University of Michigan Journal of Law Reform

Volume 50

2016

Shedding Light on the "Going Dark" Problem and the Encryption Debate

John Mylan Traylor
University of Michigan Law School

https://doi.org/10.36646/mjlr.50.2.shedding

SHEDDING LIGHT ON THE "GOING DARK" PROBLEM AND THE ENCRYPTION DEBATE

John Mylan Traylor*

ABSTRACT

In an effort to protect the enormous volume of sensitive and valuable data that travels across the Internet and is stored on personal devices, private companies have created encryption software to secure data from criminals, hackers, and terrorists who wish to steal it. The greatest benefit of encryption also creates the biggest problem: Encryption software has become so secure that often not even the government can bypass it. The "Going Dark" problem—a scenario in which the government has obtained the legal authority to search a suspected criminal's encrypted device but lacks the technical ability to do so—is becoming increasingly common. In response, the government has resorted to obtaining court orders to compel private companies to assist it in bypassing encrypted devices, in some cases demanding that companies create entirely new software to accomplish this task. This raises a plethora of political, economic, and legal questions. This Note argues that given the weighty interests on all sides of the debate and the widespread effects that these cases will have, the encryption issue should be decided by the legislative branch instead of the courts. Because of the complexity of these issues and the lack of current legislation, the courts are being forced to stretch the law in ways that will likely lead to inconsistent and undesirable rulings. This Note advocates that the best method for Congress to solve this problem is to create an administrative body with rule-making, investigative, and adjudicative powers to address these situations on a case-by-case basis and to advise Congress on future legislation regarding encryption and digital security in general.

INTRODUCTION

People worldwide have become increasingly reliant on smartphones, tablets and personal computers, so much so that these devices have become an integral part of everyday life. Individuals store data including private conversations, photos, financial information, health data, passwords, places of residence, information regarding the whereabouts of themselves and others, and

* J.D. Candidate, University of Michigan Law School, May 2017; B.A., Emory University, 2014. I would like to thank the editors of the Michigan Journal of Law Reform, Professor Leonard Niehoff, and my friend Stephanie Balitzer for their invaluable feedback.

many other forms of extremely personal information on these devices.[1] These hubs of personal information attract criminals and hackers who wish to use such information without the consent of the owner. In an effort to protect individuals' personal information, private companies spend a considerable amount of time and resources encrypting it.

The greatest benefit of encryption also creates the biggest problem: private companies are very good at preventing third parties from bypassing their encryptions. While this can be advantageous for law-abiding citizens who need to be protected from hackers, it can be dangerous when criminals and terrorists are able to use the same encryption methods to communicate secretly, hide evidence, and otherwise evade authorities and commit crimes. Problems and conflicts arise when the government seeks to obtain this information for the purposes of investigating or thwarting crimes but cannot bypass the encryption of the device where the information is stored. Companies have become so skilled at creating device encryption that the government is often unable to access encrypted information even when it has the accompanying devices in its possession.[2] Recently, the government has resorted to compelling the assistance of private companies to decrypt, or unlock, devices by obtaining court orders pursuant to the authority of the All Writs Act of 1789 ("AWA").[3] These companies have recently started resisting these orders on two grounds. First, private companies argue that the government's interpretation of the AWA is incorrect because the statute does not actually grant the government the power to compel private actors to assist in decrypting devices. Second, companies argue that compelling them to do so is unconstitutional.

This Note analyzes the competing interests in the context of device encryption, describes the inadequacy of current law, and suggests a legislative solution to the existing conflicts and issues. Part I describes the basic workings of encryption, the "Going Dark"

---

1. *See generally* Thom File & Camille Ryan, *Computer and Internet Use in the United States: 2013*, U.S. CENSUS BUREAU 1, 1 (Nov. 2014), https://www.census.gov/history/pdf/2013computeruse.pdf.

2. *See generally* Order Compelling Apple Inc. to Assist Agents in Search, In re Matter of the 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-SP (C.D. Cal. Mar. 3, 2016) (exemplifying a circumstance in which the government cannot access an encrypted device despite having acquired a search warrant and the encrypted device).

3. *See* 28 U.S.C. § 1651 (2012); Order Compelling Apple Inc. to Assist Agents in Search, In re Matter of the 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-SP (C.D. Cal. Mar. 3, 2016).

problem, and the tension between device encryption and the government's interest in upholding national security. Part I also explores the recent court case between Apple, Inc. ("Apple") and the Federal Bureau of Investigation ("FBI") and describes its significance to this issue. Part II analyzes the current state of United States law regarding device encryption. Part II also examines relevant case law and the United States Constitution to determine the limits of the government's power to compel the assistance of private companies to decrypt devices. Part III advocates that Congress pass new legislation, creating an administrative body equipped with rulemaking ability and adjudicative powers to determine on a case-by-case basis when private companies must assist the government in decrypting devices.

I. COMPETING INTERESTS: PRIVACY AND SECURITY IN REGARD TO ENCRYPTION

A. Background Information on Encryption and Its Importance

Encryption is commonly defined as "the conversion or encoding of information for transmission so as to prevent interpretation without the key for decryption."[4] Encryption enhances the security of a device by scrambling its contents so that only someone with the correct encryption key can decipher them.[5] Encryption is generally regarded as the most effective way to protect confidential information.[6] According to Dave Anderson, senior director of Voltage Security, an encryption technology provider, "[w]hen properly implemented, encryption provides essentially unbreakable security."[7] Device encryption is such a popular means of securing confidential information that technology companies constantly compete to have more secure products to respond to consumer demand.[8] Some companies focus exclusively on digital security and encryption, such

4. CHRISTOPHER G. MORRIS, ACADEMIC PRESS DICTIONARY OF SCIENCE 743 (Amy Rosen et al. eds., 1992).

5. *See Encryption*, MICROSOFT, https://www.microsoft.com/en-us/TrustCenter/Security/Encryption (last visited Oct. 29, 2016).

6. *See* Jaikumar Vijayan, *Encryption Still Best Way to Protect Data—Despite NSA*, COMPUTERWORLD, http://www.computerworld.com/article/2484714/security0/encryption-still-best-way-to-protect-data——despite-nsa.html (last visited Oct. 29, 2016).

7. *Id.*

8. *See generally* Brief of Amici Curiae for Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, Whatsapp, and Yahoo in support of Apple Inc. at 1–5, 18, In re the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD20, No. CM 16–10 (C.D. Cal. Mar. 3, 2016) (describing the high consumer demand

as companies like Symantec Corporation, while others, such as Apple, develop their own encryption technologies and use them in conjunction with their own products.[9]

As technology advances, sophisticated hackers and cybercriminals are becoming increasingly effective at bypassing encryption and cyber intrusions are increasing in frequency.[10] The cost of having weak encryption, or failing to encrypt at all, can be devastating. For example, in 2007, cybercriminals gained access to more than 100 million credit and debit card numbers from Heartland Payment Systems, Inc.[11] In October 2014, attackers hacked Sony Pictures and released confidential information ranging from employee personal data to documents about the company's upcoming projects.[12] While it was never confirmed, the FBI presented evidence that North Korea was behind this attack on Sony Pictures, but also noted, according to CNN, that "[a]nyone could have pulled this off . . . . It could have been a disgruntled Sony Employee, profit-seeking hackers, North Korea—or the combination of the three."[13]

Even more recently, the government itself was hacked when the Office of Personnel Management was hacked by criminals in 2015, putting millions of Americans' personal information at risk.[14] The breach, which constitutes the largest cyberattack on the United States government in history, resulted in the theft of sensitive information from 21.5 million people, including addresses, health and financial history, fingerprints, and other information.[15] When asked about the significance of the breach, James B. Comey, director of

---

for digital security and consumers' expectations of secure data from major technology companies and their products) [hereinafter Brief of Amici Curiae 1].

9. *See, e.g.*, SYMANTEC CORP., www.symantec.com (last visited Oct. 29, 2016) (Symantec Corp. is a corporation focused on digital security, whereas companies like Apple create encryption and security protocols for their other devices).

10. *Cyber Crime*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/cyber (last visited Oct. 29, 2016) ("Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated.").

11. Danny Yadron, *Companies Wrestle with the Cost of Cybersecurity*, WALL STREET J. (Feb. 25, 2014, 11:24 PM), http://www.wsj.com/articles/SB10001424052702304834704579403421539734550.

12. Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

13. Jose Pagliery, *What Caused Sony Hack: What We Know Now*, CNN: MONEY (Dec. 29 2014, 1:58 PM), http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/.

14. *See* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

15. *Id.*

the FBI, stated, "[It] is a treasure trove of information about everybody who has worked for, tried to work for or works for the United States government . . . . Just imagine you are an intelligence service and you had that data, how it would be useful to you."[16] Such information could be used or sold to those who seek to harm the victims of the theft or to infiltrate other governmental operations. These examples highlight the ease and frequency with which hackers are able to take advantage of weak encryption and cybersecurity systems.

Thus, both private companies and the government invest a substantial amount of time, money, and personnel to continuously make encryption systems stronger to stay one step ahead of hackers. Creating and updating encryption systems is no easy task; it requires that the software be designed, created, tested, validated, and deployed, which all take significant time and skilled technicians to accomplish.[17] As a result of this investment, encryption has become so effective that it has caused an entirely new problem: criminals, hackers and terrorist can use the same encryption to their advantage.

B. The "Going Dark" Problem

The "Going Dark" problem, a phrase coined in the 1990s, refers to situations in which the government has legally obtained the right to search certain devices, but "lacks the technical ability to carry out those orders because of a fundamental shift in communications services and technologies."[18] According to the FBI, the Going Dark problem presents a huge obstacle for law enforcement trying to conduct investigations.[19] FBI Director James Comey commented on the Going Dark problem by stating that "[a]rmed with lawful authority, we increasingly find ourselves simply unable to do that which the courts have authorized us to do, and that is to collect information being transmitted by terrorists, by criminals, by pedophiles, by bad people of all sorts."[20]

---

16. *Id.*

17. *See generally* Brief of Amici Curiae 1, *supra* note 8.

18. *Going Dark*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/operational-technology/going-dark (last visited Oct. 29, 2016) [hereinafter *Going Dark*].

19. *See id.*

20. *Id.*

The FBI also claims that these problems are exacerbated in time-sensitive situations when decrypting a device could lead to thwarting or preventing a crime or saving lives.[21] In order to overcome the Going Dark problem, the government has resorted to using the courts to obtain orders to compel private companies to assist them in their decryption efforts.[22]

C. Competing Interests

The government's demand that private companies assist it in accessing encrypted devices has created extreme tension between the competing interests of those involved. These interests include those of the government and law enforcement, encryption companies, and the many individuals who rely so heavily on these devices.[23] The relevant competing interests include national security in terms of public safety, the potential backdoor problem,[24] privacy, national security in terms of data security, and the constitutional concerns that will be covered in Part II. In order to find the proper solution to this problem, it is first necessary to consider the weighty interests on all sides of the debate.

1. National Security: Public Safety

In his testimony before the Senate Judiciary Subcommittee on the Constitution, Federalism and Property Rights, New York University School of Law professor Richard A. Epstein stated, "No one can doubt the legitimate needs of law enforcement officials at the federal, state and local levels to monitor the high tech criminal activities that threaten the security of this nation, the liberty of the

21. *See id.*

22. The government has also resorted to requesting that the courts authorize orders compelling suspects themselves to input their own passcodes or otherwise unlock their personal devices. This raises serious constitutional questions, such as a potential violation of the Fifth Amendment right against self-incrimination. This Note focuses on the government compelling companies to provide assistance and does not address individuals being compelled to unlock their devices. For more information on this issue, see RICHARD M. THOMPSON II & CHRIS JAIKARAN, ENCRYPTION: SELECTED LEGAL ISSUES 6–16 (Mar. 3, 2016).

23. *See* Tim Cook, *Answers to Your Questions about Apple and Security*, APPLE (last visited Oct. 29, 2016), http://www.apple.com/customer-letter/answers/.

24. The backdoor problem refers to the belief that if a company creates software that can decrypt its encryption software, any party that obtains the software can use it, and so if the software is stolen or otherwise falls into the wrong hands, it can be extremely dangerous. The backdoor problem is covered in more detail in Part I.C.2 Private Actors' Data Security and "Backdoor" Concerns.

citizens within it, and the security and safety of the property they own."[25] Criminals and terrorists alike use encrypted devices because of the difficulty the government has decrypting them.[26] For example, at the state level, according to Cyrus Vance, the Manhattan District Attorney, "[m]ore than 120 Manhattan criminal cases have been harmed by the failure to execute search warrants on the latest smartphones."[27] Vance even noted that there were several occasions in which "average criminal[s]" informed their associates that only the latest encryption software (iOS 8 at the time), would prevent law enforcement from decrypting devices.[28] Furthermore, the Federal Law Enforcement Officers Association noted that in an intercepted phone call from a New York prison, an inmate referred to Apple iPhone encryption software as a "gift from god" because authorities were powerless to decrypt it.[29]

This problem is not limited to domestic crimes. For example, as reported by the Washington Post, FBI Director James Comey stated, "[t]he Islamic State terrorist group is increasingly using encrypted communications to recruit troubled Americans and urge them to carry out attacks . . ."[30] According to Comey, the Islamic State operatives post on social media outlets such as Twitter to attract potential recruits.[31] Once the operatives locate a potential recruit, they instruct him or her to use an encrypted mobile messaging app, at which point the FBI is no longer able to intercept messages or otherwise monitor their activity; all further communication between operatives and potential recruits becomes undetectable to

---

25. *Hearing before the S. Judiciary Subcomm. on the Constitution, Federalism and Property Rights*, http://www.computerprivacy.org/archive/03171998-3.shtml (last visited Oct. 29 2016) (Testimony by Richard A. Epstein, on behalf of Americans for Computer Privacy) [hereinafter Epstein Testimony].

26. Mark Berman, *Police Say Criminals View iPhones as 'Another Gift from God' Because of the Encryption*, WASH. POST (Mar. 18, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/03/18/police-backing-the-fbi-in-fight-with-apple-say-criminals-love-iphones-and-call-the-encryption-a-gift-from-god/?utm_term=.108ee70af494.

27. Jonathan Atler, *Manhattan DA: Smartphone Encryption Foiled 120 Criminal Cases*, THE DAILY BEAST (Dec. 28, 2015, 12:13 AM), http://www.thedailybeast.com/articles/2015/12/28/manhattan-da-smartphone-encryption-foiled-120-criminal-cases.html.

28. *Id.*

29. Dan Levine, *Police Say Criminals Like Apple iPhones Because of Encryption*, REUTERS, (Mar. 4, 2016, 10:14 PM), http://www.reuters.com/article/us-apple-encryption-police-idUSKCN0W62AP.

30. Ellen Nakashima, *FBI chief: Terrorist Group Turning to Encrypted Communications*, WASH. POST (July 8, 2015), https://www.washingtonpost.com/world/national-security/fbi-chief-terror-group-turning-to-encrypted-communications/2015/07/08/89167f74-2579-11e5-aae2-6c4f59b050aa_story.html.

31. *Id.*

the FBI.[32] The Washington Post noted that Comey stated to Congress that "the Islamic State has attracted at least 21,000 English-speaking followers on Twitter, bombarding them with incitements to violence."[33] Thus, FBI officials advocate for the ability to compel private companies to provide reasonable assistance to help minimize these substantial national security risks.[34]

2. Private Actors' Data Security and "Backdoor" Concerns

Private individuals and corporations have a strong interest in data security. Individuals store a wealth of private information on their various electronic devices including, "financial records and credit card information, health information, location data, calendars, personal and political beliefs, family photographs, [and] information about their children" that if stolen by hackers could put them and their loved ones at risk.[35] According to a report from the Ponemon Institute, "[a]n estimated 47 percent of all American adults have been affected by data breaches over the last year [2013], with an estimated 432 million online accounts being affected."[36] Companies are vulnerable to cybercrime as well; in fact, according to the FBI, "companies are the primary victims of cyber intrusions . . . ."[37] Indeed, in 2014, Target Corporation was the victim of one of the largest breaches of consumer data in American history when hackers gained access to over 40 million customer accounts, which included information such as credit and debit card numbers.[38]

Since Target's data breach, major data breaches have been discovered almost every month, including breaches of several large companies including Michaels Stores, Sally Beauty Supply, Neiman

32. *Id.*

33. *Id.*

34. *See generally Going Dark*, *supra* note 18.

35. Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistance, In re Matter of the 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-SP, at 2–3 (C.D. Cal. Mar. 3, 2016) [hereinafter Motion to Vacate].

36. B. Dan Berger, *Cybercrime Thrives Amid Lack of National Data Security Standards for Retailer*, HUFFINGTON POST (Aug. 17, 2014), http://www.huffingtonpost.com/b-dan-berger/cybercrime-thrives-amid-l_b_5503936.html.

37. *Cyber Security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland: Statement Before the S. Comm. on Homeland Security and Governmental Affairs* (2014) (Statement of Robert Anderson, Jr., Executive Assistant Director, Criminal, Cyber, Response, and Services Branch of the FBI), https://www.fbi.gov/news/testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland.

38. Gregory Wallace, *Target Credit Card Hack: What You Need to Know*, CNN: MONEY (Dec. 23, 2013) http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/.

Marcus, AOL, eBay, and P.F. Chang's Chinese Bistro.[39] According to a report from Intel Security and the Center for Strategic and International Studies, "[c]ybercrime is costing the global economy $575 billion and the U.S. economy $100 billion annually . . . making the U.S. the hardest hit of any country."[40] The increased threat of cybercrime led companies such as Apple, Google, and Facebook to begin encrypting their devices and communication platforms by default beginning in 2014.[41]

The government's request to compel companies to create new software to bypass its own encryption may lead to what many companies and cryptology experts are referring to as a "backdoor" or master key.[42] Apple stated in a letter to its customers:

> The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks.[43]

Several leaders in the technology industry, including Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, Whatsapp, and Yahoo, filed a brief in which they collectively supported Apple's claim that the government's action would necessarily lead to the creation of a backdoor.[44] According to a group of leading cryptographers and computer scientists, "[a]ny trap door system increases the risk that someone else will be able to find, duplicate or manufacture the key to the encrypted information."[45]

Furthermore, these companies and Apple argue that neither Apple nor the government could guarantee the safety of this software because creating the backdoor creates an extremely high risk that criminals, terrorists, or even foreign countries will obtain and use the backdoor to harm the government, citizens, or the companies

---

39. Berger, *supra* note 36.

40. *Id.*

41. *See* THOMPSON & JAIKARAN, *supra* note 22, at 1.

42. *See Letter from Tim Cook, CEO, Apple, to Our Customers, Answers to Your Questions about Apple and Security* (Feb. 15, 2016), http://www.apple.com/customer-letter/[hereinafter *Letter from Tim Cook*].

43. *Id.*

44. Brief of Amici Curiae 1, *supra* note 8.

45. Epstein Testimony, *supra* note 25 (citing *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption: Leading Cryptographers and Computer Scientists Report Says Government Encryption Plan is Risky and Impractical*) (full citation omitted).

themselves.[46] In short, these companies claim that the risk in creating a backdoor is that once created, it is too difficult to secure it and to ensure that no one else comes through it.[47]

The aforementioned technology leaders and Apple also claim that—aside from the security issues—creating a backdoor is an extremely burdensome and costly process.[48]

Apple claims the government's unprecedented demand requires that it develop new software that will destroy the security features Apple has spent years creating.[49] According to Apple, no current operating system can accomplish what the government desires, and any effort to create such an operating system requires that Apple write new code, rather than simply disabling the functionality of existing software.[50] In its Motion to Vacate, Apple stated:

> Experienced Apple engineers would have to design, create, test, and validate the compromised operating system, using a hyper-secure isolation room within which to do it, and then deploy and supervise its operation by the FBI to brute force crack the phone's passcode. The system itself would have to be tested on multiple devices to ensure that the operating system works and does not alter any data on the device. All aspects of the development and testing processes would need to be logged and recorded in case Apple's methodology is ever questioned.[51]

Finally, Apple and other technology leaders have a strong interest in ensuring the security of hundreds of millions of customers who depend on them.[52] The government forcing these companies to weaken their own encryptions will cause their customers to lose confidence in these companies' ability to protect user data from criminals, hackers, and terrorists, as well as the government.[53]

---

46. *See* Brief of Amici Curiae 1, *supra* note 8, at 18–21.
47. *See id.*
48. *Cf.* Motion to Vacate, *supra* note 35, at 23.
49. *Id.*
50. *Id.*
51. *Id.* at 23–24.
52. *Id.* at 23.
53. *See* Brief of Amici Curiae 1, *supra* note 8, at 18–21; *see also* Brief Of Amici Curiae Airbnb, Inc.; Atlassian Pty. Ltd.; Automattic Inc.; Cloudflare, Inc.; Ebay Inc.; Github, Inc.; Kickstarter, Pbc; Linkedin Corporation; Mapbox Inc.; A Medium Corporation; Meetup, Inc.; Reddit, Inc.; Square, Inc.; Squarespace, Inc.; Twilio Inc.; Twitter, Inc.; and Wickr Inc. at 13–15, In re Matter of the 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-SP (C.D. Cal. Mar. 3, 2016), http://images.apple.com/pr/pdf/Airbnb_Atlassian_Automattic_CloudFlare_eBay_GitHub_Kickstarter_LinkedIn_Mapbox_Medium_Meetup_

3. National Security: Data Security[54]

The government has a very strong interest in upholding national security, and that interest necessarily requires strong encryption. The FBI webpage states, "[t]he FBI supports strong encryption, and we know firsthand the damage that can be caused by vulnerable and insecure systems. The government uses strong encryption to secure its own electronic information, and it encourages the private sector and members of the public to do the same."[55] Secretary of Defense Ashton B. Carter noted at an annual computer security conference in San Francisco: "Data security, including encryption, is absolutely essential to the Pentagon."[56] Furthermore, Mr. Carter made it clear that he is "more interested in securing data than prying into it."[57] Like all private citizens and companies, the government is also at risk from hackers, criminals, and terrorists that seek to steal private information.

The government itself has had problems in the past with data security. As discussed earlier in this Note, the federal government—specifically the Office of Personnel Management—fell victim to a breach of government computer systems in 2015 that resulted in the theft of the personal information of approximately 21.5 million people.[58] In the hacking, 19.7 million people who had undergone government background checks in the past and 1.8 million others, including spouses and friends, had their personal information stolen.[59] In a separate but related hacking, 4.2 million federal

---

Reddit_Square_Squarespace_Twilio_Twitter_and_Wickr.pdf [hereinafter Brief of Amici Curiae 2].

54. The government also has an interest in the international consequences of the United States' ultimate decision on this issue. This Note does not explore these questions or the issues regarding international diplomacy problems regarding device encryption. However, such problems are discussed in Brief Of Amici Curiae Access Now and Wickr Found. In Support Of Apple Inc.'s Motion To Vacate (In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS3000, California License Plate 35KGD20) (C.D. Cal. Mar. 1, 2016). The government also has an interest in preserving the separation of powers doctrine by ensuring that the correct branch determines the ultimate outcome of this matter and that no branch is overstepping its constitutional authority. This Note will address those concerns and ultimately advocate that the legislative branch is the proper authority to determine this issue in Part III.

55. *Going Dark*, *supra* note 18.

56. Michael D. Shear & David E. Sanger, *Competing Interests on Encryption Divide Top Obama Officials*, N.Y. TIMES (Mar. 5, 2016), http://www.nytimes.com/2016/03/06/us/politics/competing-interests-on-encryption-divide-top-obama-officials.html.

57. *Id.*

58. Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

59. *Id.*; *see also* Tom Risen, *Top FBI Attorney Worried About WhatsApp Encryption*, U.S. NEWS (Apr. 5, 2016, 5:43 PM), http://www.usnews.com/news/articles/2016-04-05/top-fbi-attorney-

employees also had their personal information stolen.[60] These coordinated breaches constitute the largest known cyberattack on the systems of the United States government.[61]

It is clear that the government has a strong interest in the preservation of national security by having both the means to access encrypted devices and the ability to use stronger encryption to secure its own sensitive information. Administrative officials stated, "The United States government firmly supports the development and robust adoption of strong encryption, which is a key tool to secure commerce and trade, safeguard private information, promote free expression and association . . . . At the same time, encryption poses a grave challenge for our national security and law enforcement professionals."[62] This challenge—the government's difficulty bypassing the encrypted devices of suspected criminals, hackers, and terrorists—is fueled by the fact that whenever advancements in device encryption can be used to better protect public and private users, criminals, hackers, and terrorists can usually also use the same technology for more unsavory purposes.

Some government officials claim that both interests can be accomplished and are not mutually exclusive.[63] Other officials claim that allowing the government to more easily bypass encrypted devices necessarily weakens encryption and that promoting stronger encryption necessarily exposes the government to the aforementioned national security risks; in other words, that both interests cannot be reconciled.[64] The Justice Department and the FBI are advocating for a compromise in the form of promoting strong encryption "with limits" to advance both interests.[65] The difficulty lies in determining what the limits should be and whether such a compromise can truly accomplish both interests.

---

james-baker-worried-about-whatsapp-encryption?int=A6f909 (FBI general counsel stated that "stronger encryption can also benefit the government." Risen added that Baker concluded by "noting that data about himself and his family were exposed during a massive Office of Personal Management breach that affected an estimated 21.5 million federal employees or job applicants").

60. Davis, *supra* note 58; *see also* Risen, *supra* note 59.

61. Davis, *supra* note 58; *see also* Risen, *supra* note 59.

62. Shear & Sanger, *supra* note 56.

63. *See id.*

64. *See id.*

65. *Id.*

C. Case Study: San Bernardino Case

The issue of device encryption has resurfaced in the form of the FBI demanding, via a court order, that Apple, a private company, assist in its investigation of a terrorist attack that took place in San Bernardino, California. In *In re the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203,*[66] ("San Bernardino case"), the FBI persuaded the court to grant a Motion to Compel Apple to reasonably assist in the FBI's investigation by decrypting Syed Rizwan Farook's Apple iPhone to obtain personal information that might relate to his participation in the terrorist incident. Though in the past Apple has complied with such orders, it recently decided to appeal the court's ruling, claiming that "[t]he U.S. government has asked us [Apple] for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone."[67] According to Apple, the government's actions constitute an overreach of its authority and an attempt to subvert the law-making process by using the courts as a means to authorize its actions as opposed to using the normal law-making process.[68] Apple further contends that being forced to create a backdoor would not only put its users at risk, but would undermine the very encryption systems it has gone to such great lengths to create.

---

66. Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search at 22, 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. CM 16-10 (C.D. Cal. Feb. 19, 2016) [hereinafter Government's Motion to Compel]. https://www.justice.gov/usao-cdca/file/826836/download.

67. See Letter from Tim Cook, CEO, Apple, to Our Customers, Answers to Your Questions about Apple and Security (Feb. 15, 2016), http://www.apple.com/customer-letter/ [hereinafter Letter from Tim Cook].

68. Several months after this matter arose, the FBI claimed that it was eventually able to unlock the iPhone without Apple's assistance and has since dropped its demand. *See* Devlin Barrett & Daisuke Wakabayashi, *FBI Opens San Bernardino Shooter's iPhone; U.S. Drops Demand on Apple*, WALL STREET J., (Mar. 28, 2016, 10:20 PM), http://www.wsj.com/articles/fbi-unlocks-terrorists-iphone-without-apples-help-1459202353. While the parties are no longer arguing about this specific case, the legal issues at the core of this debate are far from resolved. *See id.* There are still multiple similar cases between Apple and the FBI pending. Furthermore, as reported by the Wall Street Journal, Eric Berg, special counsel for Foley & Lardner communicated that "[T]echnology companies [will continue] to make their devices harder to crack with each iteration. In time, another case will test the issues of privacy and security again . . ." Indeed, Berg believes that "'[i]t's only a matter of time.'" *Id.*

1. The Significance of the San Bernardino Case

The San Bernardino case is significant because it is the first case in which the government attempted to bypass encryption by demanding that a private company create entirely new software in order to do so. In its attempt to heighten encryption security, Apple released a new operating system called iOS 8, which effectively prevented Apple itself from being able to decrypt devices running iOS software.[69] Once any Apple device is running iOS 8 or a later update, not even Apple can access the information stored on the locked device as opposed to before the update, when Apple had the ability to decrypt devices running iOS software.[70] In its letter to its consumers, Apple stated, "We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."[71]

The iPhone in the San Bernardino case, unlike the other cases, is running iOS 8, and therefore the only way Apple or the government would be able to access the device is by creating an entirely new program to decrypt it, commonly referred to as a backdoor.[72] In other words, whereas in the past Apple had access to the information and could simply hand it over to the government, it is now being asked to create a new program that would subvert its own security measures and thereby give the government the information it seeks. As this Note will explain, there are significantly different legal implications when the government requests that a private company create entirely new software as opposed to when it simply requests information the private company already has in its possession.

II. CURRENT STATE OF THE LAW

This Part addresses the sources of law that might authorize the government to compel private actors to assist it in bypassing device encryption. This Part also addresses whether the applicable statutes are being applied constitutionally and other relevant constitutional concerns. This Part concludes by commenting on the difficulty

69. Tim Cook, *Answers to Your Questions About Apple and Security*, APPLE, http://www.apple.com/customer-letter/answers/ (last visited Sept. 9, 2016).

70. Andrew Hart, *Apple Will No Longer Unlock iOS Devices For Police*, HUFFINGTON POST (Sept. 18, 2014), http://www.huffingtonpost.com/2014/09/17/apple-unlock-devices-police_n_5840064.html (explaining the different features included in iOS 8, notably that Apple itself no longer has the ability to decrypt its devices).

71. Cook, *supra* note 69.

72. *See Letter from Tim Cook*, *supra* note 42.

courts have applying the limited and antiquated statutes and case law surrounding this issue.

A. What Source of Law Might Authorize the Government to Compel Private Companies to Provide Assistance to Bypass Device Encryption?

The two primary statutes at issue are the AWA and the Communications Assistance for Law Enforcement Act ("CALEA").[73] In the several cases in which the government has demanded the assistance of private companies to bypass device encryption, it has relied on the authority of the AWA. The Supreme Court has noted that "where a statute specifically addresses the particular issue at hand, it is that authority, not the All Writs Act, that is controlling."[74] The AWA is considered to be a "gap-filler" and was created to endow the courts with "broad statutory authority to ensure they could effectively carry out the duties of an independent judiciary by issuing the orders necessary to do so—even if Congress had not had the foresight to create all of the procedural mechanisms that might be required."[75]

Apple argues that CALEA applies to the matter at hand and is therefore controlling instead of the AWA. Conversely, the government argues that the AWA is controlling. The issue is whether CALEA addresses the specific matter at hand, or if instead the AWA is controlling because neither CALEA nor any other statute directly addresses this matter. Because the AWA only applies in the absence of any other controlling statute, it is first necessary to determine whether or not CALEA applies in this situation.

1. Communications Assistance for Law Enforcement Act (CALEA)

In 1994, Congress passed CALEA to address its concern that "new and emerging telecommunications technologies pose problems for law enforcement."[76] CALEA has several limitations regarding what the government can and cannot compel third parties

73. 47 U.S.C. § 1001 (2012).

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

75. *See* In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 350 (E.D.N.Y. Feb. 29, 2016).

76. H.R. REP. NO. 103-827, pt. 1, at 14 (1994).

to do when providing technological assistance.[77] In short, "CALEA requires telecommunications carriers to retain the ability to comply with court orders for real-time interceptions and call-identifying information."[78]

In the San Bernardino Case, Apple argued that CALEA explicitly prohibits the government from compelling companies like Apple to decrypt devices and, therefore, that the government is precluded from using the AWA to circumvent CALEA.[79] CALEA states that the government cannot compel a provider of an "electronic communication service" to adopt any specific design of its equipment, facilities, services or system configuration.[80] Apple argues that it is "unquestionably a provider of electronic communications services through the various messaging services it provides to its customers through iPhones."[81] Thus, Apple argues the government cannot require it to create new software, as that would constitute adopting a specific design of its equipment, facilities, services or system configuration.[82] According to Apple, because CALEA specifically prohibits this, the government cannot use the AWA to circumvent CALEA.

Apple further argued that applying the AWA here would be "inconsistent with the intent of Congress."[83] Apple noted that CALEA contains mandatory assistance provisions, which list the types of actors that must assist the government. Apple stated, "CALEA intentionally excludes information services providers like Apple, from the scope of its mandatory assistance provisions."[84] Apple contended that because Apple does not fall into one of the categories of actors listed, Congress did not intend for the government to be able to compel companies like Apple to assist it.[85] Indeed, in another similar case involving the FBI compelling Apple to assist it, the district court noted, "CALEA . . . is part of a larger legislative scheme that is so comprehensive as to imply a prohibition against imposing requirements on private entities such as Apple that the

77. *See* 47 U.S.C. § 1001–1002.

78. Order Compelling Apple Inc. to Assist Agents in Search, In re Matter of the 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-SP, at 21–22 (C.D. Cal. Mar. 3, 2016).

79. *See id.* at 25–26; *see also* Motion to Vacate, *supra* note 35, at 15–19.

80. *See* THOMPSON & JAIKARAN, *supra* note 22, at 25–26; *see also* Motion to Vacate, *supra* note 35, at 15–19.

81. Motion to Vacate, *supra* note 35, at 16.

82. *Id.* at 17.

83. See THOMPSON & JAIKARAN, *supra* note 22, at 26; *see also* Motion to Vacate, *supra* note 35, at 15–19.

84. Motion to Vacate, *supra* note 35, at 17.

85. *See id.* at 15–19.

statute does not affirmatively prescribe."[86] Apple therefore argues that even if CALEA does not explicitly prohibit the government from compelling Apple to assist it, because Congress has indicated its intent to "allow strong encryption" and to prevent the government from "mandating that such encryption schemes contain a back door," the courts should refrain from extending CALEA to apply in this case.[87]

The government argued that CALEA does not forbid the court's order compelling Apple to provide reasonable assistance for several reasons.[88] First, the government argued that CALEA does not "meticulously, intricately, or specifically" address when a court may require a private company such as Apple to help the government bypass encryption software, and therefore did not specifically address the matter at hand.[89] The government argued that the AWA applies as long as there is no statute that explicitly controls, which is the case here. The government stated, "It is not enough for other laws to brush up against similar issues. Rather, Congress must legislate so 'intricately' as to leave 'no gap to fill."[90] Because of this silence or gap in the law, the government claimed that an order under the AWA was appropriate to compel Apple to provide assistance.[91] The government also argued that CALEA only limits the authority of law enforcement agencies and not courts.[92] Indeed, the government argued, "The Order rests not on CALEA, but on the AWA . . . ."[93] Finally, the government noted that CALEA only applies to data "in motion."[94] Data in motion is a phrase used for data that is in transit, especially via telephone or the Internet.[95] Generally, data that is still being transmitted is considered in motion,

86. In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 350 (E.D.N.Y. Feb. 29, 2016).

87. Motion to Vacate, *supra* note 35, at 17.

88. Government's Reply in Support of Motion to Compel & Opposition to Apple Inc.'s Motion to Vacate Order at 10, In re Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451 (C.D. Cal. Feb. 25, 2016) [hereinafter Government's Reply].

89. *Id.* at 11.

90. *Id.* at 10–11 (quoting The Company v. United States, 349 F.3d 1132, 1145 n.26 (9th Cir. 2003)).

91. *See id.* at 11.

92. *Id.* at 11–12.

93. *Id.* at 12.

94. Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search at 22, 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. CM 16-10 (C.D. Cal. Feb. 19, 2016) [hereinafter Government's Motion to Compel].

95. *See* THOMPSON & JAIKARAN, *supra* note 22, at 2–3.

whereas data that is stored on a device and no longer being transmitted is consider at rest. According to the government, because it sought data that was stored on a device and no longer being transferred (data at rest), the plain text of CALEA does not apply.[96] The government argued that whether Apple is an information service provider as defined by the statute is irrelevant because the statue only applies to data in motion.[97] The government stated, "Put simply, CALEA is entirely inapplicable to the present dispute and does not limit this Court's authority under the All Writs Act to require Apple to assist the government in executing a search warrant."[98]

It is unclear whether or not CALEA directly applies to the matter at hand. According to Magistrate Judge Orenstein—a United States Magistrate Judge for the Eastern District of New York who ruled on another similar matter involving the FBI and Apple—it is arguable whether or not CALEA explicitly prohibits the government from compelling companies like Apple to assist it.[99] It does at least seem to be clear that because the data in question is at rest rather than in motion, the plain text of CALEA does not explicitly prohibit the government from compelling Apple to assist it in its investigation with a court order pursuant to the AWA.

2. The All Writs Act of 1789

In the several cases in which the government has demanded the assistance of private companies to bypass device encryption, it has primarily relied on the authority of the AWA of 1789.[100] The AWA states, "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[101] The statute grants federal courts the authority to issue orders when three criteria are met:

1. Issuance of the writ must be dq;in aid of" the issuing court's jurisdiction;
2. The type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and

96. Government's Motion to Compel, *supra* note 94, at 23.
97. *See id.*
98. *Id.*
99. In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 354 (E.D.N.Y. 2016).
100. THOMPSON & JAIKARAN, *supra* note 22, at 16.
101. 28 U.S.C. § 1651(a) (2012).

3. The issuance of the writ must be "agreeable to the usages and principles of law."

If an application under the AWA meets all three of those requirements, the court "may" issue the requested writ in exercise of its discretion—but it is never required to do so.[102]

After a court has determined that the statutory requirements of the AWA have been met, it may then consider the discretionary factors laid out by the Supreme Court in *United States v. New York Telephone Company*.[103] In *N.Y. Tel. Co.*, the Court ruled that a private telephone company could be required to install pen registers (surveillance devices that record outgoing phone numbers when dialed) in order to assist the government in thwarting criminal activity.[104] In that case, the Court ruled that three discretionary factors should be taken into account when considering an application pursuant to the AWA: (1) "the closeness of the relationship between the person or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction"; (2) "the reasonableness of the burden to be imposed on the writ's subject"; and (3) "the necessity of the requested writ to aid the court's jurisdiction (which does not replicate the second statutory element, despite the overlapping language)."[105] The requirements of the AWA itself seem fairly straightforward, but the constitutionality of the government's use of the AWA still must be scrutinized.

B. Constitutionality of Deployment of the AWA

The courts have made several rulings regarding the constitutionality of the AWA. In *Pennsylvania Bureau of Correction v. United States Marshals Service*, the Supreme Court ruled that "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute. Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling."[106] Earlier, in *Plum Creek Lumber Company v. Hutton*, the Ninth Circuit held that "[t]he All Writs Act is not a grant of plenary power to the federal courts . . . . It does not authorize a court to order a party to bear risks not otherwise demanded by law,

102. In re Order Requiring Apple, Inc. to Assist, 149 F. Supp. 3d at 350.
103. *See* United States v. New York Tel. Co., 434 U.S. 159, 172 (1977).
104. *Id.* at 178–79.
105. In re Order Requiring Apple, Inc. to Assist, 149 F. Supp. 3d at 351.
106. Pennsylvania Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

or to aid the government in conducting a more efficient investigation, when other forms are available."[107]

Finally, according to Magistrate Judge Orenstein, the AWA may be appropriately used "to fill in a statutory gap that Congress has failed to consider, [but] it cannot be used to grant the government authority Congress chose not to confer." Judge Orenstein explained as follows:

> But if CALEA, considered in the context of a larger statutory scheme, does not erect such a barrier to relief on its own terms, then the Application turns on whether the gap in the laws the AWA fills is, as the government argues, the entire space between authorizing statutes and legislative prohibitions or if, as Apple would have it, it only reaches to such legislative powers as Congress has not considered and either adopted or rejected.[108]

The question is whether Congress's inaction reflects a purposeful choice not to authorize the courts to compel information service providers to provide assistance to the government or if it is simply congressional oversight.

1. First Amendment Implications

One constitutional concern this use of the AWA raises is freedom of expression via software code. It might be the case that by forcing companies to write specific software code, the government is compelling speech and therefore violating the First Amendment of the Constitution. In *Turner Broadcasting Systems Inc. v. Federal Communications Commission*, the Supreme Court ruled that government actions that "compel speakers to utter or distribute speech bearing a particular message are subject to the same rigorous scrutiny" as laws restricting speech.[109] In *Riley v. National Federation of the Blind of North Carolina, Inc.*, the Supreme Court held that compelled speech is a "content-based regulation of speech" subject to strict scrutiny.[110] In *Junger v. Daley*, the Sixth Circuit ruled that "[b]ecause computer source code is an expressive means for the exchange of information

107. Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289–90 (9th Cir. 1979).

108. In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 357 (E.D.N.Y. 2016).

109. Turner Broad. Sys., Inc. v. Fed. Commc'n Comm'n, 512 U.S. 622, 642 (1994).

110. Riley v. Nat'l Fed'n of the Blind, Inc., 487 U.S. 781, 798 (1987).

and ideas about computer programming, we hold that it is protected by the First Amendment."[111] Finally, in *Universal City Studios, Inc. v. Corley*, the Second Circuit determined that computer code is treated as speech with regard to the First Amendment.[112]

Apple and the technology industry leaders argue that these cases applied together require the courts to view the government's action under a strict scrutiny basis. They argue that the government is regulating code, which is content-based speech, and that by compelling private companies to write specific code, the government is violating those companies' First Amendment rights.[113]

The government, on the other hand, contends that the code it is requesting is functional in nature rather than expressive and therefore does not receive the full protection of the First Amendment.[114] The government relies on the Court's holding in *Universal City Studios v. Corley* that "solely functional code 'is not within the meaning of the First Amendment.'"[115] The government also claims that based on the holding in *Red Lion Broadcasting Company v. Federal Communications Commission*, 395 U.S. 367, 386 (1969), "software that is automatic and is to be used in an entirely mechanical way is not speech under the First Amendment."[116]

In the San Bernardino case, the government argues that based on the aforementioned cases, the Court should analyze motions to compel companies to create new software under an intermediate scrutiny test. Therefore "so long as the regulation services a substantial government interest [,] the interest is unrelated to the suppression of free expression and any incidental restrictions on speech must not burden substantially more speech than is necessary to further that interest."[117] The government asserts that its interest in obtaining the code is to thwart terrorist threats, which is both substantial and does not relate to the suppression of speech, and

111. Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000).

112. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 449 (2d Cir. 2001).

113. Motion to Vacate, *supra* note 35, at 32–34.

114. Government's Reply, *supra* note 88, at 31–34; *see also* Brief for Greg Clayborn et al. as Amici Curiae at 18–19, In re Matter of the 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-SP, at 19 (C.D. Cal. Mar. 3, 2016) [hereinafter Brief for Greg Clayborn et al.].

115. Brief for Greg Clayborn et al., *supra* note 114, at 18 (quoting Universal City Studios v. Corley, 273 F.3d 429, 454 (2d Cir. 2001)).

116. *Id.* (quoting Commodity Futures Trading Comm'n v. Vartuli, 228 F.3d 94, 111 (2d Cir. 2000)).

117. *Id.* at 18.

that it does not incidentally burden any speech unnecessarily because there is no other way the government can bypass the companies' encryptions.[118]

2. Fifth Amendment Implications

Another constitutional concern raised by this use of the AWA is the Fifth Amendment's guarantee of substantive due process. In the San Bernardino case, Apple argued the government violated its substantive due process right to be free from "arbitrary deprivation of its liberty by government."[119] Apple relied on the ruling in *County of Sacramento v. Lewis*,[120] in which the Court stated, "We have emphasized time and again that '[t]he touchstone of due process is protection of the individual against arbitrary action of government,' . . . [including] the exercise of power without any reasonable justification in the service of a legitimate governmental objective."[121]

The government responded that "Apple must also show that such deprivation was 'clearly arbitrary and unreasonable, having no substantial relation to the public health, safety, morals, or general welfare.'"[122] The government argued that this cannot be the case because its actions have a substantial relation to public safety and general welfare since it is using the information to conduct an FBI investigation aimed at thwarting future terrorist attempts and apprehending any accomplices to the attack.

3. There is No Fourth Amendment Argument[123]

At first glance, the government decrypting people's personal devices may seem to raise Fourth Amendment issues, but that is not the case. Although encryption is created to address its users' personal privacy concerns, the Fourth Amendment's protection against an unlawful search and seizure does not apply here. Indeed, when

---

118. *Id.* at 8.

119. Motion to Vacate, *supra* note 35, at 34.

120. County of Sacramento v. Lewis, 523 U.S. 833, 845–46 (1998).

121. *Id.* (internal citations omitted).

122. Brief for Greg Clayborn et al., *supra* note 114, at 17 (quoting Sinaloa Lake Owners Ass'n v. City of Simi Valley, 864 F.2d 1475, 1484 (9th Cir. 1989)).

123. As explained below in this Part, privacy would normally be included as a Fourth Amendment issue in Part II with the other constitutional concerns, but because the AWA requires a search warrant and thereby almost certainly complies with Fourth Amendment, the claim is listed here as more of a practical concern than a legal one. *See* THOMPSON & JAIKARAN, *supra* note 22, at 16 n.113.

discussing the San Bernardino case, City University of New York (CUNY) School of Law Professor Ruthann Robson briefly addressed the issue stating that, "Interestingly, there is no Fourth Amendment argument."[124]

The Fourth Amendment prohibits unreasonable searches and seizures and requires a judicially sanctioned warrant supported by probable cause before a search or seizure can be conducted.[125] The AWA requires a search warrant be obtained before a court can grant any motion pursuant to the statute.[126] Because the government must first obtain a search warrant before using the authority of the AWA to obtain a motion to compel private companies to assist it, the Fourth Amendment requirements have been satisfied.[127] According to a Congressional Research Report, "Since the government obtained a valid probable cause warrant in this case, Apple is not contesting the search of the device under the Fourth Amendment. Thus, any privacy interest involved must derive from some other constitutional, statutory, or extra-constitutional source."[128] The matter at hand poses little threat to individual privacy rights because, in order for the AWA to be utilized, the government must first obtain a search warrant and therefore establish probable cause, which satisfies the Fourth Amendment.[129] There are, of course, still privacy concerns in the sense that individuals have an interest in having their data protected, but there is no Fourth Amendment claim.

As exemplified by these arguments, courts struggle to determine what statutes to apply, how to apply them, and whether such applications violate the constitution. The current statutory framework provides less than clear guidance on balancing the needs of companies and the government in an area of continual technological advancements and pervasive tension between security and privacy. This problem is exacerbated by the fact that these cases are generally very fact-specific and technical, making it difficult for courts to apply the law consistently and in a way that takes into account the various interests involved.

---

124. Ruthann Robson, *Apple Responds to Order to "Unlock" IPhone*, CONSTITUTIONAL LAW PROF BLOG (Feb. 25, 2016), http://lawprofessors.typepad.com/conlaw/2016/02/apple-responds-to-order-to-unlock-iphone.html.

125. U.S. CONST. amend. IV.

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

127. *See* Brief for Greg Clayborn et al., *supra* note 114, at 10–11.

128. THOMPSON & JAIKARAN, *supra* note 22, at 16 n.113.

129. *See* U.S. CONST. amend. IV (stating "but upon probable cause . . .").

III. REFORMS AND SOLUTIONS

The conflicting interests of the need for increasingly stronger encrypted devices and of the government to thwart cybercrimes cannot be reconciled within the current system. The Apple case highlights how complex these issues can be, as well as how difficult it can be for a court to determine the proper outcome of these cases. Without reform, the Going Dark problem and cybercrime will continue to plague private actors and the government alike. This Part will first describe why the judicial branch is not the proper branch to solve issues of this kind. This Part will then propose that Congress should create an agency capable of addressing these concerns more nimbly than Congress and with more accuracy than the courts. Finally, this Part will address potential criticisms of the proposed law reform.

A. The Courts Alone Are Not the Proper Branch for Determining the Outcomes of These Situations

1. Congress is Better Equipped to Handle these Issues than the Judicial Branch

The judicial branch is not the branch best equipped to determine the outcome of compelled decryption cases. Rather, Congress should use its power to create an administrative body uniquely suited to handling Digital Security issues. There are three primary reasons the courts are not well equipped to determine the outcome of these issues: (1) the issue is one of public policy; (2) the issue involves extremely complicated and ever-changing technology; and (3) the courts are limited to applying antiquated or ill-suited law.

First, to arrive at a sensible result, the decision maker must, in each case, make a holistic ruling by taking into account issues such as national security, public safety, data security, individual privacy, innovation, and corporate competitiveness.[130] The courts are not the proper venue to balance these interests, as they are limited to considering the interests of parties involved and the relevant law at the time. This decision will affect every person, corporation, and government entity that uses encryption software. It is well-established that the legislative branch is the preferable governmental branch to determine issues that primarily concern public policy.[131]

130. *See* Digital Security Commission Act, H.R. 4651, 115th Cong. § 12 (2016).

131. *See, e.g.*, Noah Feldman, *Congress is Best to Decide the Apple-FBI case*, THE COM. APPEAL (Feb. 24, 2016), http://www.commercialappeal.com/opinion/national/noah-feldman-con

Unlike the judicial branch, the legislative branch can utilize tools such as appointing committees, inviting and considering public discourse and lobbying, amending statutes, and—as this Note advocates—delegating responsibilities to administrative bodies.[132] Indeed, according to one constitutional and international law professor at Harvard Law School, Noah Feldman, "courts that are pretty good at interpreting statutes or applying the Constitution generally aren't very good at identifying and weighing major domestic and international public policy consequences . . . . In the U.S. system, Congress is supposed to make difficult public policy decisions."[133] Furthermore, the Supreme Court in *INS v. Chadha* noted that Congress is uniquely suited to make laws because of the Framers' decision "that the legislative power of the Federal Government be exercised in accord with a *single, finely wrought* and *exhaustively* considered procedure."[134]

Second, the technological aspects of these matters are extremely complicated and rapidly evolving, such that the courts will not be able to keep pace. Indeed, several leaders in the technology industry collectively stated that "[i]n light of rapidly evolving technology and its tremendous social benefits, Congress is better suited to confront the issues here."[135] Congress has the power to call upon experts, create committees, hear from various lobbyists, and address situations without needing to wait for a party to file a claim. Unlike the courts, Congress is able to take into account factors outside of the case at hand and weigh the benefits and harms to the public at large, whereas the courts are limited to only considering the parties directly involved and the applicable statutes.

The aforementioned Eastern District of New York Apple case demonstrates that the legislative branch is better equipped than a court to determine the outcomes of these issues. In that case, Judge Orenstein's ruling was that none of the factors—the closeness of Apple to the matter, the burdensomeness on Apple, or the necessity of Apple's assistance—were such that it justified imposing the obligation to assist the government's investigation on Apple against its will. The problem is that none of the considerations in that analysis concern legal matters; they are all matters of fact, many of

---

gress-is-best-to-decide-the-apple-fbi-case-2c76ea7e-ff9a-6dd8-e053-0100007fb85b-369913001.html.

132. *See generally The Legislative Process: Overview*, CONGRESS.GOV, https://www.congress.gov/legislative-process (last visited Oct. 29, 2016).

133. Feldman, *supra* note 131.

134. Immigration and Naturalization Serv. v. Chadha, 462 U.S. 919, 951 (1983) (emphasis added).

135. *See* Brief of Amici Curiae 1, *supra* note 8, at 10.

which deal with complex technological issues. For example, the burdensomeness factor would require the court to take into account all of the aspects involved with creating new software such as the cost of paying engineers to do so, the difficulty of accomplishing such a task, the equipment needed to complete it and the difficulty of acquiring said equipment, whether such a task would require moving to or even building a new facility, and many other considerations. As is evidenced by Judge Orenstein's ruling, technological facts are often the determining factors in these cases.[136] Such factors can be extremely complicated, especially when dealing with software code, encryption software, backdoors, and other technological issues.[137] Given this complexity, experts are increasingly needed to determine the correct results of these cases. Congress is better equipped to deal with this issue because it can—and should—create an administrative body with experts in the field to more accurately determine the correct outcome of these cases. Furthermore, because of the ever-changing landscape of technology, courts will always have the problem of being limited by legislation that will continue to become outdated. In a brief supporting Apple in the San Bernardino case, several security and cryptography experts stated, "The AWA's authority to issue writs to non-parties simply does not account for the public-security dangers this Court's Order creates, nor the future risks that future orders will also pose. The plain language of the statute creates no obligations and gives no guidance to courts considering the very important and technologically nuanced underlying security risks associated with mandating forensic access to private data."[138]

While courts are limited to applying current legislation, Congress is the sole branch authorized to "update a technologically antiquated statute to address the new and rapidly evolving era of computer and cloud-stored, processed and produced data."[139] It is worth noting that Congress is, however, also limited because each time it passes legislation it will quickly become outdated. Thus, the need for the creation of an administrative body is clear. Digital security technology grows at such a rate that the only way to

136. In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 355–63 (E.D.N.Y. 2016).

137. *See generally id.*

138. Brief for iPhone Security and Applied Cryptography Experts as Amici Curiae Supporting Apple, Inc.'s Motion's to Vacate Order Compelling Apple, Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 22, In re Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. 15-0451 (C.D. Cal. Mar. 22, 2016).

139. Motion to Vacate, *supra* note 35, at 18.

effectively regulate it is to create a living, breathing administrative body that can make rules and decisions quickly and accurately enough to keep up with it.

Third, there is a clear lack of legislation, and, thus, the courts do not have sufficient tools to correctly determine the outcome of cases. For example, in the San Bernardino case, the only applicable statutes were CALEA, which may or may not apply, and the AWA, which is supposed to be used only as a gap-filler. It seems inconceivable that courts should be forced to determine issues pertaining to the latest encryption software protocols of 2016 and beyond armed with only a gap-filling statute written in 1789. Furthermore, according to Professor Feldman, "As written, the laws governing the granting of warrants don't provide sufficient latitude for a court to weigh the dangers of requiring [private companies such as] Apple to write new code against the corresponding gains for policing and national security."[140] Finally, beyond the fact that Congress is better equipped to solve this issue, relying on the courts to do so violates the separation of powers doctrine.

2. Allowing the Courts to Determine this Matter Forces them to Violate the Separation of Powers Doctrine

It is well established that courts may not exercise the legislative power by repurposing statutes to meet the evolving needs of society.[141] Allowing the courts to determine the outcomes of these cases, given the lack of legislation and strong public policy consequences, puts them in a situation in which they are responsible for weighing the aforementioned various interests and essentially determining an extremely important issue of public policy. The courts are being put in a position where they are essentially functioning as the legislature, which constitutes a violation of the separation of powers doctrine.[142] Indeed, in *Baker v. Carr,* the Supreme Court explained that courts should not make rulings that are, at bottom, "political questions."[143] The Court enumerated several factors to

140. Feldman, *supra* note 131.

141. Robson, *supra* note 124 (citing Clark v. Martinez, 543 U.S. 371, 391 (2005) (Thomas, J., dissenting)).

142. The separation of powers doctrine is a "political doctrine of constitutional law under which the three branches of government (executive, legislative, and judicial) are kept separate to prevent abuse of power. Also known as the system of checks and balances, each branch is given certain powers so as to check and balance the other branches." *Separation of Powers*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/separation_of_powers (last visited Oct. 29, 2016).

143. *See* Baker v. Carr, 369 U.S. 186, 209–11 (1962).

use in determining whether a question is a political question, including whether there is an "impossibility of deciding [the issue] without an initial policy determination of a kind clearly for nonjudicial discretion."[144] Courts determining this issue would have to decide if and when the government can compel private companies to assist it in investigations, which should constitute a "initial policy determination" as defined in Baker. Such policy determinations are better left to Congress.[145]

The need for new clarifying legislation is clear. The reason there is so much debate about this issue is because Congress has not made a clear legislative decision, hence the argument about whether the AWA may be used to fill the missing gaps in these situations.[146] Thus, the courts are put in a position where they must attempt to make the law by making rulings with limited statutory guidance and to potentially give new meaning to statutes instead of allowing Congress to update antiquated legislation or adopt new legislation.[147] Indeed, Apple convincingly argued, "[Avoiding public debate] seems fundamentally inconsistent with the proposition that such important policy issues should be determined in the first instance by the legislative branch after public debate—as opposed to having them decided by the judiciary in sealed, ex parte proceedings."[148]

Finally, in *INS v. Chadha*, the Supreme Court held that "Congress has plenary authority in all cases in which it has substantive legislative jurisdiction, so long as the exercise of that authority does not offend some other constitutional restriction."[149] The fact that Congress has already grappled issues of encryption and digital security with legislation such as CALEA demonstrates that Congress has the authority and indeed the duty to solve this issue.

---

144. *See id.* at 217; Immigration and Naturalization Serv. v. Chadha, 462 U.S. 919, 941 (1983).

145. Feldman, *supra* note 131.

146. *See* In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 353 (E.D.N.Y. Feb. 29, 2016) (Judge Orenstein noted there is some gap which Congress has not addressed, and that the question at hand is to determine whether the AWA can fill that gap).

147. While it is difficult to prove, the government might very well be attempting to "short-circuit public debate on this controversy," as Apple claims, by using the courts, which should raise suspicion of an attempt to violate the separation of powers doctrine. In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court, 2015 WL 5920207, at *3 n.1.

148. In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court, 2015 WL 5920207, at *3 n.1.

149. *Chadha*, 462 U.S. at 923 (citing Buckley v. Valeo, 424 U.S. 1 (1976)).

B. Solution

In order to correctly balance the many and heavily-weighted competing interests revolving around the issue of device encryption, Congress should enact a statute that creates an administrative agency with both rulemaking and adjudication powers pertaining to digital security, including encryption. An administrative adjudicative agency could solve these problems because it would not be constrained by many of the problems the courts and Congress face. In February 2016, several members of Congress introduced the Digital Security Commission Act of 2016 for the purpose of creating a temporary national encryption panel.[150] The bill has only been introduced in the House of Representatives and, according to LexisNexis Bill Tracking, the bill has a "low chance to pass to the next stage."[151] Even if this bill were to pass, the Agency proposed in this Note (referred to as the "Digital Security Agency") is unique in that, although it would seek to accomplish many of the same goals as the Digital Security Commission, it would go further than this bill does and would accomplish its goals by granting the agency power to make decisions. The Digital Security Commission Act of 2016 contains several useful ideas, however, it does not provide the national encryption panel any power to make decisions, and instead only serves to make periodic reports to Congress to advise it about the various benefits and risks associated with encryption technology. The Digital Security Agency would seek to accomplish many of the goals enumerated in Digital Security Commission Act of 2016, but instead of creating a panel, it would create an adjudicative agency that could hold hearings and make rulings rather than simply advise Congress. The statute this Note proposes would go much further than the Digital Security Commission Act by granting the agency the power to not only consult with experts in the field to make rules, but also to make adjudicative decisions to react to these situations more nimbly than Congress and with more resources than the courts. Finally, the Digital Security Agency would also be responsible for making periodic recommendations to Congress so that, in the event new legislation is needed, Congress will be better informed to respond.

---

150. Digital Security Commission Act, H.R. 4651, 115th Cong. (2016).

151. Digital Security Commission Act of 2016, 114 Bill Tracking H.R. 4651, https://advance.lexis.com/document/documentlink/?pdmfid=1000516&crid=07a7d614-57d5-4892-897d-c8313624edd8&pdlinktype=document&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A5J6K-R3K1-JCTT-01WM-00000-00&pdcontentcomponentid=7425&action=linkdoc&ecomp=-9zdk&prid=22264b76-524f-4a1e-b980-9fb708a35770.

The Digital Security Agency would accomplish the purpose enumerated in the Digital Security Commission Act, but would have additional powers to accomplish these goals. The mission of the Digital Security Commission Act of 2016 is as follows:

> To bring together leading experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community, global commerce and economics, and the national security community to examine the intersection of security and digital security and communications technology in a systematic, holistic way, and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace.[152]

The Digital Security Agency would have two ways to make policy and two corresponding branches: an adjudication branch and a rulemaking branch. The adjudication branch would be responsible for holding adjudicatory hearings and making orders when the government seeks to compel private actors to assist it in its investigations. The rulemaking branch would be responsible for conducting research and consulting experts, private companies and the government in order to make rules and recommendations to Congress. By utilizing the two separate branches, the Agency would be more nimble than Congress, and more accurate than the courts.

1. The Adjudication Branch

The Digital Security Agency would have the power to hold hearings to determine on a case-by-case basis whether or not the government could—after obtaining a search warrant issued by a court—proceed to compel a third party to assist in decryption efforts. Essentially, law enforcement would have to first obtain a normal search warrant by showing probable cause. After having obtained a search warrant, if law enforcement found it was unable to decrypt a device, network, or other digital source, it would file a claim to the Digital Security Agency that would in turn adjudicate the matter between law enforcement and the private company. In other words, the Digital Security Agency's primary responsibility would be to respond when law enforcement encounters the Going Dark problem.

---

152. Digital Security Commission Act, H.R. 4651, 115th Cong. § 3(b) (2016).

The adjudication branch should be comprised of an odd number of qualified administrative law judges.[153] In addition to the administrative law judges, there should be a council of experts to advise the judges on matters of fact. The council of experts should have members from the following areas: "(1) cryptography (2) global commerce and economics (3) federal law enforcement (4) state and local law enforcement (5) consumer-facing technology sector (6) enterprise technology sector (7) the intelligence community (8) the privacy and civil liberties community."[154] There should also be at least one member nominated by an interest group in support of private companies such as the Software Alliance[155] or the Information Technology Industry Council.[156] The council of experts would have no power to make the final rulings, however the administrative law judges should be advised to strongly consider the opinions of these experts when determining the outcomes of these matters. If the adjudicative branch determines by a simple majority that the government is entitled to compel a private company to provide assistance, it would issue an order stating that the company has to comply. The order would have the same effect as if a normal court granted a motion to compel a company to provide assistance. Companies could appeal this order to a federal court of appeals, but only on the grounds of a constitutional violation.

The enabling act should advise the administrative law judges to consider the factors laid out by Judge Orenstein: the closeness of the private company's relationship to the underlying criminal conduct and government investigation; the burden the requested order would impose on the private company; and the necessity of imposing such a burden on the private company.[157] In addition, the enabling act should advise the adjudication branch to consider the probability that decrypting the device in question would lead to thwarting a crime or solving an investigation. The enabling act

---

153. "The Administrative Law Judge (ALJ) function was created by the Administrative Procedure Act (APA) in 1946 to ensure fairness in administrative proceedings before Federal Government agencies." *Qualification Standard for Administrative Law Judge Positions*, U.S. OFFICE OF PERS. MGMT, https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/specialty-areas/administrative-law-judge-positions/ (last visited Oct. 29, 2016) [hereinafter *Qualification Standard*].

154. Digital Security Commission Act, H.R. 4651, 115th Cong. § 4(b) (2016).

155. *See generally* THE SOFTWARE ALLIANCE, http://www.bsa.org/ (last visited Oct. 29, 2016) [hereinafter THE SOFTWARE ALLIANCE].

156. *See generally* INFO. TECH. INDUS. COUNCIL, https://www.itic.org/ (last visited Oct. 29, 2016) [hereinafter INFO. TECH. INDUS. COUNCIL].

157. In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016).

should, however, give the agency discretion to consider other factors, as new factors will almost certainly arise as technology advances. The orders the Digital Security Agency makes should be binding on the Agency itself so that it has to follow precedent, unless the rulemaking branch creates a rule that effectively overrules a decision. In the event new discoveries are made that have a substantial effect on a ruling the court has already made, the rulemaking branch would be responsible for creating a new rule to address the concern. This way, the adjudicative branch will ensure predictable results, but will also have the ability to quickly adapt to the ever-changing landscape of digital security.

The adjudicative branch is necessary to the agency because, while the rulemaking branch can conduct research and use notice and comment rulemaking, there must still be a method for the government to obtain an order compelling a private company to assist it. Regardless of how comprehensive the rules are, there will almost certainly be some disputes that must be resolved by an adjudicator. Furthermore, because technology changes so often, there will almost certainly be disputes for which there is no applicable rule. The adjudication branch will also be instructive for the rulemaking branch, which can compile adjudicative rulings into comprehensive rules. The adjudicative branch is essential to the agency's ability to respond to disputes as they arise, and the panel of experts and the preference given to administrative law judges with some relevant expertise will lead to more accurate decisions than the courts could make.

2. The Rulemaking Branch

The primary responsibilities of the rulemaking branch would be to promulgate rules under the APA via notice and comment rulemaking pursuant to APA §553, and to provide periodic reports to Congress.[158] This branch would be responsible for providing notice, the opportunity to comment, and publication of all rules with a general statement of basis and purpose of all rules adopted as proscribed by APA §553.[159] By using notice and comment rulemaking, the agency will be able to more accurately ascertain the interests and concerns of those who will be affected by the rules. Rules made by this branch should be used by the adjudication

158. Administrative Procedure Act, 5 U.S.C. § 553 (1966).

159. *Id.*

branch in its rulings. This branch would also be responsible for submitting semi-annual reports to Congress detailing: (1) all agency action since the preceding report; (2) issues or controversies the agency believes present a problem or will become problematic in the foreseeable future; (3) an assessment of the most immediate and dangerous cyber security threats and potential methods to solve them; and (4) any information not specifically stated the agency believes is relevant and important.

This branch should be comprised of at least nine members for the purposes of making rules and sending reports to Congress regarding digital security and encryption. Like the panel of experts in the adjudicative branch, the rulemaking branch should be required to have at least one member with expertise in each of the following areas: "(1) Cryptography (2) Global commerce and economics (3) Federal law enforcement (4) State and local law enforcement (5) Consumer-facing technology sector (6) Enterprise technology sector (7) The intelligence community (8) The privacy and civil liberties community,"[160] as well as a member with some federal lawmaking experience. There should also be at least one member nominated by an interest group in support of private companies such as the Software Alliance[161] or the Information Technology Industry Council.[162] This highly qualified team would be more informed than the average member of Congress, and could create rules more quickly because it would not be burdened by the procedures Congress must follow to pass bills.

The rulemaking branch provides the ideal mechanism for quickly making rules while considering all of the competing interests. First, the rulemaking branch will almost certainly lead to better rules than Congress alone could create. By utilizing notice and comment rulemaking, the branch will allow for greater public input into the decision, thereby ensuring the agency is adequately informed of all competing interests. This branch also will allow for more comprehensive decision making than the adjudicative branch. The rulemaking branch will also benefit the agency because it will be able to impose comprehensive rules at once on all similarly situated parties, as opposed to the adjudicative branch, which will be limited rulings on the parties involved in hearings. The qualified officers of the rulemaking branch will able to foresee problems before claims arise in some cases and will therefore be able to create rules the adjudicative branch can apply in the event

160. Digital Security Commission Act, H.R. 4651, 115th Cong. § 4(b) (2016).

161. *See generally* THE SOFTWARE ALLIANCE, *supra* note 155.

162. *See generally* INFO. TECH. INDUS. COUNCIL, *supra* note 156.

that such a claim is eventually brought; this will decrease the likelihood that the adjudicative branch will have to "stretch" a rule to apply to a situation or give a rule new meaning, and will lead to more predictive outcomes. Finally, because rules must be published as soon as they are promulgated, regulated parties will have advance knowledge of their legal duties and can design their digital security protocols accordingly. Thus, the rulemaking branch is essential to the efficiency and comprehensiveness of the agency as a whole.

3. Appointment and Removal

The enabling act should specify that members for both the adjudicative branch and the rulemaking branch should be appointed by the President with the advice and consent of the Senate, pursuant to the Appointments Clause. In order to be selected to serve as an administrative law judge, candidates should be required to meet all the qualifications enumerated by the APA.[163] Special preference should be given to candidates who also have expertise in one of the aforementioned relevant areas of expertise. The enabling act should also restrict the removal of administrative officials and administrative law judges to "good cause" to insulate the agency from political pressure as much as possible.[164] Finally, in the event of a vacancy in any position, that member should be replaced in the same manner in which he or she was appointed.

C. Potential Criticisms of the Agency Approach

Critics of the agency approach will likely argue that the courts are in fact better equipped than an administrative agency because courts are better at upholding constitutional rights, which constitutes an equal if not greater concern than the potential public policy consequences. In *Marbury v. Madison*, the Court established that all cases arising under the Constitution are to be reviewed by the judicial branch.[165] The Court also stated, "It is emphatically the province and duty of the judicial department to say what the law

163. *Qualification Standard*, *supra* note 153.

164. *See* Morrison v. Olson, 487 U.S. 654, 686 (1988) (citing 28 U.S.C.S. § 596(a)(1)) (Court upheld the Independent Counsel Act, in which a prosecutor appointed to conduct an investigation who alleged wrong-doing by officials could be removed only for good cause).

165. *See* Marbury v. Madison, 5 U.S. 137, 153 (1803).

is."[166] Critics may also argue that, oftentimes, agencies do not live up to expectations and fall short of the large responsibilities they are given. Particularly because of the high volume of anticipated cases and issues in the future, critics will likely be skeptical that this agency will be able to handle all of its responsibilities.

Admittedly, there are constitutional concerns and questions of law involved in some of these cases, but the proposed agency approach takes this into account by recommending that the agency include administrative law judges. The Administrative Procedure Act of 1946 was created to establish the administrative law judge function to "[e]nsure fairness in administrative proceedings before Federal Government Agencies."[167] The inclusion of administrative law judges would help to ensure that the agency correctly and fairly interprets issues of law. Furthermore, the inclusion of people with federal law making experience in the rulemaking branch will decrease the likelihood that any unlawful rules are created. Given that administrative law judges are as qualified as ordinary judges, there is no reason to believe the agency will not correctly and fairly determine laws and avoid making rulings contrary to the letter and spirit of the Constitution. Furthermore, there are plenty of other agencies already in place that make rules and regulations that relate to constitutional and legal concerns and are highly effective. There is no reason to believe that this agency would be less effective than the many successful agencies that are essential to the United States government.

Furthermore, all of the rules and decisions the agency makes can be reviewed by courts or overruled by a statute passed by Congress. Under the proposed agency approach, in the event that a party believes its constitutional rights have been violated, that party can always appeal the agency's rulings. In such a situation, the proposed agency would have still served its purpose, as the only appeals would be decisions in which there is a potential constitutional violation and not those revolving around the public policy concerns of encryption.

The ability of agencies with adjudicative judges to succeed where the courts have failed has been well documented, as exemplified by agencies such as the NLRB, which has been successfully engaging in adjudicatory and rulemaking activities for over 80 years.[168] While

166. *Id.* at 177.

167. *Qualification Standard*, *supra* note 153.

168. *See generally National Labor Relations Board: 80 Years of Protecting Employee Rights*, NAT'L LABOR RELATIONS BD. (2015), https://www.nlrb.gov/sites/default/files/attachments/basic-page/node-1536/NLRB%2080th%20Anniversary.pdf (illustrating the 80-year history and success of the National Labor Relations Board). Furthermore, according to scholars such as

the agency approach may be imperfect, given the nature and the difficulty of the issue, it seems to be a far superior approach than forcing the courts to determine the outcome of these matters with little to no legislative guidance.

CONCLUSION

Many believe that the question of reconciling competing encryption and digital security interests is one without an easy answer, and they are correct. The complexity of the situation and the interests at stake provide all the more reason for Congress to create an administrative agency to conduct trials as new issues arise and advise Congress on potential legislation for the future. If correctly implemented, the agency approach will ultimately provide the nation with the best policy for moving forward while simultaneously protecting the interests of national and digital security, privacy and public safety.

Michael L. Wachter, Professor of Law and Economics at the University of Pennsylvania Law School, "the NLRB has been largely successful and in one key area exceedingly successful." Michael L. Wachter, *The Striking Success of the National Labor Relations Act*, *in* PENN LAW LEGAL SCHOLARSHIP REPOSITORY, RESEARCH HANDBOOKS IN LAW AND ECONOMICS 427 (Cynthia L. Estlund ed., 2012). According to the Board, "The National Labor Relations Board (NLRB) has counted millions of votes, investigated hundreds of thousands of unfair labor practice charges, and issued thousands of decisions." *Graphs & Data*, NAT'L LABOR RELATIONS BD., https://www.nlrb.gov/news-outreach/graphs-data (last visited Oct. 29, 2016). Other examples of successful adjudicative agencies with rulemaking authority include the United States Environmental Protection Agency (EPA), the United States Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC).