ENCRYPTION FRICTION

Christopher Babiarz

INTRODUCTION

The Supreme Court decision in *Riley v. California* reflects the fact that the Court is increasingly sensitive to the implications of new technologies in the lives of individuals and their subsequent impacts on reasonable expectations of privacy.[1] This increased judicial awareness for the pervasive role that technology plays in our modern privacy suggests that in the future the Court would be more inclined to protect individual privacy rights and less inclined to force technology manufacturers to only provide broken encryption to users so that the government can enjoy unfettered access to protected data.[2] Although encryption admittedly presents unique challenges to government interests in law enforcement and terrorism prevention, the proposed government solution undercuts and outweighs fundamental aspects of modern privacy.[3] Given the Court's demonstration of an increased awareness for modern privacy concerns, efforts by the government to undermine encryption should be dismissed by the Court in favor of individual privacy rights.

Following an introduction to encryption generally, this paper begins with the rekindling of a privacy issue that Michael Froomkin wrote about in the mid-1990's.[4] The lack of a solidified judicial stance on this issue sets the stage for the modern encryption battle between the FBI and Apple, and the recent Supreme Court decision in *Riley v. California* illustrates a likelihood that the current Court is ready to finally take a position on this old debate.[5] This paper argues that the Court should be

---

1 Riley v. California, 134 S. Ct. 2473 (2014).

2 *Id.* at 2484.

3 *Id.* at 2484–85, 2495.

4 Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

5 *See* Riley v. California, 134 S. Ct. 2473 (2014). *See also* Devlin Barrett, *Justice Department Seeks to Force Apple to Extract Data From About 12 Other*

prepared to make this determination in favor of individual privacy rights, despite the fact that the popularized lawsuit has been dropped for the time being.[6] Fundamentally the issues at large boil down to the conflict between "the perennial desire of law enforcement and intelligence agencies to have the capability to penetrate secrets at will, and private citizens who are acquiring the ability to frustrate these desires."[7] The answer to these questions will undoubtedly require a value judgment between the classic clash of security and privacy.[8]

I. WHAT IS ENCRYPTION AND WHY DOES IT MATTER?

Technically speaking, modern encryption refers to the process of converting plaintext into ciphertext, and represents just one aspect of the larger field known as cryptography.[9] Cryptography is defined by Microsoft as the "science of providing security for information" and is considered to be "a cornerstone of the modern security technologies used to protect information and resources . . . "[10] Of course, the science of cryptography goes back much farther than Microsoft and its modern applications.[11] In fact America's founding fathers recognized the importance of the security offered by encryption and used the science themselves.[12] For example, John Madison, the author of the Bill of Rights used encryption in letters to Thomas Jefferson, the author of the Declaration of Independence.[13] The use of encryption by these

iPhones, THE WALL STREET JOURNAL (Feb. 23, 2016, 12:39 PM), http://www.wsj.com/articles/justice-department-seeks-to-force-apple-to-extract-data-from-about-12-other-iphones-1456202213.

[6] Daisuke Wakabayashi and Robert McMillan, *Apple Win in iPhone Case Comes With Cost*, THE WALL STREET JOURNAL (Mar. 23, 2016, 12:35 AM), http://www.wsj.com/articles/apple-win-in-iphone-case-comes-with-cost-1458690530.

[7] *Froomkin*, *supra* note 4, at 713.

[8] *Id.* at 814.

[9] *Id.*

[10] *What is Cryptography?*, MICROSOFT, https://technet.microsoft.com/en-us/library/cc962030.aspx. (last visited Jan. 24, 2017).

[11] Seth Schoen and Jamie Williams, *Crypto is for Everyone – and American History Proves It*, ELECTRONIC FRONTIER FOUNDATION (Oct. 30, 2015), https://www.eff.org/deeplinks/2015/10/crypto-everyone-and-american-history-proves-it.

[12] Noa Yachot, *7 Reasons a Government Backdoor to the iPhone Would Be Catastrophic*, ACLU (Feb. 25, 2016, 5:45 PM), https://www.aclu.org/blog/speak-freely/7-reasons-government-backdoor-iphone-would-be-catastrophic?redirect=blog/speak-freely/seven-reasons-government-backdoor-iphone-would-be-catastrophic.

[13] Schoen and Williams, *supra* note 11.

figures and others such as Benjamin Franklin, and George Washington demonstrates a strong likelihood that the benefits of encryption were in mind during the establishment of America's foundational principles such as freedoms of expression, and security.[14]

In the modern context, explaining the technological complexity associated with how encryption actually works is outside the scope of this paper, and could likely fill a library. Fortunately, it does not require a significant technical understanding of the science of cryptography to understand the central legal issues at hand. However this is not to say that the technological complexity is irrelevant, in fact, the technical complexities strike at the heart of the obstacles modern technology companies face in designing products to provide the highest level of customer security.[15] In adding to the complexity, the notion of requiring manufactures to design a backdoor into their security systems further undermines this security by creating vulnerabilities hackers can exploit.[16] As we will see, these complexities provide barriers to seemingly simple requests like giving the government one time access to a locked phone.[17] Without delving too much into the science, it is possible for the public, and importantly the courts to gain a significant understanding of the legal challenges modern encryption presents while also recognizing the individual right to truly secure technology.

Simplified, the modern debate over encryption has primarily focused on 'cellphones,' however it implicates nearly every aspect of our digital lives.[18] With the recent advent of 'smartphone' technology giants like Apple and Google have begun offering default encryption of the password-protected contents of their devices.[19] What this means is that data on a smartphone is automatically protected with significant encryption technologies such that only the password holder can access the contents of the

---

14 *See id.*

15 *See* Yoni Heisler, *Here's Apple's long-awaited legal response to the FBI*, BGR (Feb. 25, 2016, 3:17 PM), http://bgr.com/2016/02/25/apple-vs-fbi-legal-filing/.

16 *Id.*

17 *Id.* ("The compromised operating system that the government demands would require significant resources and effort to develop. . . . And if the new operating system has to be destroyed and recreated each time a new order is issued, the burden will multiply.").

18 Yachot, *supra* note 12 (discussing the "Internet of Things" ranging from smart TVs, or even intelligent ovens).

19 URS GASSER ET AL., DON'T PANIC. MAKING PROGRESS ON THE "GOING DARK" DEBATE 3 (2016).

hard drive.[20] It is important to note that this level of encryption means that even the producer of the device (Apple, Google) does not have access to the contents of the hard drive without the password.[21] This means that even with a lawful court order such as a warrant, the creators of the devices are unable to assist the government in accessing the contents of the device.[22] Therefore, digital encryption presents an issue to the courts that has no physical parallel.[23] For instance, in the physical world, law enforcement would have no need to require a safe manufacturer to provide a key for a customer's safe, because the government could always use brute force to crack the safe.[24] Digital encryption not only makes 'brute force' cracking attempts by the government mathematically impossible (or near impossible), it can further ensure privacy with features that wipe a device's hard drive if too many incorrect passwords are entered, a function that a safe could never do.[25] With these security features being automatically implemented on phones, modern encryption has found itself in the hands of virtually every individual in the United States.[26] The government is not unaware of this fact either, and in 2014 FBI Director James Comey echoed concerns expressed in 2010 on the issue of "going dark" stating:

> Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.[27]

---

[20] *Id.* at 4

[21] *Id.*

[22] *Id.*

[23] Froomkin, *supra* note 4, at 871.

[24] *Id.*

[25] *See also id.* at 887–88. *See generally id.* at 829 (interestingly Froomkin speculates about the possibility of the government banning safe deposit boxes which have a self-destruct feature).

[26] Gasser, *supra* note 19, at 4.

[27] James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety*

While it is easy to sympathize with the Director's legitimate concerns given the obvious challenges encryption poses to law enforcement, there are fundamental implications to privacy and freedom of expression that must be considered.[28] Therefore, it is important to first understand why encryption matters to us as individuals before making reactionary decisions.

Modern encryption is in fact incredibly pervasive in our digital world.[29] To begin with, encryption is a necessary component of the basic functioning of banks, ATMs, and virtually person who conducts business electronically.[30] Encryption allows for businesses to confidently store commercial data and trade secrets, and is critical in protecting intellectual property from competitors.[31] Furthermore, encryption protects professionals such as doctors and lawyers who deal with sensitive client information that is not intended to be viewed by anyone other than the patient or the professional.[32] We are currently watching the consequences of this type of data being compromised unfold with the recent leak of millions of documents from the Mossack Fonseca law firm in Panama, colloquially known as the "Panama Papers."[33] While this leak disclosed countless instances of unethical conduct by prominent members of the global community and can be considered a good thing from a public perspective, it is important to note just how delicate the information is that professionals such as doctors and lawyers protect, and how effective encryption is a necessary component of their proper functioning.[34]

Yet perhaps most importantly is the role effective encryption plays in the lives of average citizens.[35] To describe today's smartphone as a phone at all is a misnomer, modern smartphones in all their forms are so much more than phones that using the name limits your thinking about what they can even do.[36] As will

on a Collision Course?, FBI (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

28 Froomkin, *supra* note 4, 717–25.

29 *Id.* at 718.

30 *Id.* at 719.

31 *Id.* at 722.

32 *Id.* at 725.

33 *The Panama Papers: Here's What We Know*, THE NEW YORK TIMES (Apr. 4, 2016), http://www.nytimes.com/2016/04/05/world/panama-papers-explainer.html?_r=0.

34 *See id.*

35 Froomkin, *supra* note 4, at 728.

36 *See generally* Comey, *supra* note 28.

be discussed, even the Supreme Court has acknowledged this trend, stating:

> The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.[37]

Even these understandings of what smartphones are today are insufficient, because smartphones also contain a wealth of unique data such as search history and geolocation which both can be used to reveal information that many individuals would prefer to keep private.[38] While it is nearly impossible to overstate the pervasiveness modern smartphones play in documenting our personal lives, it is important to remember these characteristics of the devices when considering the implications of compromising their encryption capabilities in favor of government access.[39] In sum, everyone has an interest in effective encryption, from corporations, to professionals, to the individual, and the Supreme Court's recent decision in *Riley v. California* suggests that the judiciary is ready to accept the fundamental role encryption plays in protecting these interests.[40]

II. WE HAVE BEEN HERE BEFORE

The current encryption dilemma is not new.[41] In the mid 1990's government struggled with the concept of controlling encrypted data, culminating in a proposed piece of hardware by the NSA known as the "Clipper Chip."[42]

Froomkin describes the scheme in the following way:

---

37 Riley v. California, 134 S. Ct. 2473, 2489 (2014).
38 *Id.* at 2490.
39 *Id.* at 2484.
40 *Id.*
41 *See generally* Froomkin, *supra* note 4, at 715 (discussing creation of Clipper Chip which would allow for government backdoor access to encrypted data).
42 *Id.*

> In exchange for providing the private sector with an encryption technology certified as unbreakable for years to come by NSA, the government plans to keep a copy of the keys – the codes belonging to each chip – which, the government hopes, will allow it to retain the ability to intercept messages sent by the chip's user.[43]

In essence, the government was concerned much the same way that it is today, that without technology like the Clipper Chip,[44] data could become locked away, inaccessible to law enforcement who possess a lawful order to access the information.[45] However, the Clipper Chip never really got off the ground, in part due to public concern over the obvious privacy implications, but in larger part due to the fact that people who wanted security could simply purchase devices that did not contain these Clipper Chips.[46]

Additionally the government seemed to recognize that people who were highly motivated to protect information (the high profile criminals and terrorists) would use other means of cryptography to encode their messaging.[47] Ultimately, the government conceded in their efforts, seeming to recognize that "crypto was here to stay, and if they wanted to gain access to encrypted communications and files, they would do so by warrants and their own cryptanalysis, and not by demanding that the systems themselves should be weakened."[48] Yet given the rise of widespread, default-enabled, password-protected, secure encryption on a device capable of enabling mass communication and data storage, the FBI seems interested in pushing the subject again, this time under the guise of preventing terrorism like the recent events in San Bernardino.[49]

The battle in the 1990's over the Clipper Chip ended with the fundamental questions it implicated unresolved.[50] At its core, the government's interest in equipment such as the Clipper Chip provokes the classic question of security versus privacy which "is a

---

[43] *Id.* at 716.
[44] *Id.*
[45] *Id.* at 716.
[46] Steven Levy, *Why Are We Fighting the Crypto Wars Again?* BACKCHANNEL (Mar. 11, 2016), https://backchannel.com/why-are-we-fighting-the-crypto-wars-again-b5310a423295#.ib1ft6u0a.
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*

value judgment, one that cannot be settled easily by doctrinal argument, yet one that the courts would have to make to resolve the issue. As with many value judgments, reasonable people may differ on the outcome."[51] Froomkin argues that attempts by the FBI to implement devices such as the Clipper Chip are an effort to return to the "status quo" of law enforcement access, such as in the era of wiretapping ordinary telephones.[52] However, as Froomkin further explains, the status quo actually is not a time when the government enjoyed effective wiretapping, but rather, the status quo should be remembered as the ability for one to "have a secure conversation by going for a quiet walk in an open field. Correspondents could encrypt letters in ciphers that no government could break."[53] The fact that modern technology has expanded the circle of people to whom we communicate, does not mean that this communication should be any less protected than the quiet walk in an open field.[54] Yet, technology also inherently increases our conversations' vulnerabilities, which mandating the need for secure encryption, because for instance, conversations can be eavesdropped upon by anyone that the telephone signal happens to reach and is not limited merely to people within earshot.[55] Modern encryption however offers a solution to this problem, and is uniquely suited to provide an opportunity to return to the metaphor of having a private conversation in the park, while efforts by the government to install backdoor features would undermine this possibility.[56] The lesson to be learned from the Clipper Chip fiasco is that the aforementioned principles argued by Froomkin are just as applicable today as they were in the 1990's, the only difference is that today technology has made it possible for mass surveillance to occur at an unprecedented level, with essentially no physical constraints, a reality that Froomkin speculated would soon occur.[57] In the end, although the Clinton Administration considered banning encryption that did not contain a Clipper Chip, it ultimately concluded:

---

51 Froomkin, *supra* note 4, 814–15.
52 *Id.* at 798–99.
53 *Id.*
54 *Id.*
55 *Id.*
56 Froomkin, *supra* note 4, at 799–800.
57 *Id.* at 805–06.

> [I]t would "not propose new legislation to limit use of encryption technology." A future administration might, however, reverse this decision, particularly if an investigation into a high-profile crime, such as the terrorist bombing of a major building or the management of a child pornography ring, was found to have been seriously hampered by the use of advanced cryptography. The current Administration has carefully left that option open for its successors, noting that by forgoing a ban on unescrowed encryption it is not "saying that 'every American, as a matter of right, is entitled to an unbreakable commercial encryption product.'"[58]

With the recent invigoration of efforts for a modern quasi-Clipper Chip in the wake of a terrorist attack similar to the one the Clinton administration predicted (San Bernardino), the government seeks to reignite the ashes left behind by the prior administration's inaction.[59] As further evidence of the government's intention to implement a modern version of the Clipper Chip, President Obama has also voiced his support of the FBI, stating:

> If it was technologically possible to make an impenetrable device where there's no door at all, then how do we apprehend the child pornographer? How do we disrupt a terrorist plot? . . . There has to be some concession to get into that information somewhere. . . . *We can't fetishize our phones above every other value. The dangers are real. This notion that sometimes our data is different and can be walled off from these other trade-offs is incorrect.*[60]

While it is clear where the executive branch stands on the topic, these opinions seem to contradict the strong message articulated by the Supreme Court in the recent case, *Riley v. California*, and presents and obvious tension between the branches of government

---

[58] *Id.* at 809–10.

[59] Christian Zibreg, *DOJ Threatened to Seize iOS Source Code Unless Apple Complies with Court Order in FBI Case*, IDOWNLOADBLOG (Mar. 14, 2016), http://www.idownloadblog.com/2016/03/14/dos-threats-seize-ios/.

[60] *Id.* (emphasis added).

that demands to be addressed.[61]

III. *RILEY V. CALIFORNIA*

Riley is a case decided in 2014, and stands as the latest Supreme Court decision on the issues of encryption generally, while also focusing specifically on the relationship between warrants and cellphone searches.[62] The fundamental question raised is whether police may, "without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[63]

In *Riley*, petitioner David Riley was stopped by a police officer for driving with expired registration tags, after which time Riley was arrested for possession of a concealed firearm.[64] Incident to the arrest, Riley was searched, upon which time his cell phone was seized by the officer.[65] After taking possession of the phone, which was in fact a smartphone, the officer apparently accessed the phone which was not password protected and noticed that some words on the phone were preceded by the letters "CK," an abbreviation the officer presumed to stand for "Crip Killers," a term used by gang members.[66] After the arrest, a detective searched the phone and testified that he found videos of young men fighting, as well as photographs of Riley standing in front of a car they suspected had been involved in another crime.[67] Following his arrest, Riley moved to suppress all evidence that the police had obtained from his cell phone, contending that the searches violated the Fourth Amendment because they had been performed without a warrant.[68] The trial court rejected this argument, and the appeals court affirmed, holding that "[T]he Fourth Amendment permits a warrantless search of cell phone data incident to an arrest, so long as the cell phone was immediately associated with the arrestee's person."[69]

The Court then examined a second case in which a police officer performing routine surveillance observed respondent Brima Wurie

---

61 *Id. See also* Riley v. California, 134 S. Ct. 2473 (2014).
62 Riley v. California, 134 S. Ct. 2473, 2485 (2014).
63 *Id.* at 2480.
64 *Id.*
65 *Id.*
66 *Id.*
67 *Id.* at 2481.
68 *Riley*, 134 S. Ct. at 2481.
69 *Id.*

making an apparent drug sale.[70] Following his subsequent arrest, officers seized a "flip phone" and were able to use information found on the phone to ultimately find Wurie's apartment building.[71] After obtaining a warrant, the police searched the house and found drugs and a firearm.[72] Wurie also moved to suppress the evidence obtained from the search of the apartment, arguing an unconstitutional search of his cellphone.[73] The District Court denied this motion, and a divided panel of the First Circuit reversed the denial, holding that, "cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant, because of the amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests."[74] With the procedural stage set, the Supreme Court granted certiorari for both of these cases.[75]

Upon beginning their analysis of how the "search incident to arrest" doctrine applies to modern cellphones, the Supreme Court immediately recognized the new digital landscape, explaining that modern cellphones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy."[76] While acknowledging the need to strike a balance between individual privacy and legitimate governmental interests, the Court reasoned that digital data presents no risk of harm to officers, nor is the digital evidence capable of being destroyed while it is in police custody.[77] The Court contrasted this principle with the fact that cellphones contain vast quantities of personal information, and that as such, a search of a cellphone cannot be contrasted with the searching of a person's physical possessions.[78] Ultimately, this led the Court to hold that officers must instead generally secure a warrant before conducting such a search on a cellphone.[79]

However, the Court's analysis did not stop there.[80] The Court explained that an officer could seize a cellphone during an arrest

---

70 *Id*. *See also* United States v. Wurie, 728 F.3d 1, 1 (1st Cir. 2013); United States v. Wurie, 612 F. Supp. 2d 104, 104 (2009).

71 *Riley*, 134 S. Ct. at 2481.

72 *Id.*

73 *Id.* at 2482.

74 *Id.*

75 *Id.*

76 *Id.* at 2484.

77 *Riley*, 134 S. Ct. at 2484.

78 *Id.* at 2485.

79 *Id.*

80 *Id.*

to briefly inspect it to ensure it did not contain a weapon (such as a small razorblade), or could similarly seize the phone to prevent destruction of evidence it contains by the arrestee.[81] Additionally, the Court further reasoned that the ability to conduct a warrantless search on a phone would also be inherently limited by the encryption and password protect feature most smartphones use, further diminishing the efficacy of warrantless searches.[82] Moreover, the Court criticized arguments by the government, stating that not every search is acceptable solely because a person is in custody, but rather, that a search of an arrestee's entire house touches on privacy concerns so heavily that it goes beyond the scope of a search incident to an arrest and requires a warrant.[83]

The Court was especially critical of the government's assertion that a search of all data stored on a cell phone is "materially indistinguishable" from searches of other physical items on a person subject to arrest, quipping:

> That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.[84]

The Court continued to underscore the significant features of modern cellphones that make them inherently different than any other item found on a person or their property, highlighting the storage capacity of the hardware itself, while also acknowledging the qualitative differences in the type of data that can be retrieved from a cellphone as compared even to a diary.[85]

The Court was especially careful to point out the fact that a cellphone's storage capacity allows the data stored within it to convey far more than previously possible, stating "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates . . . [p]rior to the digital age, people did not typically carry a cache of sensitive personal information

---

81 *Id.*
82 *Id.* at 2487.
83 *Riley*, 134 S. Ct. at 2488.
84 *Id.*
85 *Id.* at 2489.

with them as they went about their day."[86] The Court reasoned that people in the digital age record nearly every aspect of their lives, and that allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search any other personal item.[87]

In quoting Judge Learned Hand, "it is . . . a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him,"'[88] the Court affirmatively recognized that a cell phone search would likely result in "far *more"* evidence than even an exhaustive search of the home, because the modern cellphone contains all of the private data ordinarily found in the home, as well as a broad array of data that would never be found in a home, such as an exhaustive listing of one's search history.[89] Perhaps the most glowing endorsement for modern encryption came from the Court's conclusion:

> We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. *Privacy comes at a cost.*[90]

However, the Court supplemented this by stating that information on a cellphone is not immune from search, but rather a warrant must be acquired before such a search can lawfully occur.[91] Yet in its final words, the Court concluded that modern cell phones are more than a mere "technological convenience," recognizing they hold for many Americans "'the privacies of life.'"[92]

The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a

---

86 *Id.* at 2489–90.

87 *Id.* at 2490.

88 *Id.* at 2490–91 (quoting United States v. Kirchenblatt, 16 F.2d 202, 203 (CA 2d Cir.) (1926)).

89 Riley, 134 S. Ct. at 2490–91.

90 *Id.* at 2493 (emphasis added).

91 *Id.*

92 *Id.* at 2494–95.

cell phone seized incident to an arrest is accordingly simple – get a warrant.[93]

Although the concurring opinion expressed concern that the Court is poorly positioned to understand and evaluate the privacy interests that modern devices implicate, this belief is respectfully incorrect, for the issue fundamentally implicates Constitutional concerns.[94]

IV. FBI V. APPLE

Following the December 2, 2016 shooting rampage in San Bernardino that killed 14 people and injured 22, the Federal Bureau of Investigations ("FBI") began a major investigation into the lives of the perpetrators.[95] Amongst the evidence seized was a work issued iPhone belonging to one of the terrorists, which featured standard encryption technology which protected the contents of the phone behind a password.[96] As part of its security system, the phone also is programmed to wipe the data on its hard drive if an incorrect passcode is entered 10 times.[97] This significantly complicates the ability of law enforcement to gain access to the phone even with a lawful warrant for a known terrorist because the FBI can no longer use brute force to hack the passcode.[98] As a result, the FBI requested that Apple write software and upload it to the iPhone, disabling the feature that wipes the data on the phone after 10 incorrect password attempts.[99] In the context of the 4–6 digit numerical passwords most iPhones feature, this means that a brute force attempt can crack the code in less than a day using the FBI's technology.[100]

---

93 *Id.* at 2495.

94 *Id.* at 2497 (Alito, J., concurring).

95 Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, THE WASHINGTON 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.

96 Devlin Barrett, *Justice Department Seeks to Force Apple to Extract Data From About 12 Other iPhones*, MORNINGSTAR (Feb. 23, 2016, 12:36 PM), http://www.wsj.com/articles/justice-department-seeks-to-force-apple-to-extract-data-from-about-12-other-iphones-1456202213.

97 Nakashima, *supra* note 95.

98 *Id.* (Brute force in this context is used to describe the process of "attempting tens of millions of combinations without risking the deletion of the data.").

99 *Id.*

100 *Id.* ("Matthew D. Green, a cryptography expert at Johns Hopkins University, said the FBI could crack a six-digit numeric code in about 22 hours.").

Therefore, the request to Apple to create software which disables the data wipe feature, is to effectively require them to build a "backdoor" into the phone, which in effect startlingly resembles the Clipper Chip of the 1990s.[101]

Although the security feature which wipes the data is a fundamental obstacle for the FBI in the present case, in future cases this feature might not even be necessary as passcodes which are comprised of numbers, letters, and symbols and of lengths greater than 6 are likely to be used by people seeking privacy (including terrorists), because these added layers of complexities to passwords have a massive effect on the ability of a brute force crack to work quickly.[102] For instance, it may take years, or several hundred years depending on the complexity of the password, and as a result, the data wipe feature might not even become a necessity to avoid brute force attacks.[103] For the time being however, the data wipe feature presents a significant obstacle for the FBI when it comes to more basic passwords.[104]

As a result of these barriers U.S. Magistrate Judge Sheri Pym said in her order that Apple can and must write software that can bypass the feature.[105] Unsurprisingly, Apple has been quite vocal in its opposition to the order, stating "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 . . . No reasonable person would find that acceptable."[106] Apple's concerns over the matter should not be considered lightly either, given that Apple has a reputation for significantly complying with lawful orders in the past, and has given up all of the relevant data in this case contained in the iCloud.[107]

Nevertheless, through the use of the "All Writs Act," [108] the FBI is asking that the courts compel Apple to write this software.[109] Although the government has insisted that the software would only be used in this one case, its actions tell another story.[110] In at

---

101 *Id.*
102 *See* Nakashima, *supra* note 95.
103 *See id.*
104 *Id.*
105 *Id.*
106 *Id.*
107 *See* Nakashima, *supra* note 95.
108 All Writs Act, 28 U.S.C. § 1651 (2016).
109 *See* Nakashmia, *supra* note 95.
110 Barrett, *supra* note 96.

least a dozen other cases which do not involve terrorism charges, the Justice Department is pursuing court orders to force Apple to help investigators retrieve data.[111] If the government thinks that Apple can easily create this software and destroy it for each and every case without fear of the key falling into the wrong hands, they are mistaken.[112] In fact, such a task would require countless hours of engineering development, and would present an unrealistic and unreasonable burden on any technology manufacturer.[113]

There is also the question of why the FBI cannot crack the encryption on its own, given the full resources of the U.S. government using methods other than basic brute force attacks.[114] Many professionals in the cybersecurity field suggest that more sophisticated hackers could easily crack the phone, regardless of the data wipe feature.[115] While this may seem speculative, it is in fact exactly what ultimately happened in the present case.[116]

In a last minute decision, the government decided to postpone the case against Apple, claiming that an outside party was able to present a successful method for unlocking the phone without requiring any action from Apple.[117] Although the responsible party remains unclear, the actions of this individual singlehandedly brought the case against Apple to a halt.[118] However, this unexpected solution comes with unique problems of its own, namely the reality that "It is in law enforcement's best interests to not only find and exploit vulnerabilities, but keep that information out of the company's hands."[119] This troubling fact runs contrary to federal policies which encourage companies to share information about security flaws so they can be fixed, and has the potential to have harmful consequences on the notion of cybersecurity as a whole.[120] Although the case has been dropped for now,[121] there

111 *Id.*
112 Heisler, *supra* note 15.
113 *Id.*
114 John McAfee, *I'll Decrypt the San Bernardino Phone Free of Charge so Apple Doesn't Need to Place a Backdoor on its Product*, BUSINESSINSIDER (Feb. 18, 2016), http://www.businessinsider.com/john-mcafee-ill-decrypt-san-bernardino-phone-for-free-2016-2.
115 *Id.*
116 Wakabayashi, *supra* note 6.
117 *Id.*
118 *Id.*
119 *Id.*
120 *Id.*
121 *Id.*

appears to be a critical opportunity and necessity for the Supreme Court to step in before a complete arms race between private and public security interests unfolds.

At the same time the San Bernardino case against Apple was unfolding, a similar case in New York was also decided.[122] New York Magistrate Judge Orenstein rejected the government's arguments suggesting that the All Writs Act could be used to compel technology companies to unlock their products.[123] Although this case, along with the San Bernardino case, was ultimately dropped because the government used methods outside of the courtroom to access the phones,[124] this case represents a significant victory for encryption, as it has the potential to serve as a baseline for higher appellate courts to expand protections of encrypted devices.[125]

As a matter of policy, there are several major implications that would result from a government victory in these types of cases, and the need for careful judicial consideration is paramount.[126] First, requiring technology manufactures such as Apple to implement updates on all of their products featuring backdoor encryption would significantly dissuade consumers from updating their individual products to current versions which contain backdoors, creating a dangerous environment in which users could be exposed to malware and malicious attackers due to their lack of up-to-date equipment.[127] Second, if the United States establishes a precedent for forcing technology manufacturers to include backdoors, then it is probable other governments will attempt to do the same.[128] This is especially frightening when considering other governments do not have the same protections for citizens that are offered by our Constitution.[129] The human rights implications of facilitating a totalitarian government's ability to survey and crush its opposition is a startling consequence that must be seriously considered.[130] Finally, the fact that in our global market, not every country will

---

122 Russell Brandom, *With Its Retreat in New York, the FBI has Lost the Encryption Fight,* THEVERGE (Apr. 25, 2016, 11:16 AM), http://www.theverge.com/2016/4/25/11501992/fbi-apple-new-york-case-unlock-iphone-lost.

123 *Id.*

124 *Id.*

125 *Id.*

126 *See* Yachot, *supra* note 12.

127 *Id.*

128 *Id.*

129 *Id.*

130 *See id.*

require its technology manufacturers to include such a backdoor encryption device will likely result in an overall harm to American businesses, and instead encourage purchasing of foreign technology.[131] Terrorists and other criminals would undoubtedly find other means to communicate outside of backdoor-encrypted technology, and the benefit to true crime prevention could problematically become minimal at best.[132] All of these policy considerations and more must be at the forefront of any decision maker's mind when handling the issue of encryption.

V. CONSTITUTIONAL CONCERNS IMPLICATING THE SUPREME COURT

While the President has clearly been vocal in his stance on the encryption debate,[133] it is plain to see that the President and the Executive branch lack the authority to do much more on the subject.[134] It is suggested however that the debate over the ability of technology manufacturers to provide fully secure encryption to its customers should be decided by Congress.[135] In fact, even Apple has suggested that the courtroom is an inappropriate venue to decide the subject, further suggesting that Congress is better situated to make the determination.[136] This is an understandable position for Apple to take, given that many members of Congress have publicly expressed support for encryption, and that forcing Apple to unlock the iPhone is a "fool's errand."[137] Although the criticisms of Congress are extraordinarily valid, and recognize the fundamental need for effective encryption, any legislation passed by Congress on the issue will have to fit within the confines of a Supreme Court constitutional analysis.[138]

Congress and all other venues outside of the Supreme Court are limited in their ability to make a final decision restricting

---

131 *See* Gasser, *supra* note 19, at 1.

132 *See id.*

133 *See* Darlene Superville, *In Debate Over Encryption, Obama says 'Dangers are Real'*, PYS.ORG (Mar. 11, 2016), https://phys.org/news/2016-03-obama-absolutist-view-wont-encryption.html.

134 *See* Zibreg, *supra* note 59.

135 Heisler, *supra* note 15.

136 *Id.*

137 Spencer Ackerman, Sam Thielman, and Danny Yadron, *Congress Tells FBI that Forcing Apple to Unlock iPhones is 'a fool's errand',* THE GUARDIAN (Mar. 1, 2016), https://www.theguardian.com/technology/2016/mar/01/apple-fbi-congress-hearing-iphone-encryption-san-bernardino.

138 *Id.*

encryption because the aforementioned issues discussed implicate fundamental constitutional rights, and short of a full blown overhaul of the Bill of Rights, the Supreme Court will be the only institution with the authority to decide the issue definitively.[139] Even if Congress takes an affirmative position and passes legislation, say, requiring backdoor installation on every smartphone, such a statute would likely immediately be challenged in court by any number of technology manufacturers on Constitutional grounds.[140] Froomkin explained in the 1990's that mandatory key escrow such as the Clipper Chip would "reduce associational freedoms, chill speech, and constitute an intrusive search" and would require a court's balancing of "the potential costs to personal privacy against the gains for law enforcement and national security."[141] It is therefore critical that Congress take an interest in the issue and help to ensure legislation that respects encryption is passed, so as to impress upon the Court the strong interest the People have in effective security, however any legislation will still need to pass the scrutiny of the Court.[142]

A. The First Amendment

As a preliminary matter, it has already been established that source code is speech for First Amendment purposes.[143] In *Bernstein v. U.S. Dept. of Justice*, the court held that "encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine."[144] As such, when the government seeks to force companies like Apple to create code which undermines the security of their own operating systems, this is *compelled speech*, and it violates strong viewpoints that the company may hold regarding consumer security and privacy.[145] As Froomkin notes, the "Supreme Court treats compelled disclosure of noncommercial information as akin to a content-based restriction on speech, demanding the strictest scrutiny."[146] Furthermore, given the

139 *See* Froomkin, *supra* note 4, at 810–11.
140 *Id.*
141 *Id.*
142 *See id.*
143 Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999).
144 *Id.*
145 Heisler, *supra* note 15.
146 Froomkin, *supra* note 4, at 813.

Court's recent opinion in *Riley* it seems even more obvious that the Court would be inclined to apply the highest level of scrutiny with regard to compromising the security of a device so central to our lives.[147] However, the Supreme Court has stated that mandatory disclosure laws will be sustained if there is a substantial relation between the governmental interest and the information required to be disclosed.[148] Although the government interest in preventing terrorism and protecting national security would seem to be sufficiently compelling arguments, forcing technology companies to compromise the security of their systems with backdoor technology is far from being considered a "least restrictive" means of achieving that end, given that individuals who truly want to remain hidden will use devices which do not feature backdoor technologies, perhaps purchased in other countries.[149]

For most smartphone users, the phone is used for a variety of different First Amendment purposes, ranging from texting friends, to posting in an online forum, sharing photos, and the list goes on.[150]

The thought of always being potentially watched by the government, however, effectively imposes a chilling effect on the autonomous First Amendment expressions that a smartphone facilitates.[151] Warrants served on websites such as reddit, internet service providers, and even device manufacturers oftentimes expressly forbid an organization from informing a user that the user is a government surveillance target, or that the user's personal information has been surrendered.[152] In evaluating

---

147 Riley v. California, 134 S. Ct. 2473 (2014).

148 Froomkin, *supra* note 4, at 814 ("If the state interest in telling donors how charities use their contributions is sufficient to justify a mandatory disclosure statute, then the state interest in crime fighting and national security should be sufficiently compelling too. Because the government keeps the key in escrow, the rule is more narrowly tailored than a public disclosure rule.").

149 *See id.*

150 Aaron Smith, *Americans and Their Cellphones*, PEW RESEARCH CENTER (Aug. 15, 2011), http://www.pewinternet.org/2011/08/15/americans-and-their-cell-phones/.

151 *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 815 (1995) (quoting KIM LANE SCHEPPELE, LEGAL SECRETS 302 (1988)), http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3556&context=penn_law_review ("Few thoughts are more threatening to people who value autonomy than the thought of being constantly watched. . . .").

152 *See, e.g.*, Dustin Volz, *Reddit Deletes Surveillance 'Warrant Canary' in Transparency Report*, REUTERS, Mar. 31, 2016, http://www.reuters.com/article/us-usa-cyber-reddit-idUSKCN0WX2YF.

whether a law has a chilling effect, the Supreme Court evaluates "(1) the extent to which speech is likely to be chilled; (2) the degree to which the prohibition falls unevenly on a particular group as opposed to society at large; and (3) the availability of alternate channels of communication."[153] Given the pervasive nature of cellphones recognized by the *Riley* Court,[154] it is likely that a court will find the third factor easily satisfied. Further, a court will likely see the first prong is satisfied given the fear of always being potentially watched in the storage of a user's most intimate secrets.[155] Finally, such a prohibition could disparately impact individuals who lack the means to communicate broadly using other channels, and it is therefore likely that a court will be concerned with the significant chilling effect such a law could possibly have.[156]

"Built-in back doors" also pose significant threats to anonymity, an often underappreciated value which allows individuals to speak freely on political issues when they might otherwise fear government retribution.[157] Anonymity also touches on freedoms of associations, such that forcing all devices to include a backdoor for the government will require all associations seeking to communicate in a modern fashion to be subject to possible surveillance.[158] This too will result in a likely chilling effect on an individual's interest in associating with other individuals privately.[159] In sum, it is clear that government efforts to force backdoor encryption features will significantly invoke the First Amendment in a way that demands input from the Supreme Court.

B. The Fourth Amendment

The Fourth Amendment guarantees plainly the "right of the people to be secure in their persons, houses, papers, and effects

---

153 Froomkin, *supra* note 151, at 816 (citing City of Ladue v. Gilleo, 512 U.S. 43, 56 (1994)).

154 *See* Riley v. California, 134 S. Ct. 2473, 2484, 2488–93 (2014).

155 *See id.* at 2489–91, 2493–95; Froomkin, *supra* note 151, at 815–16.

156 *See* Froomkin, *supra* note 151, at 816–17.

157 *See id.* at 817, 820 (first quoting Hynes v. Mayor of Oradell, 425 U.S. 610, 628 (1976) (Brennan, J., concurring in part); Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 99–101 (1982)).

158 *See id.* at 818–19 (quoting NAACP v. Ala. *ex rel.* Patterson, 357 U.S. 449, 462 (1958) quoting Bd. of Dirs. of Rotary Int'l v. Rotary Club, 481 U.S. 537, 544 (1987)).

159 *See id.*

against unreasonable searches and seizures."[160] However, by forcing the installation of backdoor technology, the government is failing to acknowledge the fact that smartphones are "effects," and that such an installation would be akin to search and seizure.[161] "A search is a governmental invasion of a 'reasonable expectation of [personal] privacy[,]'" and nonconsensual searches require a warrant.[162] Given that users have demonstrated a strong privacy interest in the data stored on their devices, and that technology manufacturers recognize this interest by designing software to protect this security, it is seems clear that their users have a reasonable expectation of personal privacy in the content stored on their devices.[163] Therefore, forcing a technology manufacturing company to in effect "turn over the keys" to the encrypted content would certainly constitute a search for Fourth Amendment purposes.[164]

However, all of this merely establishes that the government's conduct is in fact, a search or seizure, but it does not address the implicit, failing assumptions the Fourth Amendment makes regarding technology in determining what is a "reasonable" search is.[165] When the Bill of Rights was adopted in the 18th century, our Founding Fathers could have never imagined the levels of communication and intimate details that a smartphone contains about its user.[166] Also, the Founders could have never fathomed the fact that physical limitations on the government's ability to make "reasonable" searches may one day not exist.[167] In fact, "the basic assumption that the police cannot be everywhere at once" is becoming increasingly false given the advent of mass data storage which is simultaneously tied to the high-resolution cameras and sensitive microphones stored in the pockets of virtually every citizen in the country.[168] This reasonable expectation of privacy lies at the heart of the problem, for as technology increases in its surveillance capacity, it shrinks what a "reasonable" expectation

---

160 U.S. CONST. amend. IV. *See also* Froomkin, *supra* note 151, at 823.

161 *See* Riley v. California, 134 S. Ct. 2473, 2485, 2491–92 (2014); Froomkin, *supra* note 151, at 844.

162 *See* Froomkin, *supra* note 151, at 827–28 (quoting Oliver v. United States, 466 U.S. 170, 178 (1984); citing Katz, v. United States, 389 U.S. 347, 357 (1967)).

163 *Id.* at 829. *See Riley*, 134 S. Ct. at 2484–87.

164 Froomkin *supra* note 151, at 829. *See Riley*, 134 S. Ct. at 2491.

165 Froomkin, *supra* note 151, at 843–46. *See Riley*, 134 S. Ct. at 2489–91.

166 Froomkin, *supra* note 151, at 843–46.

167 *See Riley*, 134 S. Ct. at 2488, 2490–91.

168 Froomkin, *supra* note 151, at 844. *See Riley*, 134 S. Ct. at 2489–91.

of privacy is.[169] Whereas an individual's backyard was once considered private, the law no longer recognizes such a "reasonable expectation" and permits government surveillance using cameras to photograph property below.[170] As the capacity for providing unprecedented levels of information about individuals' lives expands, it inherently conflicts with the notion that the Fourth Amendment protection against "unreasonable" searches is adequate as this list of "unreasonable" behavior continues to shrink.[171] Given the dramatic quantity of personal data stored on modern devices and the ability for this information to be surveyed with frightening efficiency, the true "reasonableness" of such searches should be reconsidered. However, it remains clear that these issues are fundamentally constitutional in nature, and require careful jurisprudence which can only be offered by the Supreme Court. As a result, any legislation passed by Congress which acts as a restriction on these constitutional concerns will need to fit within the confines of the Court's scrutiny.

CONCLUSION

In our modern digital world, technological advances have created unparalleled growth in communication, and individuals enjoy an intimate closeness to their digital devices. This closeness gives rise to an unprecedented level of personal information that can be found on such a device. Given this wealth of personal data, it comes as no surprise that users expect significant levels of privacy that obviates the need for extensive security measures. As a result, when the government seeks to compel technology manufacturers such as Apple to compromise this security in favor of allowing backdoor surveillance, considerable backlash is expected. Although the recent case against Apple has been temporarily suspended, the need for a firm judicial answer remains. Due to the constitutional implications associated with the inherent issues presented by encryption, the Supreme Court should be at the forefront in deciding between competing interests that the government may have in national security and the individual interest in privacy. However, our entire conceptual framework is potentially obsolete when it comes to Fourth

169 *See* Froomkin, *supra* note 151, at 823–24.

170 Froomkin, *supra* note 151, at 823 (citing Florida v. Riley, 488 U.S. 445, 451–52 (1989) (plurality opinion)).

171 *See* Froomkin, *supra* note 151, at 823–24.

Amendment protections against "unreasonable" searches because the Fourth Amendment is seemingly unprincipled for determining the extent of "reasonableness," concerning modern technological advances in surveillance capabilities and the ease for which extensive searches can be conducted. Perhaps what smartphone users really need is a positive right to privacy, not a negatively framed right to be secure from unreasonable search and seizure. The Supreme Court's holding in *Riley* would seem to indicate that the Court is ready to recognize such a right, and should be prepared to take this stance definitively when the next encryption war invariably begins.