] Until Congress provides the judiciary with clear guidance, courts will continue to struggle to apply outdated legislation on ever-increasingly powerful encryption technology to aid law enforcement. After battling for years, the time has come for law enforcement and the private sector to come together in a dialogue and create a legal scheme to provide law enforcement with the assistance it so desperately needs.

[221] Although encryption technology has evolved, the United States has struggled since the 1990s with solutions for regulating encryption. *See supra* Part III.B and accompanying text.