4-1-2018

The Fight Over Encryption: Reasons Why Congress Must Block the Government from Compelling Technology Companies to Create Backdoors into Their Devices

Shannon Lear
Cleveland-Marshall College of Law

THE FIGHT OVER ENCRYPTION: REASONS WHY CONGRESS MUST BLOCK THE GOVERNMENT FROM COMPELLING TECHNOLOGY COMPANIES TO CREATE BACKDOORS INTO THEIR DEVICES

SHANNON LEAR*

ABSTRACT

Advances in technology in the past decade have blurred the line between individuals' privacy rights and the government's ability to access information. How should this issue be handled in a manner that balances the privacy rights of individuals and the government's access to information in the interest of national security?

This Note proposes a bright-line rule that would continue to allow the government to obtain specific information from a data service provider without forcing the company to circumvent its own security features. Under this rule, a company shall relinquish specific information in its control or possession only by court order and only when necessary to aid the government in the interest of national security. Such information would not include security software, but instead only account information, which the company can readily access. Further, no court shall order a data service provider to create or modify programming that would bypass security features as a means to access protected information. Such programming would provide hackers and governmental entities with a backdoor into other similar devices. Indeed, once created and surrendered, this programming is at risk of being hacked or used by the government in other circumstances. The suggested legislation would not bar a technology company from voluntarily assisting the government or law enforcement in gaining access to encrypted data by creating or modifying programming. If a company chooses to do so, the company could assist and would receive reasonable compensation for the costs incurred.

The legal battles between Apple and the FBI demonstrate that without a bright-line rule, the government will continue to attempt to gain access to as much information as it can through legislation such as the All Writs Act. Further, forcing a technology company to create or modify programming violates constitutional rights. The costs associated with creating a backdoor far exceed the benefits. Therefore, until Congress speaks to this issue, the legal battle will continue, as the line between privacy rights and the government's access to information remains blurred.

CONTENTS

* J.D. Candidate, May 2018, Cleveland-Marshall College of Law. I would like to thank Professor Patricia Falk for her advice and guidance while writing this Note. I would also like to thank Michael and Colleen Lear for their endless support.

I. INTRODUCTION

Over one billion Apple devices are active worldwide.[1] In the United States, 95% of individuals own a cellphone, and 77% own a smartphone.[2] Additionally, approximately 80% of adults own a computer, and 50% own a tablet.[3] These statistics suggest that an overwhelming amount of the population stores personal information on the Internet.[4] But, what degree of protection exists for such personal information? Is it safe to store our information online? Of course, technology companies worldwide have installed security features on their devices to protect their customers' personal information.[5] These security systems encrypt data, "turn[ing] your data into indecipherable text that can be read only by those with the right key."[6] However, not all information can be protected; some electronic data can be accessed remotely through surveillance techniques.[7] Further, electronic data companies surrender information to the government or law enforcement agencies upon service of a court order or presentation of a search warrant.[8]

In 2013, reporters published secret, government documents that revealed surveillance of phone and Internet communications.[9] Throughout these operations, the government collected data from millions of Internet users and telephone subscribers.[10] Since these leaks, a majority of Americans have attempted to secure their personal

---

[1] Nick Statt, *1 Billion Apple Devices Are in Active Use Around the World*, VERGE (Jan. 26, 2016), http://www.theverge.com/2016/1/26/10835748/apple-devices-active-1-billion-iphone-ipad-ios.

[2] *Mobile Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017) [hereinafter PEW RES. CTR.], http://www.pewinternet.org/fact-sheet/mobile/. Oxford Dictionary defines smartphone as "[a] mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps." *Smartphone*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/smartphone (last visited Feb. 14, 2017).

[3] PEW RES. CTR., *supra* note 2.

[4] Personal information that is often stored on devices includes conversations, photographs, music, contact information, calendar events, financial information, and health information. *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/.

[5] Patrick Gray, *Tech Companies and Government May Soon Go to War over Surveillance*, WIRED (Aug. 29, 2013), https://www.wired.com/2013/08/stop-clumping-tech-companies-in-with-government-in-the-surveillance-scandals-they-may-be-at-war/.

[6] *Our Approach to Privacy*, APPLE, https://www.apple.com/privacy/approach-to-privacy/ (last visited Feb. 14, 2017).

[7] *See* 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.

[8] *Id.*

[9] Paul Szoldra, *This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks*, BUS. INSIDER (Sept. 16, 2016), http://www.businessinsider.com/snowden-leaks-timeline-2016-9.

[10] *Id.*

information, believing that the government's surveillance of communications was "unacceptable."[11]

Recently, the government has sought to broaden privacy laws in technology and government access to data.[12] One example of this is the legal battle between the Federal Bureau of Investigation ("FBI") and Apple, Inc. ("Apple").[13] Following a shooting in San Bernardino, California, the FBI obtained the iPhone of San Bernardino shooter Rizwan Farook, but the FBI was unable to access certain information stored on the device.[14] The FBI requested a court order demanding that Apple create a backdoor to its security features so the government could access the secure information contained on Farook's iPhone.[15] A magistrate judge for the United States District Court for the Central District of California ordered Apple to assist the FBI in hacking into the iPhone.[16] Apple fought the court order and refused to create a backdoor.[17] Shortly thereafter, the FBI dropped its case against Apple after an anonymous third party helped the FBI gain access to the iPhone.[18]

Another recent legal battle between the FBI and Apple involved a locked device belonging to Jun Feng, a drug offender.[19] The FBI sought a court order to compel Apple to assist the FBI in hacking into the locked device.[20] Although Feng pleaded guilty to the charges against him, the FBI and Apple requested that the United States District Court for the Eastern District of New York still address the issue of whether

---

[11] Arik Hesseldahl, *Snowden Leaks Have Changed How Americans See Their Privacy*, RECODE (Mar. 16, 2015), http://www.recode.net/2015/3/16/11560290/snowden-leaks-have-changed-how-americans-see-their-privacy.

[12] *See* Lichtblau & Benner, *supra* note 7.

[13] Elizabeth Weise, *Apple v FBI Timeline: 43 Days that Rocked Tech*, USA TODAY (Mar. 30, 2016), http://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400/.

[14] *Id.*

[15] Memorandum of Points & Authorities at 1, United States v. Black Lexus IS300 California License Plate 5KGD203, handicap placard 360466F, Vehicle Identification No. JTHBD192X50094434, No. 15–0451M 2016 WL 680288, at *2 (C.D. Cal. Feb. 16, 2016).

[16] Order Compelling Apple, Inc. to Assist Agents in Search at 1, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15–0451M 2016 WL 618401, at *1–2 (C.D. Cal. Feb. 16, 2016) [hereinafter Order Compelling Apple to Assist].

[17] *A Message to Our Customers*, *supra* note 4.

[18] Julia Edwards, *FBI Paid More than $1.3 Million to Break into San Bernardino iPhone*, REUTERS (Apr. 21, 2016), http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB.

[19] Kevin McCoy, *Apple Doesn't Have to Unlock Drug Dealer's iPhone, Judge Says*, USA TODAY (Mar. 3, 2016), http://www.usatoday.com/story/money/2016/02/29/judge-denies-fed-request-force-apple-bypass-iphone-passcode/81125500/.

[20] *Id.*

the government was able to compel Apple to create software to hack into the device.[21] After hearing from Apple and the Department of Justice ("DOJ"), the magistrate judge refused to order Apple to modify its programming to enable the FBI to bypass security features on the iPhone.[22]

Advocates on both sides of this issue are vying for legislation.[23] Meanwhile, the government is taking these matters to court and seeking a judgment in its favor. If the court issues a writ compelling Apple to create or modify programming that would disable security features on an iPhone, the government would rely on this precedent in future matters.[24] This issue posits important questions: (1) to what information does (and should) the government legally have access; (2) should the government and law enforcement be allowed to compel technology companies to hack into devices to gain access to encrypted data; and (3) if so, under what circumstances should this be allowed? Recently, Apple has had requests to help gain access to data stored on locked iPhones from many other agencies.[25] While the discussed battles between Apple and the FBI may be over, we will continue to see litigation between the government and technology companies over this issue in the future.[26] To settle this dispute, Congress should enact legislation drawing a line between what the government and law enforcement agencies can and cannot compel technology companies to do. More specifically, Congress should not allow the government and law enforcement agencies to have access to encrypted data, if the only means by which to obtain the data is by forcing companies to write or rewrite programming to hack into locked devices.

Section II of this Note will provide the history of the right to privacy and will discuss limitations on these privacy rights. Section III will address current problems regarding privacy rights and the government's access to electronic information. It also will explore the current laws surrounding this issue, using the recent legal battles between the FBI and Apple—the FBI's attempts to gain access to the iPhone of Syed Rizwan Farook, the San Bernardino shooter, and the FBI's attempts to gain access to the locked device belonging to drug dealer Jun Feng—as examples. Section III also will address other legal issues facing technology companies when they fail to comply with overreaching search warrants.

Section IV will argue that Congress should enact legislation setting out a hard and fast rule that would protect encrypted data. Safeguarding encrypted data would protect, rather than harm, national security. Legislation preventing the compelled

---

[21] Alison Frankel, *How a N.Y. Judge Inspired Apple's Encryption Fight with Justice*, REUTERS (Feb. 17, 2016), http://blogs.reuters.com/alison-frankel/2016/02/17/how-a-n-y-judge-inspired-apples-encryption-fight-with-justice/.

[22] *Id.*

[23] *See The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 2 (2016); Katie Benner & Joseph Goldstein, *Apple Wins Ruling in New York iPhone Hacking Order*, N.Y. TIMES (Feb. 29, 2016), https://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html.

[24] *See Answers to Your Questions About Apple and Security*, APPLE, http://www.apple.com/customer-letter/answers/ (last visited Nov. 22, 2017).

[25] *Id.*

[26] *See* Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016), https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.

creation of backdoors will prevent the government from becoming too powerful, thus keeping Big Brother at bay. Conversely, a law allowing the government to compel the creation of backdoors would violate Constitutional rights and would incur more costs than benefits.

Finally, Section V will propose a legislative solution. The proposed law would prohibit the government and law enforcement agencies from compelling a technology company to modify or create programming to bypass security codes on locked devices. However, this law would not preclude technology companies from deciding to provide technological assistance to aid investigations in which threats to public safety or national security exist. In circumstances where a company does provide technological assistance, this law would require that the government or law enforcement agency provide reasonable compensation to the company in exchange for the services rendered. Further, this law would prohibit companies from selling a hack or backdoor. These measures are necessary to protect national security, to protect individuals' Constitutional rights by limiting government power, and to promote efficiency, predictability, and uniformity in the law.

II. THE HISTORY OF PRIVACY RIGHTS

While not expressly stated in the United States Constitution, the right to privacy is implied in the Fourth Amendment to the Constitution.[27] The Fourth Amendment states:

> The right of the people to be secure in their persons, 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 describing the place to be searched, and the persons or things to be seized.[28]

Through case law, the Supreme Court has interpreted the Fourth Amendment and defined the right to privacy. In *Katz v. United States*, the Supreme Court recognized that the Fourth Amendment protects an individual rather than a specific constitutionally protected area.[29] The Court ruled that electronic surveillance of a public phone booth conversation was a search and seizure under the Fourth Amendment because the defendant intended that the telephone conversation be private and "sought to exclude . . . the uninvited ear."[30] Though the phone booth was publicly accessible, the defendant sought to exclude others from hearing the communication.[31] By contrast, the Court held that information that a person does not attempt to secure

---

[27] Tim Sharp, *Right to Privacy: Constitutional Rights & Privacy Laws*, LIVE SCI. (June 12, 2013), http://www.livescience.com/37398-right-to-privacy.html.

[28] U.S. CONST. amend. IV.

[29] Katz v. United States, 389 U.S. 347, 351 (1967) (overturning Olmstead v. United States, 277 U.S. 438 (1928), and Goldman v. United States, 316 U.S. 129 (1942), which allowed the warrantless search and seizure of intangible property).

[30] *Id.* at 352.

[31] *Id.*

and instead "knowingly exposes to the public" was not protected under the Fourth Amendment.[32]

In 2012, the Supreme Court expanded *Katz* in *United States v. Jones*; the Court found that global positioning system tracking of a motor vehicle was a "search" within the meaning of the Fourth Amendment.[33] Two years later, in *Riley v. California*, the Supreme Court held that a warrantless search of cell phone data contained on a device seized during an arrest was unconstitutional.[34] This case acknowledged an individual's right to privacy in content stored on cell phones and held that law enforcement must obtain a warrant to access this private information.[35]

In addition to case law interpreting privacy rights, Congress has enacted legislation that governs the access to, and use of, electronic information.[36] For example, the Electronic Communications Privacy Act of 1986 ("ECPA") classifies different types of information and ascribes a different level of protection to each classification.[37] Based on the classification under which information falls, access to such information may require a subpoena, court order, or a search warrant.[38] Yet, the ECPA protects only a subset of virtual communication and affords little protection to workplace communications.[39]

Following the September 2001 terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act"). The Patriot Act updated the ECPA

---

[32] *Id.* at 351.

[33] United States v. Jones, 565 U.S. 400, 404–05 (2012) ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."); *id.* at 406 ("[W]e must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting Kyllo v. United States 533 U.S. 27, 31 (2001))).

[34] Riley v. California, 134 S. Ct. 2473, 2477 (2014).

[35] Naomi Lachance, *At Supreme Court, Debate over Phone Privacy Has a Long History*, NPR (Mar. 8, 2016), http://www.npr.org/sections/alltechconsidered/2016/02/29/468609371/at-supreme-court-debate-over-phone-privacy-has-a-long-history.

[36] *See, e.g.*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–21, 2701–10, 3121–26).

[37] *Id.*; U.S. DEP'T OF JUSTICE, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C.§ 2510–22*, JUST. INFO. SHARING, [hereinafter U.S. DEP'T OF JUSTICE, *ECPA*], https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last revised July 30, 2013).

[38] 18 U.S.C. § 2518 (1986); *see* U.S. DEP'T OF JUSTICE, *ECPA*, *supra* note 37. The ECPA criminalizes electronic surveillance of "wire, oral, or electronic communication." 18 U.S.C. § 2511 (1986); ELEC. PRIVACY INFO. CTR., *Electronic Communications Privacy Act (ECPA)*, EPIC.ORG, https://www.epic.org/privacy/ecpa/ (last visited Feb. 15, 2017). However, exceptions to this rule exist. *See, e.g.*, 18 U.S.C. § 2516–17 (1986). For example, an employer is allowed to surveil employee communications, so long as the employer included this in employee contracts. *See* ELEC. PRIVACY INFO. CTR., *supra* note 38.

[39] *Privacy*, USLEGAL.COM, https://internetlaw.uslegal.com/privacy/ (last visited Dec. 1, 2016).

and expanded government access to information.[40] The Act extended the range of terrorist activities on which the government could gather information through surveillance.[41] Further, the Patriot Act gave the government broad authority to gather information on a specific person without specifying the exact electronic devices to be surveilled.[42] Yet, despite such legislation and case law on privacy rights in consumer electronic data, many gaps still exist in the law. The line between individual rights and government rights to encrypted data stored on locked devices remains unclear.

III. THE RAPID ADVANCEMENT OF TECHNOLOGY RAISES NEW CONCERNS REGARDING PRIVACY RIGHTS & NATIONAL SECURITY

In 2013, reporters leaked government documents that revealed a high level of government surveillance of civilian phone and Internet communications.[43] The government conducted this surveillance unknowingly to the public; upon learning of such government action, many Americans sought to secure their data.[44] Yet, in recent years, the government has sought to broaden its access to data[45]—taking Apple, Google, and Microsoft to court over access to electronic data.[46] Further, government and law enforcement requests for electronically stored personal information have increased in the past few years.[47]

A. The Problem

The year 2013 shed light on the issue of privacy in the age of technology. That year, former National Security Agency ("NSA") contractor Edward Snowden leaked information on government surveillance.[48] "Whistleblower" Snowden leaked this information to reporters who subsequently reported it to the public, thereby exposing

---

[40] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272 (2001); *see* U.S. DEP'T OF JUSTICE, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, JUST. INFO. SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1281#contentTop (last revised July 29, 2013).

[41] U.S. DEP'T OF JUSTICE, THE USA PATRIOT ACT: PRESERVING LIFE AND LIBERTY 1, https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (last visited Feb. 12, 2018).

[42] *Id.* Congress expanded the government's surveillance authority "because international terrorists are sophisticated and trained to thwart surveillance by rapidly changing locations and communication devices such as cell phones . . . ." *Id.* at 2.

[43] Szoldra, *supra* note 9.

[44] *See* Hesseldahl, *supra* note 11.

[45] *See id.*

[46] Matt Apuzzo et al., *Apple and Other Tech Companies Tangle with U.S. over Data Access*, N.Y. TIMES (Sept. 7, 2015), https://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html.

[47] Rafia Shaikh, *Apple & Google Report Sharp Increase in Government Data Requests*, WCCFTECH (Sept. 29, 2017), https://wccftech.com/google-apple-report-high-data-requests/.

[48] *Edward Snowden: Leaks that Exposed US Spy Programme*, BBC NEWS (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964.

details of secret government operations.[49] One such exposed operation concerned a government order granted by the Foreign Intelligence Surveillance Court ("FISC") that compelled Verizon to turn over all call information in their system on a daily basis.[50] FISC granted the order under the "business records" provision of the Patriot Act.[51] This systematic collection of communication records is alarming because the communications were "collected indiscriminately and in bulk—regardless of whether [the government] suspected . . . any wrongdoing."[52] This collection is also unusual because of the all-encompassing nature of the order.[53]

Typically, a court order for records granted by FISC relates to a specific individual or group suspected of terrorist activities.[54] Instead, this court order, which excluded message content and personal information attached to cell phone numbers, "would allow the NSA to build easily a comprehensive picture of who any individual contacted, how and when, and possibly from where, retrospectively."[55] United States senators have voiced concerns that the government's "extreme interpretation of the law" allows the NSA to "engage in excessive domestic surveillance."[56] Snowden described these operations as "the systematic surveillance of innocent citizens."[57] The leaks elucidated how easily the government could obtain electronic data and communications without the public's knowledge.

Snowden argued regarding government action:

> So long as there's broad support amongst a people, it can be argued there's a level of legitimacy even to the most invasive and morally wrong program, as it was an informed and willing decision. . . . However, programs that are implemented in secret, out of public oversight, lack that legitimacy, and that's a problem. It also represents a dangerous normalization of

---

[49] Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance; *see Edward Snowden: Leaks That Exposed US Spy Programme*, *supra* note 48.

[50] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013) [hereinafter Greenwald, *NSA*], https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Angus West, *17 Disturbing Things Snowden Has Taught Us (So Far)*, PUB. RADIO INT'L (June 1, 2015), http://www.pri.org/stories/2013-07-09/17-disturbing-things-snowden-has-taught-us-so-far.

[51] Greenwald, *NSA*, *supra* note 50 (citing 50 U.S.C. § 1861 (2017)).

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] Barton Gellman et al., *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST (June 9, 2013), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

> "governing in the dark," where decisions with enormous public impact occur without any public input.[58]

The government is given much leeway when it uses our national intelligence agencies to collect information.[59] With the rise of technology comes the emergence of new threats to our national security. To combat cybercrime, the government collects information such as "logs of telephone, Skype, and cell phone calls, tweets, Facebook posts, emails, Internet-site visits, GPS coordinates, and so forth."[60] One commentator described this extensive collection of information as "the amassing of an enormously large haystack, within which intelligence and law enforcement agencies would, under current U.S. law, be entitled to search for a very few, legally distinct needles."[61] Since the 2013 intelligence leaks, courts have issued fewer and fewer court orders that would allow the government access to civilian records through surveillance.[62] Despite this abatement of pro-government court orders, the issue of privacy remains pervasive and will continue to spark debate.[63] Most recently, the legal battles between Apple and the FBI have individuals talking about privacy concerns.[64]

B. The Federal Bureau of Investigation Versus Apple

The following two cases provide background information on the growing tension between Apple and the FBI. These cases also illustrate the problem of Congressional silence on government authority to force companies to assist in gaining access to content stored on locked devices.

1. Syed Farook's iPhone

Early in December of 2015, Syed Rizwan Farook and Tashfeen Malik killed fourteen people and injured twenty-two others in a shooting in San Bernardino, California.[65] Farook was born in the United States and married Malik, who was born in Pakistan and moved to the United States in 2015.[66] The couple spent years plotting

---

[58] George R. Lucas, Jr., *NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden*, 28 ETHICS & INT'L AFF. 29, 29 (2014) (quoting James Risen, *Snowden Says He Took No Secret Files to Russia*, N.Y. TIMES, Oct. 18, 2013, at A1).

[59] *Cf. id*. at 32 (comparing data collection to a haystack).

[60] *Id.* at 31.

[61] *Id.* at 32.

[62] *Cf. id.*

[63] *See* Michael Hack, *The Implications of Apple's Battle with the FBI*, NETWORK SECURITY July 2016 at 8, 8–10.

[64] *See id.*

[65] *San Bernardino Shooting Updates*, L.A. TIMES, http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory.html (last visited Feb. 12, 2018).

[66] *Id.*

the attack.[67] An investigation into their communications over the Internet suggested that the couple was communicating with a religious extremism group.[68]

Following the shooting, which resulted in the death of Farook and Malik among others, the United States government attempted to gain access to the content of Farook's iPhone with little success.[69] The iPhone was locked with a numeric password set by Farook.[70] However, the FBI was unable to attempt to determine the passcode because Apple codes an auto-erase setting into all iPhones.[71] This setting, if enabled by the user, erases all data after ten incorrect attempts to unlock the phone with a passcode.[72] There is no way to tell whether or not the auto-erase function is enabled on a device.[73]

The FBI cited the All Writs Act[74] in its argument and requested a court order to compel Apple to help the FBI gain access to the content contained on the iPhone by altering Apple's software as a means of disabling the auto-erase function.[75] The broad text of the All Writs Act, which Congress passed in 1789,[76] "permits a court, in its 'sound judgment,' to issue orders necessary 'to achieve the rational ends of law' and 'the ends of justice entrusted to it.'"[77]

In its argument, the FBI relied on *United States v. New York Telephone Co*., a case in which the Supreme Court upheld a district court's order pursuant to the All Writs Act.[78] Since the Supreme Court's decision in that seminal case in 1977, "the All Writs

---

[67] Richard Serrano, *Senator: How Could Malik Get a K-1 Visa?*, L.A. TIMES (Dec. 9, 2015, 9:28 AM) (citing a conversation between Senator Charles Schumer (D–N.Y.) and FBI Director James Comey), http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory.html.

[68] *See Everything We Know About the San Bernardino Terror Attack Investigation So Far*, L.A. TIMES, http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html (last visited Feb. 12, 2018). Farook and Malik "jointly pledged allegiance to Islamic State on social media" not long before the shooting occurred. *Id.* In Facebook messages to a couple of her friends from Pakistan dating back to 2012 and 2014, Malik "pledg[ed] her support for Islamic jihad and sa[id] she hoped to join the fight one day . . . ." *Id.*

[69] Memorandum of Points & Authorities, *supra* note 15, at 2–3.

[70] *Id.* at 3.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] 28 U.S.C. § 1651(a) (2017). The All Writs Act states, "[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 to the usages and principles of law." *Id.*

[75] Memorandum of Points & Authorities, *supra* note 15, at 9.

[76] Robert Longtin, *Apple, the FBI, and an Act from 1789: The FBI's Impermissible Use of the All Writs Act*, COLUM. BUS. L. REV. (Mar. 28, 2016), https://cblr.columbia.edu/apple-the-fbi-and-an-act-from-1789-the-fbis-impermissible-use-of-the-all-writs-act/.

[77] Memorandum of Points & Authorities, *supra* note 15, at 9 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 172–73) (1977)).

[78] *Id.* at 10 (citing *N.Y. Tel. Co.*, 434 U.S. at 174).

Act has been understood to authorize a federal court, in conjunction with a validly obtained search warrant, to issue writs to *non*-parties directing the recipient to provide 'reasonable technical assistance' to the government in the execution of the warrant."[79] In *N.Y. Telephone Co.*, the FBI sought an order from the United States District Court for the Southern District of New York to compel a telephone company to provide technical assistance to the FBI for the use of pen registers in an investigation into alleged gambling offenses.[80] The FBI submitted an affidavit alleging that "certain individuals were conducting an illegal gambling enterprise" and that "there was probable cause to conclude that an illegal gambling enterprise using the facilities of interstate commerce was being conducted."[81] Further, the affidavit claimed that two telephones were being used in relation to the described offenses.[82] On appeal, the Supreme Court found that "the order compelling respondent to provide assistance was clearly authorized by the All Writs Act and comported with the intent of Congress."[83]

For Apple to comply with a court order compelling the company to assist the FBI in unlocking Farook's iPhone, Apple would have to create programming to undermine the iPhone's security features, essentially creating a backdoor.[84] Once created, this programming could be used on any iPhone to get past security features and hack into any device.[85] While the government asserts that it would only use the programming in this specific instance, "[l]aw enforcement agents around the country . . . have hundreds of iPhones they want Apple to unlock if the FBI wins this case."[86] Beyond the fear that the government and law enforcement agencies around the country would use this "key" to gain access to other devices, a risk of "hackers and cybercriminals" getting their hands on this programming also exists, which would put electronic information at high risk.[87]

---

[79] Robert Chesney & Steve Vladeck, *A Coherent Middle Ground in the Apple-FBI All Writs Act Dispute?*, LAWFARE BLOG (Mar. 21, 2016, 7:00 AM) (citing *N.Y. Tel. Co.*, 434 U.S. at 159), https://www.lawfareblog.com/coherent-middle-ground-apple-fbi-all-writs-act-dispute.

[80] *N.Y. Tel. Co.*, 434 U.S. at 161. The United States Code defines pen register as

> a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business . . . .

18 U.S.C. § 3127(3) (2009).

[81] *N.Y. Tel. Co.*, 434 U.S. at 162.

[82] *Id.* at 161.

[83] *Id.* at 160 (quoting the syllabus).

[84] *See Answers to Your Questions About Apple and Security*, *supra* note 24.

[85] *Id.*

[86] *Id.*

[87] *Id.*

Apple fought the court order, describing the backdoor as "something we consider too dangerous to create."[88] Apple explained:

> In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.
>
> The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks—from restaurants and banks to stores and homes. No reasonable person would find that acceptable.[89]

According to Apple, creating the backdoor would destroy years of Apple's efforts in creating security features that secure customers' personal data ranging from photographs to financial information.[90] Not only would this backdoor make information vulnerable to criminals and hackers, it would also put personal, protected information into the hands of the government, thereby threatening the rise of "Big Brother."

On February 16, 2016, the United States District Court for the Central District of California issued an order compelling Apple to provide assistance to the FBI in accessing the protected data on Farook's iPhone.[91] This order compelled Apple to assist the FBI in accessing content on the iPhone by way of modifying or creating programming to circumvent the security features on the iPhone to allow the government multiple attempts to determine the passcode.[92] Despite the court order, Apple refused to assist the FBI in gaining access to the contents of the iPhone.[93]

On March 28, 2016, the FBI gained access to the iPhone with the help of a third party and dropped its case against Apple.[94] The conclusion of the legal battle between the FBI and Apple was both a win and a loss for the technology company.[95] The FBI dropping its case against Apple meant that Apple no longer had to comply with the court order.[96] However, the FBI was able to gain access to the content on the iPhone without the assistance of Apple, revealing a weakness in Apple's security features.[97]

---

[88] *A Message to Our Customers*, *supra* note 4.

[89] *Id.*

[90] *Id.*

[91] Order Compelling Apple to Assist, *supra* note 16, at 1.

[92] *Id.*

[93] Benner & Goldstein, *supra* note 23.

[94] David Pierson, *FBI vs. Apple: How Both Sides Were Winners and Losers*, L.A. TIMES (Mar. 29, 2016), http://www.latimes.com/business/technology/la-fi-tn-apple-fbi-explainer-20160329-snap-htmlstory.html.

[95] *Id.*

[96] *Id.*

[97] *Id.*

The government did not reveal how it was able to gain access to the iPhone and likely never will.[98] However, speculation exists that the FBI hired Cellebrite, an Israeli company specializing in digital forensics, to unlock the iPhone.[99]

2. Jun Feng's iPhone

The battle between the FBI and Apple did not end with the case regarding Farook's iPhone. While the FBI dismissed its case against Apple over Farook's iPhone, the FBI still fought against Apple to gain access to another iPhone.[100] That iPhone belonged to Jun Feng, a New York resident who was indicted on charges in connection to a drug conspiracy on July 9, 2014.[101] Similar to Farook's iPhone, ten incorrect passcode attempts to unlock Feng's iPhone would automatically erase all data stored on the device if the auto-erase function was enabled.[102] The government issued a search warrant to search the contents on Feng's iPhone.[103] After Apple failed to comply with the search warrant, the FBI, citing the All Writs Act, asked the court to order Apple to help unlock the device.[104]

In contrast to the Farook case, a federal magistrate judge for the District Court for the Eastern District of New York declined to issue the order without first hearing from Apple.[105] In his brief, Judge Orenstein distinguished Apple from *N.Y. Telephone Co*.[106] In *N.Y. Telephone Co.*, the Supreme Court held that authority granted pursuant to the All Writs Act allowed the Court to issue an order compelling N.Y. Telephone Co. to

---

[98] *Id.*

[99] Steve Morgan, *John McAfee: 'Professional Hackers Did Not Unlock the Shooter's iPhone, Cellebrite Helped the FBI'*, FORBES (Apr. 17, 2016), http://www.forbes.com/sites/stevemorgan/2016/04/17/john-mcafee-professionals-hackers-did-not-unlock-the-shooters-iphone-cellebrite-helped-the-fbi/#111ac58266a0; Jose Pagliery, *Cellebrite Is the FBI's Go-to Phone Hacker*, CNN (Apr. 1, 2016), http://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/; *Source: Israeli Firm Helped FBI Hack San Bernardino Terrorist's iPhone* (NBC television broadcast Mar. 29, 2016).

[100] Devlin Barrett, *Federal Prosecutors Drop Court Case to Force Apple to Unlock iPhone*, WALL ST. J. (Apr. 22, 2016) [hereinafter Barrett, *Federal Prosecutors*], https://www.wsj.com/articles/federal-prosecutors-drop-court-case-to-force-apple-to-unlock-iphone-1461377642.

[101] McCoy, *supra* note 19.

[102] Kevin Collier & William Turton, *Here's Why Apple Will No Longer Unlock Phones for Police*, DAILY DOT (Jan. 23, 2016), http://www.dailydot.com/layer8/apple-unlock-iphone-court/.

[103] Jose Pagliery, *Feds Demand Apple's Help in Unlocking Brooklyn Drug Dealer's iPhone*, CNN (Apr. 8, 2016), http://money.cnn.com/2016/04/08/technology/fbi-iphone-brooklyn/.

[104] *Id.*; McCoy, *supra* note 19.

[105] Frankel, *supra* note 21.

[106] Memorandum & Order at 5, *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 1:15–MC–1902–JO (E.D.N.Y. Oct. 9, 2015), 2015 WL 5920207 at *5.

assist the government with pen registers.[107] Judge Orenstein cited four main differences between that case and Feng's case:

(1) N.Y. Telephone Co. owned the pen registers and had access to the relevant information at its place of business. Apple did not own the device at issue.[108]

(2) N.Y. Telephone Co. provided public services and had a "substantial interest" in aiding law enforcement.[109] The company also had a habit of using pen registers "for its own business purposes."[110] Apple was a private entity, had an interest in protecting its customers' privacy, and did not in its regular course of business access customers' secure data by bypassing security measures.[111]

(3) In *N.Y. Telephone Co.*, law enforcement only had one option by which to obtain the necessary information, which was to have the telephone company install the pen registers and provide law enforcement with the information.[112] Here, the government had not exhausted all other options. The government could have used "coercive contempt sanctions" to procure the phone password from the property owner.[113]

(4) In *N.Y. Telephone Co.*, legislation was consistent with the court's order requiring that the telephone company assist law enforcement in its surveillance.[114] Here, among pleas by the government to enact legislation, Congress had not legislated on this issue.[115] Further, members of Congress had introduced bills to limit the government's power in similar circumstances, showing that Congress is aware of the issue and could legislate if it wanted.[116]

Because the United States District Court for the Eastern District of New York disagreed with the government that *N.Y. Telephone Co.* was applicable to the case at hand, the court requested that Apple weigh in on the matter to decide whether the All Writs Act "permits the relief that the government seeks."[117] Both Apple and the

---

107 United States v. N.Y. Tel. Co., 434 U.S. 159, 160 (1977).

108 Memorandum & Order, *supra* note 106, at 7.

109 *Id.*

110 *Id.*

111 *Id.*

112 *Id.*

113 *Id.*

114 *Id.*

115 *Id.*

116 *Id.* at 8.

117 *Id.* at 10.

government filed briefs that argued their points of view.[118] In a brief filed on October 19, 2015, Apple addressed the issues of "feasibility" and "burden."[119] Apple explained that with each update of its operating system, compliance with an order compelling Apple to bypass security features installed on an iPhone would be increasingly burdensome.[120] Apple designed its security features to protect against all invasions, including those from Apple itself.[121] Further, Apple stated that it was concerned about the public reaction that would accompany Apple's compliance with an order compelling Apple to bypass security features on iPhones.[122]

In its second brief filed on October 23, 2015, Apple argued that the All Writs Act should not provide relief to the government under these circumstances and cited the Communications Assistance for Law Enforcement Act ("CALEA").[123] CALEA requires telecommunications carriers to assist law enforcement by "redesign[ing] their network architectures to make . . . surveillance easier."[124] CALEA does not apply to stored information.[125] Apple noted that Congress could have amended CALEA to apply to stored information on cell phones, but it had not yet done so.[126] Thus, the

---

[118] *See* Frankel, *supra* note 21.

[119] Apple Inc.'s Response to Court's Oct. 9, 2015 Memorandum & Order at 1–4, *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 1:15–MC–1902–JO (E.D.N.Y. Oct. 19, 2015).

[120] *Id.* at 1.

[121] *Id.*

[122] *Id.* at 4. In its argument regarding potential public reaction to a court order compelling Apple to force its way into Feng's iPhone, Apple stated the following:

> [P]ublic sensitivity to issues regarding digital privacy and security is at an unprecedented level. This is true not only with respect to illegal hacking by criminals but also in the area of government access—both disclosed and covert. Apple has taken a leadership role in the protection of its customers' personal data against any form of improper access. Forcing Apple to extract data in this case, absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand.

Id.

[123] Apple Inc.'s Supplemental Response to Court's Oct. 9, 2015 Order & Op. at 2, *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 1:15–MC–1902–JO (E.D.N.Y. Oct. 23, 2015) [hereinafter Apple's Supplemental Response]. In October 1994, Congress enacted CALEA "in response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance." *Communications Assistance for Law Enforcement Act (CALEA),* FED. PRIVACY COUNCIL, https://www.fpc.gov/communications-assistance-for-law-enforcement-calea/; *see* 47 U.S.C. §§ 1001–10 (2014); 47 C.F.R. §§ 1.20000–08 (2006); *Communications Assistance for Law Enforcement Act*, FCC, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance (last updated Oct. 5, 2017).

[124] *FAQ on the CALEA Expansion by the FCC*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/calea-faq#15 (last visited Feb. 11, 2017).

[125] *Id.*; Apple's Supplemental Response, *supra* note 123, at 5.

[126] Apple's Supplemental Response, *supra* note 123, at 5.

government should not be able to use the All Writs Act to give itself power that Congress had failed to grant.[127]

After the court received argumentative briefs from both parties, but before Judge Orenstein ruled on the matter, Jun Feng pleaded guilty to the charges on October 29, 2015.[128] The FBI argued that it still needed access to the phone to assist in its continuing investigation of the conspiracy.[129] Apple sent a letter to Judge Orenstein urging him to decide the question of whether the government could use the All Writs Act to compel Apple to write software that would bypass security features on the device.[130]

In his final ruling issued on February 29, 2016, Judge Orenstein considered various factors such as "the relative closeness of Apple's relationship to the underlying criminal case and government investigation, the burden the requested order would place on the company and the 'necessity of imposing such a burden on Apple.'"[131] He reached the conclusion that "[n]one of those factors justifie[d] imposing on Apple the obligation to assist the government's investigation against the company's will . . . ."[132] The DOJ appealed the Judge's final ruling; however, the DOJ dropped its case against Apple on April 22, 2016 when Jun Feng provided the DOJ with his passcode after he "learned his phone had become an issue in a high-stakes legal fight between prosecutors and Apple."[133]

On March 1, 2016, in the midst of the case regarding Feng's iPhone, the government and Apple testified before the House Judiciary Committee and urged Congress to settle the matter of whether the government can compel technology companies to act under similar circumstances.[134] Employees of the DOJ and Apple were not the only individuals trying to get legislation passed on the issue. Senators Dianne Feinstein and Richard Burr drafted a bill that would impose fines on any company, such as Apple, that fails to comply with a court order to assist law

---

127 *See id.* at 6.

128 Frankel, *supra* note 21; Cyrus Farivar, *After Guilty Plea, Judge Confused as to Why Prosecutors Still Want iPhone Unlocked*, ARS TECHNICA (Oct. 30, 2015), https://arstechnica.com/tech-policy/2015/10/feds-apple-must-still-unlock-iphone-5s-even-after-defendant-pled-guilty/.

129 Spencer Ackerman et al., *Apple Case: Judge Rejects FBI Request for Access to Drug Dealer's iPhone*, GUARDIAN (Feb. 29, 2016), https://www.theguardian.com/technology/2016/feb/29/apple-fbi-case-drug-dealer-iphone-jun-feng-san-bernardino.

130 Frankel, *supra* note 21.

131 McCoy, *supra* note 19; *see* Memorandum & Order at 1, *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016) (No. 1:15–MC–1902–JO).

132 McCoy, *supra* note 19.

133 Barrett, *Federal Prosecutors*, *supra* note 100; *see* Julia Love et al., *U.S. to Continue Appeal of iPhone Data Case in New York*, REUTERS (Apr. 8, 2016), http://www.reuters.com/article/us-apple-encryption-idUSKCN0X51UQ.

134 Benner & Goldstein, *supra* note 23.

enforcement in decrypting data on cellphones.[135] However, the bill died before reaching the Senate.[136] On the other side of the issue, Representative Mike McCaul and Senator Mark Warner were attempting to put together a commission of experts to determine the potential effects of encryption legislation.[137] Regardless of the efforts being made to legislate the matter, Congress has not yet settled the debate.[138] Until then, the war over encryption will rage on.[139]

C. Other Legal Battles over Data Access

Apple was not the only technology company involved in legal controversies with law enforcement over access to data.[140] In 2014, the government obtained a search warrant pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. § 2703, that compelled Microsoft to release data stored on a Microsoft server located in Dublin, Ireland in relation to a drug trafficking case.[141] The United States District Court for the Southern District of New York held Microsoft in contempt of court after Microsoft

---

[135] Levi Sumagaysay, *Apple vs. FBI: A Look at Proposed Laws on Phones and Encryption*, SILICONBEAT (Mar. 10, 2016), http://www.siliconbeat.com/2016/03/10/apple-vs-fbi-look-proposed-laws-phones-encryption/?doing_wp_cron=1486758699.1264860630035400390625; Dustin Volz & Mark Hosenball, *Senators Close to Finishing Encryption Penalties Legislation: Sources*, REUTERS (Mar. 9, 2016), http://www.reuters.com/article/us-apple-encryption-legislation-idUSKCN0WB2QC.

[136] Shara Tibken, *Apple vs. FBI One Year Later: Still Stuck in Limbo*, CNET (Feb. 15, 2017), https://www.cnet.com/news/apple-vs-fbi-one-year-later-still-stuck-in-limbo/.

[137] Brian Barrett, *The Apple-FBI Battle Is Over, but the New Crypto Wars Have Just Begun*, WIRED (Mar. 30, 2016), https://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/; Volz & Hosenball, *supra* note 135.

[138] *See* Tibken, *supra* note 136.

[139] Joseph Marks, *The Encryption Wars Will Return One Way or Another*, NEXTGOV (Jan. 23, 2017), http://www.nextgov.com/cybersecurity/2017/01/encryption-wars-will-return-one-way-or-another/134802/.

[140] Tibken, *supra* note 136.

[141] Joon Ian Wong, *Microsoft's Win over the US Government Is a Rare Moment of Clarity Around Global Data Laws*, QUARTZ (July 18, 2016), https://qz.com/733538/microsofts-win-over-the-us-government-is-a-rare-moment-of-clarity-around-global-data-laws/. 18 U.S.C. § 2703 provides in relevant part the following:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

18 U.S.C. § 2703(a) (2009).

failed to comply with the request.[142] Microsoft appealed the district court's decision to the United States Court of Appeals for the Second Circuit.[143] On appeal, Microsoft argued that "the DOJ . . . exceeded its authority with potentially dangerous consequences."[144] Amicus briefs filed by entities such as Apple, Fox News, NPR, the Guardian, and the government of Ireland argued, "the case could set a precedent for governments around the world to seize information held in the cloud."[145] However, the United States government argued that it had "the right to demand the emails of anyone in the world from any email provider headquartered within US borders . . . ."[146] On July 14, 2016, the United States Court of Appeals for the Second Circuit decided the case in favor of Microsoft.[147] The Court of Appeals concluded:

> Congress did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States.[148]

Regarding the court's decision, Microsoft stated that:

> The decision is important for three reasons: it ensures that people's privacy rights are protected by the laws of their own countries; it helps ensure that the legal protections of the physical world apply in the digital domain; and it paves the way for better solutions to address both privacy and law enforcement needs.[149]

Following the Microsoft decision, a federal magistrate judge ordered Google to comply with a search warrant that requested emails stored outside of the country.[150]

---

[142] Microsoft Corp. v. United States, 829 F.3d 197, 201–02 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (2017) (No. 17–2; set for argument on Feb. 27, 2018).

[143] *Id.*

[144] Sam Thielman, *Microsoft Case: DoJ Says It Can Demand Every Email from Any US-Based Provider*, GUARDIAN (Sept. 9, 2015), https://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant.

[145] *Id.*

[146] *Id.*

[147] *Microsoft Corp.*, 829 F.3d at 201–02.

[148] *Id.* at 222.

[149] Brad Smith, *Our Search Warrant Case: An Important Decision for People Everywhere*, MICROSOFT (July 14, 2016), https://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#sm.0001y50mmsftseaxyiq233trt2lq0.

[150] Natasha Lomas, *Google Told to Hand Over Foreign Emails in FBI Search Warrant Ruling*, TECHCRUNCH (Feb. 4, 2017), https://techcrunch.com/2017/02/04/google-told-to-hand-over-foreign-emails-in-fbi-search-warrant-ruling/.

The government obtained the search warrants in August 2016.[151] The search warrants requested that Google release electronic information to the government in connection with two criminal investigations.[152] Google handed over data that was stored on its servers inside the country.[153] As to the other emails requested, Google stated that it could not know where the emails were located.[154] The district court, relying on Google's stipulations, described Google's data system as follows:

> Google stores user data in various locations, some of which are in the United States and some of which are in countries outside the United States. Some user files may be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time. Google operates a state-of-the-art intelligent network that, with respect to some types of data, including some of the data at issue in this case, automatically moves data from one location on Google's network to another as frequently as needed to optimize for performance, reliability, and other efficiencies. As a result, the country or countries in which specific user data, or components of that data, is located may change. It is possible that the network will change the location of data between the time when the legal process is sought and when it is served. As such, Google contends that it does not currently have the capability, for all of its services, to determine the location of the data and produce that data to a human user at any particular point in time.[155]

Therefore, Google argued that it did not have to comply with the search warrants and cited *Microsoft* in support of its position.[156] However, the United States District Court for the Eastern District of Pennsylvania rejected the holding in *Microsoft*.[157] The court held "that the disclosure by Google of the electronic data relevant to the warrants at issue here constitute[d] neither a 'seizure' nor a 'search' of the targets' data in a foreign country."[158] The court stated that the "conduct relevant to the SCA's focus will occur in the United States."[159] Therefore, these cases presented "a permissible domestic application of the SCA, even if other conduct (the electronic transfer of data) occurs abroad," and the court ordered Google to comply with the search warrants.[160]

---

[151] *In re* Search Warrant No. 16–960–M–01 to Google, 232 F. Supp. 3d 708, 709 (E.D. Pa. 2017) [hereinafter *In re* Google].

[152] *Id.*

[153] Orin Kerr, *Google Must Turn Over Foreign-Stored Emails Pursuant to a Warrant, Court Rules*, WASH. POST (Feb. 3, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/03/google-must-turn-over-foreign-stored-e-mails-pursuant-to-a-warrant-court-rules/?utm_term=.7cc97e5ef299.

[154] *Id.*

[155] *In re* Google, 232 F. Supp. 3d at 712 (internal citations omitted).

[156] *Id.* at 709–10.

[157] *Id.* at 713 (internal citations omitted).

[158] *Id.*

[159] *Id.* at 722.

[160] *Id.* at 722, 725.

The differences in the outcomes of *Microsoft* and the Google case further illustrate the importance of Congressional action on matters involving electronic data. Law enforcement has also requested that Amazon hand over Echo smart speaker recordings in relation to a murder in Arkansas.[161] The amount of government requests for data information has increased in the past few years, shedding even more light on the growing tension between the government and technology companies.[162]

IV. CONGRESS MUST ENACT LEGISLATION ADDRESSING THE LIMITS OF THE GOVERNMENT'S POWER OVER TECHNOLOGY COMPANIES IN ORDER TO PROMOTE EFFICIENCY, PREDICTABILITY, AND UNIFORMITY IN THE LAW

Because neither Congress nor the Supreme Court has answered the question of how far the government and law enforcement agencies are able to go in compelling technology companies to assist in investigations, the cases regarding this issue are unpredictable. When an issue involving data encryption reaches the court, it is unclear whether the court will issue an order compelling a company to assist the government

---

[161] Tibken, *supra* note 136. The Amazon Echo speaker "is a hands-free, voice-controlled device that uses Alexa to play music, control smart home devices, provide information, read the news, set alarms, read audiobooks from Audible, and more." *Echo Dot (2nd Generation)—Black*, AMAZON, https://www.amazon.com/All-New-Amazon-Echo-Dot-Add-Alexa-To-Any-Room/dp/B01DFKC2SO (last visited Apr. 28, 2017). When Amazon Echo is in use, it records pieces of conversation. *Amazon Echo Murder Case Renews Privacy Questions Prompted by Our Digital Footprints*, NPR (Dec. 31, 2016), http://www.npr.org/2016/12/31/507670072/amazon-echo-murder-case-renews-privacy-questions-prompted-by-our-digital-footpri. When Echo records bits of conversation, it sends the recording to an Amazon server. *Id.* When law enforcement requested that Amazon hand over the recordings, Amazon refused and filed a motion to quash the search warrant due to First Amendment and privacy rights. Eliott C. McLaughlin, *Suspect OKs Amazon to Hand Over Echo Recordings in Murder Case*, CNN (Apr. 26, 2017), http://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/. However, the court did not have to rule on the motion because the suspect in the murder investigation gave his consent to have the recordings released to the government. *Id.*

[162] Steve Dent, *Reddit Law Enforcement Requests Have Tripled in Two Years*, ENGADGET (Apr. 4, 2017), https://www.engadget.com/2017/04/04/reddit-law-enforcement-requests-have-tripled-in-two-years/; Laura Hautala, *Facebook: Law Enforcement Requests for User Data Up 9 Percent*, CNET (Apr. 27, 2017), https://www.cnet.com/news/facebook-law-enforcement-requests-for-user-data-up-9/; Sooraj Shah, *Microsoft Reveals that US Government Data Requests Have Doubled*, INQUIRER (Apr. 19, 2017), http://www.theinquirer.net/inquirer/news/3008555/microsoft-reveals-that-us-government-data-requests-have-doubled. Most companies and social media services publish "transparency reports" detailing the number of government requests that they receive each year for electronic data and information and the number of requests in which the company or service provided data to the government. *Government Requests Report*, FACEBOOK, https://govtrequests.facebook.com/ (last visited Apr. 28, 2017); *Transparency Report: Information Requests*, TWITTER, https://transparency.twitter.com/en/information-requests.html (last visited Nov. 25, 2017); *Report History*, APPLE, https://www.apple.com/privacy/transparency-reports/ (last updated Apr. 14, 2017); *Transparency Report*, UBER, https://transparencyreport.uber.com/ (last visited Apr. 28, 2017); *Verizon's Transparency Report for the 2nd Half of 2016*, VERIZON, http://www.verizon.com/about/portal/transparency-report/ (last visited Apr. 28, 2017).

in hacking a device.[163] In the two recent cases involving the FBI and Apple, the United States District Court for the Southern District of New York and the United States District Court for the Central District of California reached opposite conclusions on the issue.[164] A magistrate judge for the United States District Court for the Southern District of New York denied the FBI's request for a court order after asking Apple to weigh in on the matter.[165] In stark contrast, a magistrate judge for the United States District Court for the Central District of California issued a court order without first allowing Apple to plead its case.[166]

What the United States District Court for the Central District of California considered in reaching its decision to issue the court order is unclear.[167] Moreover, the law in districts where this issue has not yet surfaced also is unclear. A technology company might be compelled to hack into a device to assist law enforcement if the judge issuing the order sides with encryption legislation. However, if a judge's personal view is that data encryption should remain intact, then that judge might deny a request to issue such a court order. A court may not have any rhyme or reason as to whether it will issue an order compelling a technology company to assist law enforcement or the government in hacking into locked devices. The outcome of cases that set the government at odds with technology companies might be based on which judge hears the case or in which district the court is located. This unpredictability is a problem because neither party knows what to expect. This issue is highly debated nationwide and has been gaining momentum; therefore, it warrants federal legislation.[168]

If the legislature does not step in and solve the problem, the issue may eventually reach the judiciary. This is the case for the issue in *Microsoft*, as the Supreme Court recently granted certiorari.[169] *Microsoft* raises the issue of government access to consumer data that is stored overseas, which is just one gap in the legislation regarding government access to data and individual privacy rights. The outcome of this case may fill in that tiny gap in legislation, but will not speak to the issue of whether the government and law enforcement agencies can compel companies to modify or create programming to assist in access to encrypted data. When, or even if, appeals from other cases involving the government and technology companies will reach the Supreme Court is not clear.[170] The lack of indication of when such an appeal would reach the Supreme Court results from the FBI dropping its cases against Apple as soon as it gains access to the devices in question.[171] Even if an appeal did reach the Supreme

---

163 McCoy, *supra* note 19.

164 *See* Order Compelling Apple to Assist, *supra* note 16, at 1; McCoy, *supra* note 19.

165 Frankel, *supra* note 21.

166 Order Compelling Apple to Assist, *supra* note 16, at 1.

167 *See id.* at 1–3.

168 *See, e.g.*, Hack, *supra* note 63; Lachance, *supra* note 35.

169 Microsoft Corp. v. United States, 829 F.3d 197, 201–02 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (2017) (No. 17–2; set for argument on Feb. 27, 2018).

170 *See* McCoy, *supra* note 19.

171 *US Government Drops Another iPhone Case Against Apple*, BBC NEWS (Apr. 26, 2016), http://www.bbc.com/news/technology-36139981.

Court, the Court may or may not grant certiorari to hear the case.[172] Meanwhile, precious resources such as time and money are being used in litigation and problem solving. Moreover, the government and technology companies will continue to exhaust resources in litigating these matters until either Congress legislates or the Supreme Court decides a case on the issue. District courts will continue to be bogged down with cases regarding access to locked devices, stealing time and attention away from other important matters.

Because Apple and other technology companies would have to expend resources to hack into locked devices, they should know what they are legally obligated to do. Federal legislation setting out a hard and fast rule defining what the government can and cannot force a technology company to do to gain access to content on locked devices would create predictability and uniformity in the law. Technology companies would be better prepared to take on their legal obligations if they knew what to expect ahead of time. If the Supreme Court decides that the government can force technology companies into writing or modifying programming, technology companies would need to prepare resources to comply.[173] For example, creating a backdoor would take the work of "six to ten Apple engineers and employees dedicating a very substantial portion of their time."[174] This issue must be handled uniformly, predictably, and with efficiency, which is why it calls for Congress's immediate attention.

A. Legislation that Prevents the Creation of a Backdoor Will Protect, Rather than Harm, National Security

The FBI attempted to compel Apple to create a backdoor into its iPhone so that the FBI could gain access to personal information contained on the device to protect national security.[175] However, the government's reasoning had a fatal flaw. The very act of creating the backdoor undermines national security because it creates a vulnerability in data security.[176] The backdoor is analogous to a dangerous weapon. Apple explained that the creation of an operating system is unlike the creation of something tangible.[177] Once created, the operating system cannot be destroyed.[178] In regard to the creation of the backdoor, Apple stated, "[we] would do our best to protect

---

[172] The Supreme Court only grants certiorari in a small percentage of cases. *Supreme Court Procedures*, U.S. COURTS, http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/supreme-1. One reason the Supreme Court may deny to hear a case is if it considers the matter nonjusticiable. *See Political Question Doctrine*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/political_question_doctrine, (last visited Feb. 13, 2018). For example, the Supreme Court may decide that the matter presents a political question—a question that is best resolved by one of the coordinate branches of government. *Id.*

[173] *See* Jose Pagliery, *Here's What It Would Cost Apple to Help the FBI Hack an iPhone*, CNN (Feb. 28, 2016) [hereinafter Pagliery, *Here's What It Would Cost Apple*], http://money.cnn.com/2016/02/26/technology/apple-iphone-fbi-hack-cost/.

[174] *Id.*

[175] Kharpal, *supra* note 26.

[176] *See id.*; *see also Answers to Your Questions About Apple and Security*, *supra* note 24.

[177] *See Answers to Your Questions About Apple and Security*, *supra* note 24.

[178] *See id.*

that key, but in a world where all of our data is under constant threat, it would be relentlessly attacked by hackers and cybercriminals."[179] Further, any individual or entity would be vulnerable to such an attack.[180]

In January 2017, Cellebrite, the company that allegedly provided the hack to the FBI to gain access to Farook's iPhone, was itself a victim of a hack.[181] The hackers sent "customer information, databases, and a vast amount of technical data regarding Cellebrite's products" to Motherboard, a website for technology and science publications.[182] Cellebrite is not the only hacking company that has been the victim of a cybercrime. In 2015, a hacker known as Phineas Fisher gained access to the servers of Hacking Team, an Italian hacking company, and "took everything there was to take, laying bare all the company's secrets, including its once closely-held list of customers."[183] The hack on Cellebrite appeared to be connected to the hack that Cellebrite provided to the FBI as a means of bypassing security features on Farook's iPhone.[184] In an online chat, the hacker made the following statement to Motherboard:

> The debate around backdoors is not going to go away, rather, its [sic] is almost certainly going to get more intense as we lurch toward a more authoritarian society . . . . It's important to demonstrate that when you create these tools, they will make it out. History should make that clear . . . .[185]

The hack on Cellebrite is a perfect example of the dangers lurking behind the creation of a backdoor. Even companies whose purpose of business is to provide hacking tools are not protected from being hacked themselves.[186] Apple would struggle to protect the backdoor if created.[187] Further, if Apple were compelled to create a backdoor and this became precedent, law enforcement agencies around the country would seek access to the backdoor. It would only be a matter of time before the backdoor found its way into the wrong hands.

Another shortcoming in the argument for legislation prohibiting technology companies from failing to comply with court orders to hack into devices is that it fails

---

179 *Id.*

180 *See id.*

181 Joseph Cox, *Hacker Steals 900 GB of Cellebrite Data*, MOTHERBOARD (Jan. 12, 2017), https://motherboard.vice.com/en_us/article/hacker-steals-900-gb-of-cellebrite-data.

182 *Id.*; *see About Motherboard*, MOTHERBOARD, https://motherboard.vice.com/en_us/page/about-motherboard (last visited Feb. 14, 2017).

183 Lorenzo Franceschi-Bicchierai, *The Vigilante Who Hacked Hacking Team Explains How He Did It*, MOTHERBOARD (Apr. 15, 2016), https://motherboard.vice.com/en_us/article/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it.

184 *See* Joseph Cox, *Hacker Dumps iOS Cracking Tools Allegedly Stolen from Cellebrite*, MOTHERBOARD (Feb. 2, 2017), https://motherboard.vice.com/en_us/article/hacker-dumps-ios-cracking-tools-allegedly-stolen-from-cellebrite.

185 *Id.* (quoting the hacker responsible for the public release of a cache of files allegedly stolen from Cellebrite).

186 *See id.*

187 *See Answers to Your Questions About Apple and Security*, *supra* note 24.

to consider actions taken in response to the legislation. If the Supreme Court sets precedent or Congress enacts legislation compelling technology companies to assist the government in hacking devices, criminals will take steps to ensure that no evidence is available for law enforcement to discover.[188] Criminals will erase data stored on devices, use burner phones,[189] or dispose of their devices before committing an illegal act. Another problem Apple foresees is that "[c]riminals and bad actors will still encrypt, using tools that are readily available to them."[190] Therefore, this precedent or legislation would not help protect national security, but rather, "would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data."[191]

Until Congress writes legislation creating a concrete rule, the legal battles between law enforcement agencies and technology companies will continue. The unpredictability of this issue leaves the population uncomfortable, with a sense that personal information is no longer protected.[192] These legal battles have already had ramifications. Technology companies such as Apple, Facebook, and WhatsApp have been upgrading their security features to make it nearly impossible for data to be hacked.[193]

However, the proposed law will not change the fact that agencies still must comply with valid search warrants. Upon a showing of probable cause, law enforcement agencies will still be able to obtain search warrants authorized by a court to allow them to order technology companies to release all information in their control, possession, or both.[194] In this respect, law enforcement still has the means to protect national security. The government and law enforcement agencies will continue to have access to important information, by way of a search warrant or court order, to further criminal investigations and prove an individual's criminal activity in a court of law.[195] For example, Apple provided the FBI with all data that Farook had backed up to his iCloud

---

188 Marc Saltzman, *Why You Might Want to Own a 'Burner Phone'*, USA TODAY (Sept. 17, 2016), http://www.usatoday.com/story/tech/columnist/saltzman/2016/09/17/whats-a-burner-phone/90382874/.

189 "Burner phones can be bought with cash and with no contract, plus providers that sell these devices don't track personal data." *Id.*

190 *A Message to Our Customers*, *supra* note 4.

191 *Id.*

192 *Id.*

193 *See* Matt Apuzzo & Katie Benner, *Apple Is Said to Be Trying to Make It Harder to Hack iPhones*, N.Y. TIMES (Feb. 24, 2016), https://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html; Zach Epstein, *The FBI's Worst Nightmare Is Coming True*, BGR (Mar. 15, 2016), http://bgr.com/2016/03/15/fbi-vs-apple-encryption-strengthening-oops/.

194 *See* Lomas, *supra* note 150.

195 *See* Lichtblau & Benner, *supra* note 7.

account from his iPhone.[196] Apple obtained this information from its iCloud servers.[197] The data provided important information to the FBI; it "showed that Farook was in communication with individuals who were later killed."[198] While the proposed law would block the government from forcing companies to create backdoors into their devices, the government still would retain the means to obtain crucial information from companies. Further, the law would protect national security by continuing to protect encrypted data.

B. Law that Allows the Government to Force Technology Companies to Write Programming Violates Constitutional Rights

If the government succeeds in forcing Apple or any technology company to create backdoor programming, this type of order would violate companies' and customers' First, Fourth, and Fifth Amendment rights under the United States Constitution.[199] In its fight against the government, Apple argued that forcing the company to write programming would violate its First Amendment right to freedom of speech.[200] The right to freedom of speech includes the right not to be forced to say something.[201] Apple argued that well-settled law had "established code as free speech within the context of the First Amendment."[202] The court order, which would force Apple to "cryptographically 'sign' any software it creates," would essentially "amount[] to compelled speech and viewpoint discrimination in violation of the First Amendment."[203]

Apple further argued that a court order compelling it to create programming would violate its Fifth Amendment right to due process of law.[204] Forcing the company to create programming would be "highly burdensome, and contrary to the party's core

---

196 Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.04475ae11d8b.

197 *Id.*

198 *Id.*

199 *E.g.*, Ron Fein, *How Apple Could Best the FBI*, U.S. NEWS (Feb. 22, 2016), www.usnews.com/opinion/articles/2016-02-22/apple-may-not-have-a-right-to-privacy-but-its-iphone-customers-do; Christina Sterbenz, *Apple Is Using 2 Main Arguments in Its Epic Fight Against the FBI*, BUS. INSIDER (Feb. 25, 2016), www.businessinsider.com/apple-using-first-and-fifth-amendment-2016-2.

200 *See* sources cited *supra* note 199. The First Amendment of the United States Constitution states, in relevant part, "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ." U.S. CONST. amend. I.

201 West Virginia Bd. of Educ. v. Barnette, 319 U.S. 624, 634, 636–37 (1943) (holding that the right not to speak was protected by the First Amendment).

202 Sterbenz, *supra* note 199.

203 *Id.*

204 *Id.* The Fifth Amendment of the United States Constitution states, in relevant part, "No person . . . shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; . . . ." U.S. CONST. amend. V.

principles . . . ."[205] Further, forcing Apple to write programming for the government would violate "Apple's substantive due process right to be free from the 'arbitrary deprivation of [its] liberties.'"[206]

Additionally, a court order would violate Apple's consumers' Fourth Amendment right to privacy.[207] If the government could force Apple to create a backdoor, weakening its security features, it would "compromise the privacy of people who aren't even involved in the case . . . ."[208] Individuals have a right to encrypt their data and to be provided protections from companies that will keep that data protected from hackers and cybercriminals.[209] The proposed law would protect the privacy rights of innocent individuals. Further, citizens would have peace of mind that their personal information is protected against an increased risk of hacks. Compelling a technology company to create a "key" or backdoor to its security features undermines the effort that the company has put into securing the personal information of its customer base. Thus, the proposed law would protect individuals against violations of their First, Fourth, and Fifth Amendment rights.

C. Legislation Restricting the Government's Power Would Keep Big Brother at Bay

The backdoor is not only dangerous if placed in the hands of criminals or hackers, but also because the government could exploit it. In the Farook case, the FBI argued that the backdoor would be used only in that particular instance; however, Apple argued that "there [was] no way to guarantee such control."[210] In other words, Apple would have no way to ensure that the government would not abuse the "key" by exploiting the tool for matters unrelated to the Farook case.[211] Apple stated:

> If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.[212]

While the question remained whether Farook's actions were tied to terrorist activity[213] directly affecting our national security, not all criminal cases involving locked devices are threatening to the security of our nation. A judgment in favor of the FBI could create a slippery slope. Law enforcement around the country would use

---

[205] Sterbenz, *supra* note 199.

[206] *Id.* (quoting Apple's attorneys).

[207] *See* Fein, *supra* note 199.

[208] *Id.*

[209] *A Message to Our Customers*, *supra* note 4.

[210] *Id.*

[211] *See id.*

[212] *Id.*

[213] *But see* Pete Williams & Halimah Abdullah, *FBI: San Bernardino Shooters Radicalized Before They Met*, NBC NEWS (Dec. 9, 2015), https://www.nbcnews.com/storyline/san-bernardino-shooting/fbi-san-bernardino-shooters-radicalized-they-met-n476971.

this precedent to compel Apple and other technology companies to hack into locked devices in connection to any criminal case law enforcement is investigating, not just those cases that put our national security in jeopardy. In regard to a homicide investigation, the district attorney of Baton Rouge stated that "[i]t just doesn't seem fair" in response to Apple's answer that it could not obtain all data from a locked device.[214] The district attorney of San Bernardino County also thought that Apple should be compelled to assist the government to gain access to iPhones "for certain kinds of investigations," such as homicide and missing persons investigations.[215]

A similar problem would exist if Congress enacts legislation compelling companies to comply with court orders to assist law enforcement by hacking into phones. Law enforcement would cite that act to compel technology companies to hack into all locked devices. Even if Congress did set parameters for the rule, law enforcement would try to stretch the rule to apply to all situations regardless of the gravity of the issue. For example, consider a situation where Congress passed a bill into law that states technology companies must comply with court orders to hack into devices when national security is at risk. Law enforcement agencies will make the argument that national security is at risk in every case that involves a locked device. Congress would have difficulty explaining under what circumstances our national security is at risk versus circumstances that would not suggest that our national security is at risk. It would be hard to say whether the security of our nation is at risk if we do not have access to certain information. Therefore, law enforcement would argue that the security of our nation could be in jeopardy in most cases. Where would Congress draw the line? To ensure protection against governmental abuse of power, Congress should prohibit the government from compelling technology companies to write programming to hack into locked devices with no exceptions.

D. The Costs Associated with Creating a Backdoor Outweigh the Benefits

If the FBI won its case against Apple, Apple would need to spend over one hundred thousand dollars in labor costs alone to rewrite its security programming.[216] Apple also estimated that it would take anywhere from two to four weeks to create the backdoor.[217] One could argue that the cost to Apple in creating the backdoor is less than the cost to the government in hacking an iPhone without the help of Apple. For example, according to one source, the government paid over one million dollars to a third party to hack Farook's iPhone.[218] Further, the government pledged to Apple that it would pay for the monetary costs associated with reworking the software.[219]

---

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

[215] *Id.*

[216] Pagliery, *Here's What It Would Cost Apple*, *supra* note 173. In regard to creating a backdoor, Apple stated, "the effort would take 'six to ten Apple engineers and employees dedicating a very substantial portion of their time.'" *Id.*

[217] *Id.*

[218] Edwards, *supra* note 18.

[219] *See* Pagliery, *Here's What It Would Cost Apple, supra* note 173.

However, this argument fails to look at other costs associated with creating the backdoor.

Once Apple creates the backdoor, Apple would "'likely' build 'one or two secure facilities' similar to a 'Sensitive Compartmented Information Facility'" to protect the hack from being leaked.[220] Apple also stated that it would "spend 'additional time' destroying every line of code in [the hack]—and closely guarding any logs that led to its creation."[221] Apple would repeat this effort in every future case in which Apple is ordered to hack into an iPhone.[222] Former FBI Director James Comey stated that a judgment in the FBI's favor could serve as precedent in the future to compel companies to assist the government in hacking into phones.[223] According to a survey, law enforcement cannot gain access to potential evidence on over one thousand locked devices.[224] In Manhattan alone, the district attorney would use this precedent to have Apple unlock devices in connection with almost two hundred criminal cases.[225]

The government would argue that expending these resources is necessary to protect national security. However, one cannot say with certainty that unlocking a device in question will lead to evidence. While unlocking a device may uncover evidence, the possibility exists that the phone contains nothing worth discovering. After spending $1.3 million to hack Farook's iPhone, the FBI did not gain much more insight into the case.[226] The phone lacked "evidence of contacts with other ISIS supporters or the use of encrypted communications during the period the FBI was concerned about."[227] Further, the FBI still has questions regarding the incident that "remain[] unsolved."[228]

Also, if Apple were to create a backdoor, the company's reputation likely would suffer significant damage.[229] Apple consumers would no longer trust the company's

---

220 *Id.* (quoting Apple lawyer Lisa Olle).

221 *Id.*

222 *See id.*

223 *See* Mark Berman & Ellen Nakashima, *FBI Director: Victory in the Fight with Apple Could Set a Precedent, Lead to More Requests*, WASH. POST (Mar. 1, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/03/01/fbi-apple-bringing-fight-over-encryption-to-capitol-hill/?utm_term=.65cb402fb966.

224 Kevin Johnson & Elizabeth Weise, *1,000 Locked Devices in Limbo After FBI Quits iPhone Case*, USA TODAY (Mar. 30, 2016), http://www.usatoday.com/story/tech/news/2016/03/29/fbi-withdrawal-apple-iphone-farook-brooklyn-locked-encryption-case-san-bernardino/82378416/.

225 Pagliery, *Here's What It Would Cost Apple*, *supra* note 173.

226 Edwards, *supra* note 18; *see* Evan Perez et al., *Sources: Data from San Bernardino Phone Has Helped in Probe*, CNN (Apr. 20, 2016), http://www.cnn.com/2016/04/19/politics/san-bernadino-iphone-data/.

227 Perez et al., *supra* note 226.

228 *Id.*

229 Alina Selyukh & Camila Domonoske, *Apple, the FBI and iPhone Encryption: A Look at What's at Stake*, NPR (Feb. 17, 2016), https://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake.

promise of protection, and the company would lose consumers as a result.[230] Foreign corporations, as well as United States consumers, would no longer buy a device from a technology company such as Apple that has a backdoor.[231] Instead, consumers would buy from technology companies outside of the United States.[232]

V. PROPOSED LAW PROHIBITING THE GOVERNMENT FROM FORCING TECHNOLOGY COMPANIES TO GAIN ACCESS TO ENCRYPTED DATA BY CREATING BACKDOORS INTO THEIR DEVICES

Congress should enact legislation limiting the government's power over technology companies. The proposed legislation would prevent the government and law enforcement agencies from using the All Writs Act as a catchall, giving them the power to force companies to do that which Congress has not given them the power to do. This law would prohibit the government and law enforcement agencies from compelling technology companies to modify or create software, which would weaken their security features allowing law enforcement to gain access into an individual's locked device. The government would not have authority to force companies to create backdoors into their devices that would undermine the company's security efforts. However, this law should not deprive technology companies of the right to aid the government or law enforcement in investigations in which threats to national security or public safety exist. This law would only allow the government and law enforcement agencies to provide reasonable compensation to companies in exchange for their services, thus banning companies from selling backdoors or hacks into data security systems.

The proposed legislation would contain four main components. The first component is a requirement that all companies that provide data services must provide data security to their customers. This would also require technology companies to comply with legal court orders. The second component would prohibit the government and law enforcement agencies from forcing data service providers to provide technological assistance by way of creating or modifying programming. The third component would give permission to data service providers to provide such technological assistance to law enforcement or the government to aid in law investigations in which a present danger to national security or public safety exists. The fourth and final component would be a requirement that the government and law enforcement agencies provide reasonable compensation in exchange for any technological assistance that is given to them, but no more than what is reasonable for the services.

A. Legislation Should Include a Statement that Data Service Providers Shall Provide Security, but also Comply with Legal Court Orders

The proposed legislation would acknowledge that data service providers should first and foremost provide security to their customers, but that they must also comply with all legal court orders. To be in compliance with a court order requesting information, a data service provider shall provide requested information that the

---

230 *See id.*

231 *See* Todd Bell, *Apple vs. FBI: The Economics of Back Doors*, CSO (Feb. 24, 2016), http://www.csoonline.com/article/3036779/security/the-economics-of-backdoors.html.

232 *See id.*

company has within its control or possession. The request may encompass user account information, which can include the name and address of the individual associated with the account, and documents, contacts, calendars, and other information stored on the account if the company can access the account through its servers.[233]

For example, this section could state:

> [A]ll providers of communications services and products (including software) should protect the privacy of United States persons through implementation of appropriate data security and still respect the rule of law and comply with all legal requirements and court orders; . . . to uphold both the rule of law and protect the interests and security of the United States, all persons receiving an authorized judicial order for information or data must provide, in a timely manner, responsive . . . information or data [that the provider has in its control or possession] . . . .[234]

B. Legislation Should Prohibit the Government and Law Enforcement Agencies from Forcing Technology Companies to Provide Technological Assistance in the Form of Created or Modified Programming

The most important component of the proposed legislation is the prohibition of the government and law enforcement agencies from compelling a data service provider to create a backdoor to its devices. This section would prohibit the government and law enforcement agencies from forcing companies to modify or create programming to bypass security features on their devices. This restriction would contain no exceptions. Under no circumstances should the government or law enforcement agencies be permitted to force companies to provide this specific technological assistance. If an exception were written into the proposed legislation, the government would attempt to shoehorn all circumstances into the exception; thus, to allow one exception would be a slippery slope. The following is an example of language for this section of the proposed legislation:

> The government and law enforcement agencies, in seeking a court order to compel a data service provider to render information valuable to an ongoing

---

[233] *Report on Government Information Requests*, APPLE (Jan.–June 2016) https://images.apple.com/legal/privacy/transparency/requests-2016-H1-en.pdf; *Transparency Report*, APPLE, https://www.apple.com/privacy/government-information-requests/ (last visited Apr. 22, 2017).

[234] Compliance with Court Orders Act of 2016, 114th Cong. § 1–4 (2016), https://www.eff.org/document/burr-feinstein-encryption-bill-discussion-draft. The quoted language is borrowed from the Burr-Feinstein Encryption Bill Discussion Draft, referred to in the bill as the Compliance with Court Orders Act of 2016, a bill drafted by Senators Richard M. Burr (R–N.C.) and Dianne Feinstein (D–Cal.) that would require all technology companies to provide technological assistance in response to a court order if enacted. Although language is borrowed from this bill for the proposed legislation, the proposed legislation would do the opposite, barring the government from compelling companies to provide technological assistance. *See Intelligence Committee Leaders Release Discussion Draft of Encryption Bill*, U.S. SEN. FOR CAL. DIANNE FEINSTEIN (Apr. 13, 2016) https://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649.

> investigation, shall not compel a data service provider to modify or create programming in order to provide comprehensible information.

This language is merely one example, as there are many other ways in which the text of the proposed legislation could prohibit the government and law enforcement from forcing companies to breach their own security.

C. Legislation Should Give Technology Companies the Option to Provide Technological Assistance to the Government or Law Enforcement

While the basis for the proposed legislation is that the government and law enforcement cannot, under any circumstances, compel technology companies to create or modify programming, the legislation would not prohibit technology companies from providing assistance to the government or law enforcement per se. The proposed legislation would give data service providers the option to provide technological assistance to aid the government or law enforcement in investigations in which national security and public safety are threatened. In investigations in which the immediate threat has been neutralized and investigators have little reason to suspect an ongoing threat to public safety or national security, the proposed legislation would prohibit technology companies from assisting the government or law enforcement by creating a backdoor to their systems. This limited permissiveness would provide a balance between national security and the privacy rights of citizens. This section could read as follows:

> This Act shall not preclude providers of communications services and products from providing technical assistance, by way of creating or modifying programming, to aid law enforcement or government investigations in which there is an ongoing, perceived threat to national security or public safety.

D. Requirement of the Government to Provide Reasonable Compensation to a Company in Exchange for Technological Assistance and Prohibition of Technology Companies from Selling Hacks or Backdoors

The fourth and final component of the proposed legislation is a requirement that the government or law enforcement agencies provide reasonable compensation to any technology company that provides technological assistance to aid in an investigation. This piece of the proposed legislation would also ban companies from selling their hacking services to the government or law enforcement agencies. If a technology company decides to provide technological assistance to the government or law enforcement to assist them in an investigation, the technology company would only be able to receive reasonable compensation in exchange for their services. This restriction would deter companies from creating hacks or backdoors to security systems for pecuniary gain. In deciding whether to provide technological assistance to aid an investigation in which national security or public safety is threatened, a company would be less likely to use personal gain as a motivating factor. Rather, the company would be left to weigh only competing interests such as citizens' Constitutional rights, national security, and public safety. As an example, this section of the proposed legislation could state the following:

> In the event that a provider of communications services or products provides technical assistance in response to a request from a government or law enforcement agency, the entity requesting such information shall

compensate the provider "for such costs as are reasonably necessary and which have been directly incurred in providing such technical assistance or such data in an intelligible format."[235]

VI. CONCLUSION

Recent legal battles between the government and technology companies reveal a problem with the gap in legislation regarding what the government and law enforcement agencies can and cannot force technology companies to do as a means of gaining access to encrypted data on locked devices. While the government is attempting to broaden its access to information, the concern over privacy rights and national security increases. Citizens are increasingly aware of the vast information to which the government already has access.[236] Recently, the government has sought court orders from districts courts to compel technology companies to write or rewrite programming to bypass security features on locked devices.[237] The district courts are split on this issue.[238] The FBI has taken Apple to court in two recent cases to gain access to locked iPhones. In one case, a magistrate judge for the district court granted the order.[239] In the other case, a magistrate judge declined to issue the order.[240] The issue is unpredictable; Apple and the government have no guess as to how courts will decide similar cases.[241]

To resolve this issue, Congress should pass federal legislation to block the government and law enforcement agencies from obtaining access to court orders compelling technology companies to change their security programming as a means of gaining access to locked devices. A court order compelling a technology company to write programming would violate the First, Fourth, and Fifth Amendment rights of companies and consumers.[242] Because individuals nationwide store personal information on encrypted devices, this backdoor is dangerous. Not only could the government and law enforcement agencies use the backdoor as precedent to act as "Big Brother," but it creates a risk that hackers and cybercriminals could obtain the hack.[243] Encryption of data is important to the safety of our personal data. Companies spend time and money to design operating systems that ensure the protection of data.[244]

---

[235] Compliance with Court Orders Act of 2016, 114th Cong. § 3 (2016), https://www.eff.org/document/burr-feinstein-encryption-bill-discussion-draft.

[236] *See* Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, ATLANTIC (Sept. 11, 2015), https://www.theatlantic.com/technology/archive/2015/09/how-the-government-surveils-cell-phones-a-primer/404818/.

[237] *See* Frankel, *supra* note 21.

[238] *Id.*

[239] Order Compelling Apple to Assist, *supra* note 16, at 1.

[240] Frankel, *supra* note 21.

[241] We anxiously await the Court's decision, as it could completely change the game. Microsoft Corp. v. United States, 829 F.3d 197, 201–02 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (2017) (No. 17–2).

[242] Fein, *supra* note 199.

[243] *A Message to Our Customers*, *supra* note 4.

[244] *See* Pagliery, *Here's What It Would Cost Apple*, *supra* note 173.

Compelling companies to rewrite their programming undermines efforts made to secure data.[245] Therefore, our national security is put in jeopardy by the very act taken by the government to protect the security of our nation. Therefore, Congress must enact legislation that will prevent the government from undermining the very thing that the government is trying to protect: national security.

This law would not bar technology companies from providing technological assistance by creating or modifying security programming to aid law enforcement or the government in investigations in which public safety or national security are threatened. However, if a company decides to provide this type of assistance, the company cannot put a price on the backdoor or hack. Under the legislation proposed in this Note, the government or law enforcement agency would only be authorized by law to provide reasonable compensation to companies in exchange for services rendered. This restriction would prevent companies from selling hacks or backdoors for pecuniary gain. The proposed legislation is necessary to protect and balance the interests of national security and the Constitutional rights of companies and citizens.

[245] *A Message to Our Customers*, *supra* note 4.