The Precarious Balance Between National Security and Individual Privacy: Data Encryption in the Twenty-First Century

Jacob Zarefsky*

I. INTRODUCTION

A. Overview

First, this Comment discusses the definition of data encryption and the historical context surrounding the current debate between the government, technology companies, and individuals. Part I establishes the foundations of the ongoing debate and simplifies the technical language for laypersons.

Second, this Comment analyzes the constitutional protections related to the government compelling individuals to produce data on electronic devices. Part II first analyzes the individual protections provided by the

* © 2021 Jacob Zarefsky. Managing Editor, Volume 23, *Tulane Journal of Technology and Intellectual Property*. J.D. candidate 2021, Tulane University Law School; B.A. 2018, Communications, University of Virginia. The author would like to thank his mother, Jacqueline, and his father, Paul, for their everlasting love and support.

Fourth Amendment and then transitions to address the necessary balance between preserving citizens' privacy and providing effective tools for law enforcement. Next, Part II describes how digital data has complicated the traditional conventions of the Fifth Amendment protection against self-incrimination. In addition, Part II analyzes the circuit split on this issue and its practical consequences on criminal investigations.

Third, this Comment describes the role of technology companies in the encryption debate, specifically third-party telecommunications providers. Part III demonstrates the technical obstacles introduced by contemporary digital security and the government's current efforts to lawfully combat strong encryption. Part III also critiques the government's application of judicial precedents and existing federal laws, such as the All Writs Act and the Communications Assistance for Law Enforcement Act, to compel the assistance of telecommunication companies.

Finally, this Comment argues that the combination of out-of-date laws and broad judicial discretion of court orders promotes an inequitable, inefficient, and ineffective investigation and criminal prosecution system without standardized digital surveillance practices. Part IV describes the main legal and practical problems of current encryption laws (or lack thereof) and then proposes potential solutions to clarify the procedures related to conducting surveillance and digital evidence production. Ultimately, Part IV concludes that major tech firms and the government must compromise to effectively protect everyday consumers and detect criminal wrongdoers.

B. Historical Context of Encryption Debate

Since the advent of the digital age, technological advancements have revolutionized citizens' ability to protect information and securely communicate. The primary catalyst for the data security of modern smartphones, tablets, and computers is encryption technology. In simplified terms, encryption refers to the act of encoding information or messages to prevent unauthorized users from access.[1] Conversely, decryption describes the process of deciphering encrypted information to its original form.[2] Although encryption is not a new phenomenon, the advancements of modern data encryption have altered the status quo for American citizens and law enforcement alike. While data encryption has

1. *Data Encryption*, ENCYCL. BRITANNICA, http://www.britannica.com/technology/data-encryption (last visited Mar. 12, 2020).

2. *Decryption*, TECHOPEDIA, http://www.techopedia.com/definition/1773/decryption (last visited Mar. 12, 2020).

significantly improved digital security (and thus individual privacy), government officials assert that the technology facilitates criminal wrongdoing without reasonable safeguards.

The encryption debate between law enforcement and technology companies has become more prevalent as digital security continues to improve for everyday consumers. The federal government claims strong encryption technology may protect the disclosure of information, even with a warrant.[3] National intelligence agencies have subsequently labeled this problem as "going dark."[4] In 2017, the Federal Bureau of Investigation (FBI) alleged that nearly 7,000 confiscated electronic devices could not be accessed because of encryption technology.[5] But sources of the Washington Post claimed the actual number is probably closer to 1,000–2,000 unlockable devices.[6] Nevertheless, it is impossible to precisely quantify the effect of encryption on law enforcement surveillance and evidence-gathering practices.

II. HOW CRIMINAL SUSPECTS COULD EVADE CULPABILITY: GOVERNMENT COMPULSION OF INDIVIDUALS

A. Fourth Amendment Inquiry

The balance between maintaining tools for effective law enforcement and protecting the privacy rights of individuals has been a contentious source of debate since the ratification of the U.S. Constitution. Accordingly, the Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[7] At the same time, the Fourth Amendment sets requirements for the valid issuance of warrants, namely: a judge's finding of probable cause, supported by oath or affirmation,

---

3. *Lawful Access*, U.S. DEP'T OF JUST., OFF. OF LEGAL POL'Y, http://www.justice.gov/olp/lawful-access (last updated Oct. 30, 2020).

4. William P. Barr, Att'y Gen., *Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security* (July 23, 2019), *at* http://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

5. *FBI Failed to Access 7,000 Encrypted Mobile Devices*, BBC (Oct. 23, 2017), http://www.bbc.com/news/technology-41721354.

6. Devlin Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, WASH. POST (May 22, 2018), http://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8a4a4c070ef53f315_story.html.

7. U.S. CONST. amend. IV.

including particular descriptions of "the place to be searched and the persons or things to be seized."[8] The Fourth Amendment not only illustrates the importance of individual civil liberties, but also the necessity of standard procedures legitimizing governmental interference on citizens' rights.

While the same tension persists between tools for law enforcement and individual privacy rights today, recent technological advancements have fundamentally altered how American citizens communicate and store information. Over the twentieth century, the development of technology and rise of globalization has blurred preconceived notions of which possessions and property comprise people's "persons, houses, papers, and effects."[9] Although individuals still retain constitutional protection of certain private information, the mediums of communication and storage have generally evolved into intangible data. Thus, courts have been obliged to further modernize the standards of the Fourth Amendment to the technological advancements of the twentieth and twenty-first century.

Most notably, in *Katz v. United States*, the United States Supreme Court expanded Fourth Amendment protection by emphasizing individuals' reasonable expectation of privacy and overruling its previously interdependent connection with physical intrusion.[10] The landmark case ruled that the government's wiretap on a public telephone booth, without a warrant, constituted an unreasonable search and seizure of the criminal suspect's privacy.[11] Furthermore, the decision famously held that the Fourth Amendment protects people—not places—which expanded traditional conceptions of individuals' civil liberties.[12] The invention of personal computers, tablets, and smartphones have further obscured the tangibility of individuals' confidential information and private space. Additionally, the amelioration and omnipresence of these electronic devices have further complicated law enforcement's capacity to conduct surveillance and collect evidence.

On the other hand, the digital security of these devices, maintained by encryption, protects the average American consumer's sensitive information from theft, fraud, and other unlawful acts. The intricacy of decryption aside, in *Riley v. California*, the Supreme Court recently

8. *Id.*
9. *Id.*
10. Katz v. United States, 389 U.S. 347, 353 (1967).
11. *Id.*
12. *Id.*

delineated the reasonableness standard for searches and seizures of digital data on cell phones.[13] The Supreme Court held that the police generally must possess a search warrant with a valid finding of probable cause to search the digital data of an arrestee's electronic devices.[14] Unlike prior conventions of suspects' papers and effects, the stored data of cell phones (commonly referred to as "data at rest") possess a much larger scope of potentially incriminating information.[15] Furthermore, the search incident to arrest exception typically does not apply for searches of cell phone contents because law enforcement officers will not be put in imminent danger by digital evidence.[16]

Despite this landmark decision, the enhanced security of modern devices still impedes police from administering searches and seizures in a reasonable and effective manner. Even with a valid search warrant, law enforcement may not possess the technological means or expertise to successfully decrypt targeted communications and stored information.[17] The encryption debate (or "going dark" problem) has existed in some form for over a decade and continues to become more prevalent with increasingly advanced digital security.[18] As a result, the Department of Justice has alleged that "warrant-proof" encryption can provide a "lawless space" for criminals to evade electronic surveillance and other modern police practices.[19] The complexity of modern decryption has transformed law enforcement's traditional procedures of evidence collection and production and thus necessitates sensible reform to provide standardized practices.

While the relationship between the Fourth Amendment and electronic devices has not been codified, the *Riley* decision lays the foundation for legislative action.[20] Throughout the twentieth century, courts have invoked the Fourth Amendment as a fluid, case-by-case

13. Riley v. California, 573 U.S. 373, 381-82 (2014).
14. *Id.* at 386.
15. *See Lawful Access*, *supra* note 3.
16. *Riley*, 573 U.S. at 387.
17. *See* Tom Spring, *US Top Law Enforcement Calls Strong Encryption a 'Serious Problem'*, THREATPOST (Oct. 6, 2017, 3:53 AM), http://threatpost.com/us-top-law-enforcement-calls-strong- encryption-a-serious-problem/128302/.
18. *See id.*
19. *Lawful Access*, *supra* note 3.
20. *See Riley*, 573 U.S. at 407-08.

standard for protection of individuals and their property against unreasonable government intrusion.[21]

The Fourth Amendment invokes protection under civil and criminal law, and courts apply its standard to maintain protection across various technological mediums. Nevertheless, legal scholars have critiqued the inherent arbitrariness of the "reasonable expectation of privacy" test.[22] That being said, the reasonable expectation of privacy test for electronic devices has been detailed relatively clearly.

Although federal courts have established the Fourth Amendment protection for user information and digital data on electronic devices, law enforcement officials face unprecedented challenges in criminal investigations and prosecutions.[23] As previously mentioned, the police commonly seize encrypted cell phones and computers without the technological mechanisms to unlock the devices.[24] Thus, law enforcement agencies' options to produce certain digital evidence can comprise of either communicating with third-party service providers or directly compelling criminal suspects to produce digital evidence.[25] The latter has generated another related legal dispute between individual rights and standards of police practices.

More specifically, parties disagree on whether government compulsion of individuals to produce digital evidence (through court-ordered decryption) violates the Fifth Amendment's protection against self-incrimination.[26]

B. Fifth Amendment Inquiry

Among the enumerated rights provided by the U.S. Constitution, the Fifth Amendment guarantees the protection of individuals against self-incrimination in criminal law proceedings.[27] When sophisticated data encryption proves to be inaccessible by intelligence agencies, the government may order individuals to unlock digital devices, submit

---

21. *See id.* at 382-87.
22. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 528-29 (2007).
23. *See Riley*, 573 U.S. at 373; *Lawful Access*, *supra* note 3.
24. *See Lawful Access*, *supra* note 3.
25. *See id.*
26. Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 768-69 (2019).
27. U.S. CONST. amend. V.

passwords, and decrypt stored data.[28] As the security of electronic devices has ameliorated, court-ordered evidence production has become more commonplace. Although decryption court orders are a novel phenomenon, the United States government has generally issued these orders under the All Writs Act, originally enacted in 1789.[29] The All Writs Act proclaims that federal courts "may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[30] The federal statute undoubtedly establishes minimum specific guidelines to reduce impediments to law enforcement. However, the inherently arbitrary language of the All Writs Act has produced inconsistent opinions and inequitable results throughout the criminal justice system. This procedural dispute regarding criminal suspects' production of evidence on their mobile devices has produced a circuit split among the federal courts.[31]

On one hand, several judges believe current law enforcement agencies do not possess effective tools to compel individuals without the application of the All Writs Act. The United States Court of Appeals for the Third Circuit affirmed a government court order to decrypt devices as "necessary or appropriate" under the All Writs Act.[32] The court affirmed the validity of the original search warrant for the suspect's digital devices and held that the decryption order "'effectuate[s] and prevent[s] the frustration' of that warrant."[33] Since the government did not possess the means to produce the citizen's data, the court opined that the order was in aid of its jurisdiction and did not classify as a form of constitutionally protected self-incrimination.[34]

In contrast, the United States Court of Appeals for the Eleventh Circuit ruled that a compelled production of unencrypted contents on hard drives did invoke Fifth Amendment protection.[35] The court concluded that the suspect's act of production comprised a constitutionally protected

28. *See* Marjorie A. Shields, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data*, 84 A.L.R. 6th 251 (2013).

29. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 186 (1977).

30. 28 U.S.C. § 1651.

31. *See In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012); United States v. Apple MacPro Comput., 851 F.3d 238, 248 (3d Cir. 2017).

32. *Apple MacPro Comput.*, 851 F.3d at 244 (quoting *N.Y. Tel. Co*., 434 U.S. at 172).

33. *Id.* at 245 (quoting *N.Y. Tel. Co*., 434 U.S. at 172).

34. *Id.* at 248.

35. *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1352.

testimonial.[36] Ultimately, the federal courts differed because the evidence gathered by police tactics provided distinct standards of proof in the respective cases. In reaching their respective holdings, both circuit courts examined whether the "foregone conclusion" exception to the Fifth Amendment applied to the facts of their case.[37]

The exception to Fifth Amendment protection against self-incrimination applies when the existence and location of the relevant documents to be produced are a "foregone conclusion."[38] On the one hand, the Eleventh Circuit held that the government did not possess the requisite knowledge of the encrypted devices' contents to employ the evidentiary exception.[39] The court added that law enforcement officials must establish "reasonable particularity" to substantiate allegations that incriminating files exist on digital devices in encrypted form.[40] In contrast, the Third Circuit held that the suspect's act of production may be testimonial but falls under the "foregone conclusion" exception regardless.[41] The court differentiated its holding from the Eleventh Circuit decision by emphasizing the government's particular knowledge of the content of the encrypted devices.[42] The court concluded that the government "provided evidence to show both that files exist on the encrypted portions of the devices and that [the suspect] can access them."[43]

In practice, court orders to produce decrypted files represent a difficult and uncertain procedure for law enforcement. National intelligence agencies may investigate and conduct surveillance for months only to discover the seized evidence against a perpetrator cannot be lawfully accessed. Since protection against self-incriminating digital evidence remains unresolved, the government is frequently compelled to communicate with third-party service providers and manufacturers to decrypt the suspicious data of electronic devices.[44]

---

36. *Id.* at 1346.
37. *See id.* at 1343-46; *Apple MacPro Comput.*, 851 F.3d at 247-49.
38. Fisher v. United States, 425 U.S. 391, 411 (1976).
39. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d at 1349-50.
40. *Id.*
41. *Apple MacPro Comput.*, 851 F.3d at 247-48.
42. *Id.*
43. *Id.* at 248.
44. *See* Mariam Baksh, *End-to-End Encryption and Law Enforcement Access to Data Can Coexist, Justice Official Says*, NEXTGOV (Feb. 25, 2020), http://www.nextgov.com/cybersecurity/2020/02/end-end-encryption-and-law-enforcement-access-data-can-coexist-justice-official-says/163310/.

III. HOW TECH FIRMS COULD AVOID COOPERATION: GOVERNMENT COMPULSION OF THIRD-PARTY SERVICE PROVIDERS AND MANUFACTURERS

The deficiency of the police's modern surveillance devices and the substantial degree of judicial discretion involved in government seizure of electronic devices has caused law enforcement to contact and subpoena third-party technology companies (mainly telecommunications and software providers) for assistance. While the federal government acknowledges the benefits of data encryption for the personal security of average consumers, administrative agencies and the former Attorney General of the United States have criticized its unintended safe harbor for terrorists and violent criminals.[45] The U.S. Department of Justice has stressed the dangers of advanced encryption to criminal investigations and claimed "[s]ervice providers, device manufacturers, and application developers" furnish wrongdoers with warrant-proof software and facilitate the perpetration of serious crimes.[46]

Among the technology companies, Apple has been the focal point of the encryption debate, receiving national media attention and pressure from security agencies and the national intelligence community. While Apple will not reveal exactly how many court orders it has received, sources have indicated the company received at least nine government requests in a period of less than six months.[47] As a result, Apple provides "Legal Process Guidelines" for government and law enforcement officials within the United States on its website.[48] Among the detailed list of guidelines, the document states that Apple typically cannot extract data from passcode locked devices running iOS 8.0 and later because the information is encrypted and they do not possess the decryption key.[49] In other words, as digital security has advanced, data encryption of modern devices such as iPhones, has become so secure that even its software developers and hardware manufacturers cannot unlock them without a passcode or fingerprint. Ironically, technology companies have

45. Barr, *supra* note 4.

46. *Lawful Access*, *supra* note 3.

47. *See* Jenna McLaughlin, *New Court Filing Reveals Apple Faces 12 Other Requests to Break into Locked iPhones*, THE INTERCEPT (Feb. 23, 2016, 11:59 AM), http://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/.

48. *Legal Process Guidelines*, APPLE INC., http://apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (last visited Mar. 13, 2020).

49. *Id.*

significantly improved consumer privacy standards since Edward Snowden's infamous disclosure of leaked documents revealing the U.S. National Security Agency's intensive surveillance practices.[50] Nevertheless, law enforcement agencies continue to serve Apple with court orders to assist in criminal investigations and indictments.[51]

Similarly, the U.S. government has issued warrants and court orders to these technology companies under the All Writs Act. The application of the 200-year-old federal statute has fueled a series of legal battles across the federal district courts.[52] The crux of the disagreement centers on whether the All Writs Act provides a legal remedy for courts to address the encryption dilemma. In order to invoke the All Writs Act, the Act must possess an absence of alternative remedies and be necessary or appropriate "'in aid of' the issuing court's jurisdiction."[53] Ultimately, the novelty of the encryption debate provides minimal case law to guide federal judges' decisions. Therefore, federal district courts have been pressured to analogize the constitutional protection of electronic devices with prior mediums of communication.

For example, the U.S. government has paralleled the previous assistance of telecommunications companies in the implementation of pen registers (or DNR recorders) and wiretaps.[54] In *United States v. New York Telephone Co.*, the Supreme Court held that law enforcement officials may obtain a court order pursuant to the All Writs Act compelling telephone companies to operate electronic recording devices.[55] Moreover, the Court ruled the telecommunications company's status as a third party was not "so far removed from the underlying controversy . . . [because its] facilities were being employed to facilitate a criminal enterprise on a continuing basis."[56] The All Writs Act authorized the compelled third-party assistance because the installment of the recording device was not unduly burdensome and the FBI could not administer successful

50. *See* Zach Whittaker, *Five Years On, Snowden Inspired Tech Giants to Change, Even if Governments Wouldn't*, ZDNET (June 6, 2018, 6:44 AM), http://www.zdnet.com/article/edward-snowden-five-years-on-tech-giants-change/.

51. *See* McLaughlin, *supra* note 47.

52. *See* Oscar Raymundo, *Here's a Map of Where Apple and Google are Fighting the All Writs Act Nationwide*, MACWORLD (Mar. 30, 2016, 2:30 PM), http://www.macworld.com/article/3049994/heres-a-map-of-where-apple-and-google-are-fighting-the-all-writs-act-nationwide.html.

53. Clinton v. Goldsmith, 526 U.S. 529, 534-35 (1999).

54. *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 1:15-mc-01902-JO, 2015 WL 5920207, at *4-5 (E.D.N.Y. Oct. 9, 2015).

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

56. *Id.* at 174.

surveillance of the criminal suspect alone.[57] Government officials have cited the All Writs Act to assert the legality of third-party compulsion for the criminal investigation of electronic devices, specifically, the acts of decrypting stored data and unlocking users' passcodes.[58]

However, critics continually emphasize the technical discrepancies between telephone wiretaps and decryption orders to differentiate their lawfulness. First, orders to decrypt electronic devices generally involve data-at-rest.[59] In contrast, telephone wiretaps monitor suspects' communications in real time. Thus, court-ordered decryption divulges a larger scope of intimate information and undoubtedly poses a more significant risk to individual privacy. Second, critics challenge the absence of alternative remedies required by the All Writs Act for decryption orders.[60] Based on courts compelling users to unlock their devices, technology companies may argue for the existence of alternative remedies.[61] As previously mentioned, federal courts have disagreed whether decryption orders of individuals constitute lawful remedies for law enforcement. Third, the sophistication of modern encryption security casts doubts to whether service providers have the technical means to unlock devices without an undue burden. For these reasons, legal battles between law enforcement and third-party providers remain subject to substantial judicial discretion.

As a result, technology companies such as Apple, Google, and Facebook have stated their apprehension towards government regulation of digital security practices.[62] Nevertheless, due to the increasingly ineffective tools of modern law enforcement, Congress continues to face pressure to take legislative action. All major tech companies, however, have strongly opposed recent bill proposals involving encryption

57. *Id.* at 175.

58. *See* Govt's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search at 7-12, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 5:16-cm-00010 (C.D. Cal. Feb. 19, 2016).

59. *See What Is Data Encryption at Rest?*, SECURITYFIRST (Dec. 17, 2018), http://security firstcorp.com/what-is-data-encryption-at-rest/.

60. *See* Clinton v. Goldsmith, 526 U.S. 529, 537 (1999).

61. *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 1:15-mc- 01902-JO, 2015 WL 5920207, at *5 (E.D.N.Y. Oct. 9, 2015).

62. Angelique Carson, *Tech Companies Push Back Against Lawmakers' Demands for Encryption Backdoors*, IAPP (Dec. 11, 2019), http://iapp.org/news/a/tech-companies-push-back-against-lawmakers-demands-for-encryption-backdoors/.

security.[63] Tech companies claim that any invention of "backdoor" encryption keys for the government will significantly undermine the security of everyday users' devices.[64] Thus, reports indicate law enforcement agencies have taken alternative measures to court orders and have resorted to collaboration with independent third parties to unlock suspects' devices.[65]

However, other developed countries have already enacted legislation to mitigate the dangers of strong encryption.[66] For example, Australia and the United Kingdom recently enacted regulations of technology companies to address this problem.[67]

Before examining the proposed solutions of current U.S. lawmakers, this analysis will detail the existing laws relating to government interception of digital communications.

The controlling law for government interception of digital communications is the Communications Assistance for Law Enforcement Act (CALEA).[68] In 1994, President Bill Clinton signed into law the CALEA to impose stronger tools for law enforcement to conduct lawful interception of digital communications.[69] This federal law requires telecommunications carriers and manufacturers to maintain built-in capabilities for surveillance.[70] While digital data existed at the time, no one could have anticipated the technological progress of the next two decades, especially the development and ubiquity of modern smartphones. Ultimately, the CALEA has become obsolete for encryption purposes because the statute focuses on telephone wiretapping procedures rather than decryption methods.

Put simply, the statutory provisions of the Communications Assistance for Law Enforcement Act do not address the legal problems

---

63. *See id.*

64. *Id.*

65. *See Israeli Firm Helping FBI to Open Encrypted iPhone: Report*, REUTERS (Mar. 23, 2016, 5:55 AM), http://www.reuters.com/article/us-apple-encryption-cellebrite/israeli-firm-helping-fbi-to-open-encrypted-iphone-report-idUSKCN0WP17J.

66. Robert McMillan & Dustin Volz, *Apple and Facebook Fighting International Encryption Battle*, WALL ST. J. (Feb. 26, 2019, 5:30 AM), http://www.wsj.com/articles/apple-and-facebook-fighting-international-encryption-battle-11551177000.

67. *Id.*

68. Lillian R. BeVier, *The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T*, 51 STAN. L. REV. 1049, 1049 (1999).

69. *Id.* at 1051.

70. 47 U.S.C. § 1002(a)(2).

established by modern encryption security.[71] Nevertheless, the legislature and tech conglomerates still disagree on the ideal alternative to the twenty-year-old law. Yet, any degree of legislative reform will likely make a significant impact on the application of the All Writs Act. The Supreme Court has held that courts may not authorize ad hoc writs issued pursuant to the All Writs Act "whenever compliance with statutory procedures appears inconvenient or less appropriate."[72] Thus, any codification of modern policing standards regarding encryption will likely complicate the application of the All Writs Act. In the case of the encryption debate, the rapid advancement of technology and the inaction of lawmakers have provided nominal statutory procedures to standardize surveillance practices. For these reasons, Congress has faced significant pressure from intelligence agencies and the Attorney General's office to codify government regulations of technology companies.

IV. THE POTENTIAL PROBLEMS AND SOLUTIONS TO "GOING DARK" WITH ENCRYPTION: LEGAL REFORM/POLICY ANALYSIS

The excessive judicial discretion of court ordered decryption generates an inequitable, inefficient, and ineffective criminal investigation system without standard police surveillance practices. And although the Supreme Court has clarified the standard of Fourth Amendment protection for the search and seizure of individuals' electronic devices, a multitude of encrypted cell phones and computers remain inaccessible and thus inadmissible for criminal proceedings. Law enforcement agencies have referred to the obstacle of strong encryption as "going dark."[73] The Department of Justice and the FBI claim the digital security tools provided by major tech companies such as Apple, Google, and Facebook facilitate the wrongdoing of terrorists, pedophiles, and other violent criminals.[74] Nonetheless, these same national intelligence agencies also acknowledge the government's reliance on strong encryption for its own protection

71. *See* Barbara J. Van Arsdale, Annotation, *Construction and Application of Communications Assistance for Law Enforcement Act, 47 U.S.C.A. §§ 1001 to 1010*, 25 A.L.R. Fed. 2d 323 (2008).

72. Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

73. Barr, *supra* note 4.

74. *Lawful Access*, *supra* note 3.

against cyberattacks.[75] Meanwhile, other developed nations have instituted decryption laws regulating major technology companies.[76]

The technological progress of digital security in the twenty-first century has presented the legislature with several substantive and procedural uncertainties regarding law enforcement standards and practices: Should encryption laws be regulated by state or federal law? Can the government compel technology companies to manufacture decryption keys? Which party should possess the potential decryption keys? Should the standards of proof for police practices be identical for pre-crime and post-crime indictments? What role should the courts have in the targeted surveillance of suspects? How will legislation balance the interests of average individuals, criminal suspects, telecommunications providers, and manufacturers?

Although several states have introduced bills to regulate encryption, the federal government possesses more effective means to combat this issue.[77] Furthermore, major telecommunications and software firms naturally operate across all fifty states. Among the practical obstacles faced by law enforcement, the details of how the government can lawfully compel technology companies to weaken digital security on certain mobile devices are especially intriguing. On the one hand, some nations require assistance from criminal suspects following a valid warrant.[78] On the other hand, other nations regulate third-party telecommunications carriers to diminish the threat of self-incrimination.[79] However, technology companies argue that the coerced development of decryption keys is both impractical and unconstitutional.

As the advanced protection of digital security has increasingly developed, major tech firms have become more and more skeptical of their capacity to unlock electronic devices. As previously mentioned, Apple generally claims their inability to decrypt their devices with recent

---

75. Barr, *supra* note 4.

76. McMillan & Volz, *supra* note 66.

77. *See* David Ruiz, *The ENCRYPT Act Protects Encryption from U.S. State Prying*, EFF (June 11, 2018), http://www.eff.org/deeplinks/2018/06/encrypt-act-protects-encryption-us-state-prying.

78. John Oates, *Youth Jailed for Not Handing over Encryption Password*, THE REGISTER (Oct. 6, 2010, 9:12 AM), http://www.theregister.co.uk/2010/10/06/jail_password_ripa/; *World Map of Encryption Laws and Policies*, GLOB. PARTNERS DIGIT., http://www.gp-digital.org/world-map-of-encryption/ (last visited Mar. 13, 2020).

79. *Australia Data Encryption Laws Explained*, BBC (Dec. 7, 2018), http://www.bbc.com/news/world-australia-46463029; *World Map of Encryption Laws and Policies*, GLOB. PARTNERS DIGIT., http://www.gp-digital.org/world-map-of-encryption/ (last visited Mar. 13, 2020).

software updates.[80] Moreover, the technology industry will likely challenge any government compelled decryption as a violation of their First Amendment rights.[81] Furthermore, the creation of decryption keys will cause another debate disputing the rightful possessor of these powerful digital tools. The possession of decryption keys by the government, code developers, and neutral third parties present respective advantages and disadvantages for each party. Thus, the coerced formulation of decryption keys appears technically impractical and a potential constitutional violation. Nevertheless, law enforcement agencies proclaim technology companies cannot be authorized to manufacture strong encryption software without any governmental regulations.

In addition, the legislature must address the procedural details involving the timing of investigative court orders and the requisite standards of proof for lawful digital surveillance. The breadth of sensitive information on users' mobile devices demonstrates the importance of maintaining a reasonable expectation of privacy among individuals. Fortunately, the Supreme Court has established the requirement of a warrant to search all cell phones (and conceivably analogous electronic devices).[82] Although mobile devices generally produce a substantial amount of confidential information, policymakers should recognize the heightened privacy expectations among Americans and adapt the proper constitutional standards of reasonableness accordingly. Ultimately, the rapid advancements in technological innovation have caused existing laws on the interception of digital communications to become obsolete, especially the Communications Assistance for Law Enforcement Act.[83] In addition, the ambiguity of the All Writs Act further complicates the standardization of court-ordered decryption and government compulsion of individuals and third-party service providers.[84]

First and foremost, the All Writs Act of 1789 presents challenges for law enforcement agencies and American citizens because the federal law's provisions are excessively broad and arbitrary.[85] For example, the statute

---

80. *Legal Process Guidelines*, *supra* note 48.

81. *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 453 (2d Cir. 2001); Junger v. Daley, 209 F.3d 481, 484-85 (6th Cir. 2000).

82. Riley v. California, 573 U.S. 373, 403 (2014).

83. *See FBI Seeks New Mandates on Communications Technologies*, CTR. FOR DEMOCRACY & TECH. (Feb. 24, 2011), http://cdt.org/insights/fbi-seeks-new-mandates-on-communications-technologies/.

84. *See* 28 U.S.C. § 1651.

85. *See id.*

does not define the meaning of the terms "necessary or appropriate" or "in aid of respective jurisdictions."[86] Furthermore, the government has struggled to establish the specific protections provided by the undue burden and "absence of alternative remedies" standards.[87] In practice, this promotes an inequitable criminal investigation system with unclear procedural guidelines for law enforcement. Likewise, the Communications Assistance for Law Enforcement Act of 1994 addressed the obstacles to police surveillance at the time of its enactment.[88] Although the federal statute addresses digital telephony, the provisions of the CALEA are not nearly equipped to compel telecommunications providers to assist in targeted police surveillance methods.[89] For these reasons, the current standards for law enforcement have become too reliant on the judiciary.

Moreover, federal district courts still disagree on the legality of court orders mandating criminal suspects to unlock electronic devices and decrypt digital data.[90] For these reasons, the Supreme Court should grant certiorari to this issue and modernize the criminal rules of procedure and evidence production. Moreover, Congress should enact legislation to compel certain individuals to assist law enforcement in the production of digital evidence. For example, other countries have instituted penalties of fines and jail time for criminal suspects refusing to comply with decryption orders.[91] The legislature should also clarify the requisite standards of proof for monitoring digital communications. Likewise, the federal statute should establish a more rigid standard to compel the decryption of criminal suspects' data-at-rest. Ultimately, the existing system concedes too much judicial discretion and relies too heavily on individual instances of police surveillance and investigation. Thus, the proposed legislation should specify the role and authority of federal courts throughout the process.

V. CONCLUSION

The balance between maintaining tools for effective law enforcement and protecting the privacy rights of individuals has been a contentious source of debate since the ratification of the U.S. Constitution. While

86. *Id.*
87. *See* Clinton v. Goldsmith, 526 U.S. 529, 537 (1999).
88. *See* 47 U.S.C. § 1002(b)(1)(A).
89. *See id.*
90. *Compare* United States v. Apple MacPro Comput., 851 F.3d 238, 248 (3d Cir. 2017) *cert. denied*, 138 S. Ct. 1988 (2018), *with In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349-50 (11th Cir. 2012).
91. *See* Oates, *supra* note 78.

mediums of communication have changed, the requirement of constitutional protection continues to exist. This Comment has analyzed existing jurisprudence, federal statutes, and the practices of foreign governments (albeit briefly) to illuminate the current obstacles faced by law enforcement and technology companies.

In conclusion, the ideal solution to the encryption debate requires compromise from both law enforcement and technology firms. On the one hand, encryption provides valuable security for individuals' information and communication networks. On the other hand, the digital technology impedes police surveillance tactics, positions potential violent offenders above the law, and has caused inequitable results in the U.S. criminal justice system.

For these reasons, the absence of governmental regulations on strong encryption technology is unacceptable. Congress and major technology corporations must collaborate to establish informed and practical solutions to the ongoing encryption debate. Although there are no perfect solutions to this debate, the current system of inequity and uncertainty significantly harms the constitutional freedom of every American citizen.