SMU Science and Technology Law Review

Volume 19 | Number 2 Article 6

January 2016

Can You Keep a Secret: Some Wish to Ban Encryption Technology for Fears of Data Going Dark

Steven B. Taylor

Can You Keep a Secret?: Some Wish to Ban Encryption Technology for Fears of Data "Going Dark"

*Steven B. Taylor**

I. INTRODUCTION

A national debate is growing over the widespread distribution and use of unbreakable encryption technology in consumer electronics. In the interest of law enforcement and national security, some governmental officials have pushed to regulate against such technology to prevent data from "going dark."[1] Those concerned with individual privacy, on the other hand, welcome encryption and oppose government interference with its use and distribution.[2] This group includes large technology companies that have additional interests in maintaining customer satisfaction and sales figures.[3] These well-funded companies are poised to battle legal opponents that attempt to encroach on their efforts to secure privacy.[4]

Compounding the debate are recent exposures of seemingly unconstitutional government programs that target U.S. citizens in bulk data collection and mass surveillance efforts. Against this backdrop, tension has grown between the competing interests. This comment explores several constitutional and prudential challenges posed by proposals to stifle the use of encryption.

> Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously. Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds

---

* Steven B. Taylor is a J.D. candidate scheduled to graduate from the SMU Dedman School of Law in May 2017. Steven would like to thank Professor Jeffrey for delivering inspiring lectures and for guidance during the preparation of this comment. Steven would also like to thank his amazing wife, Kelli, for encouraging him and making it possible for him to focus.

1. *See* James B. Comey, Dir., Fed. Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Keynote Address as the Brookings Institute (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

2. *See* Steven Morgan, *Apple's CEO on Encryption: "You Can't Have a Back Door That's Only for the Good Guys"*, FORBES (Nov. 15, 2015, 6:57 AM), http://www.forbes.com/sites/stevemorgan/2015/11/21/apples-ceo-on-encryption-you-cant-have-a-back-door-thats-only-for-the-good-guys/#2443644112d7.

3. *See id.*

4. *See id.*

> contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means-to declare that the government may commit crimes in order to secure the conviction of a private criminal-would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face.[5]

II. HISTORY OF THE ISSUE

A. Government Privacy Infringements Lead to the Widespread Use of Strong Encryption

In June 2013, Edward Snowden, a former National Security Agency (NSA) contractor leaked classified documents revealing NSA surveillance of American telephone records pursuant to the § 215 of the Patriot Act.[6] Among the leaked documents was an order from a secret court authorized under the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008; the order required Verizon, on an "ongoing, daily basis," to provide the government with information on all telephone calls, and it forbade Verizon's disclosure of the order.[7] The document shows that "under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing."[8]

Days later, news outlets reported that the NSA had "obtained direct access to the systems of Google, Facebook, Apple and other US internet giants."[9] Through PRISM, a previously undisclosed program, NSA officials gained direct access to company servers in order to "collect material including search history, the content of emails, file transfers and live chats."[10]

The Protect America Act of 2007 initially enabled the NSA surveillance program by making changes to applicable U.S. surveillance laws.[11] Congress

5. Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting).

6. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see* Emma Roller, *This is What Section 215 of the Patriot Act Does*, SLATE (June 7, 2013, 1:17 PM), http://www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html.

7. *Id.*

8. *Id.*

9. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013, 3:23 PM), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

10. *Id.*

11. *See* Protect America Act, S. 1927, 110th Cong. (2007) (enacted).

reauthorized the applicable changes through the FISA Amendments Act of 2008 and renewed the changes in December 2012.[12] These statutes allow "the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US."[13] The statutes also create the possibility of warrantless collection of communications made entirely within the United States.[14] Under these statutes, the NSA developed PRISM to facilitate "extensive, in-depth surveillance on live communications and stored information."[15]

"These reports spoke to, and helped add fuel to, concerns among interest groups and a significant percentage of the public about perceived government abuses of privacy."[16] Suddenly, privacy became a mainstream topic in the conversations of ordinary citizens. Through what is now referred to as the "Snowden effect," U.S. citizens began to reevaluate the security of their private data and communications.[17]

B. Technology Companies Respond by Providing Strong Encryption to Allow Customers to "Go Dark"

Suspicion from other nations and privacy demands from their customers created market pressures that motivated both Apple and Google to enable strong encryption as the default setting for their mobile handheld devices.[18] Encryption is the process of converting readily discernable information into a format that is unrecognizable unless the reader has some secret information

12. Greenwald & MacAskill, *supra* note 9.

13. *Id.*

14. *See id.*

15. *Id.*

16. Jason M. Weinstein et al., *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era*, 52 AM. CRIM. L. REV. 729, 730 (2015); *see, e.g.*, David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES, Sep. 26, 2014, at A1, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html ("At Apple and Google, company executives say the United States government brought these changes on itself. The revelations by the former N.S.A. contractor Edward J. Snowden not only killed recent efforts to expand the law, but also made nations around the world suspicious that every piece of American hardware and software—from phones to servers made by Cisco Systems—have 'back doors' for American intelligence and law enforcement.").

17. *See* Trevor Timm, *The Snowden Effect: New Privacy Wins Await After Data Transfer Ruling*, THE GUARDIAN (Oct. 8, 2015, 7:15 AM), http://www.theguardian.com/commentisfree/2015/oct/08/snowden-effect-new-privacy-wins-data-transfer-ruling.

18. Comey, *supra* note 1.

that allows deciphering of the message.[19] A more commonly known, simplistic form of encrypted messages are cryptograms found in entertainment sections of newspapers. Deciphering newspaper cryptograms is a relatively easy task, but the methods used in computer encryption have become increasingly complex. These complex encryption methods have made deciphering practically impossible without complete knowledge of the secret encrypting method.[20] Deciphering encrypted information to the original format (e.g., video files, images, or simple messages) usually requires both knowledge of the encrypting method (publicly known) and knowledge of a piece of information called a key—often an extraordinarily large, random number that is kept private.[21] The encryption methods used by Apple and Google are unbreakable (i.e. Strong Encryption); even the companies themselves cannot decipher the information.

In October 2015, Apple explained to a federal judge in the Eastern District of New York that the company would be incapable of accessing data in devices running its newest operating system (iOS 8).[22] Apple explained, "[t]hose devices include a feature that prevents anyone without the device's passcode from accessing its data, including Apple itself."[23] The feature was adopted in 2014 amid "heightened privacy concerns following leaks by former National Security Agency contractor Edward Snowden about NSA surveillance programs."[24]

C. The Threat of "Going Dark" Has Prompted FBI Director Comey to Propose Banning Its Distribution

Law enforcement officials, accustomed to having limitless data access, are frustrated by hindrances to investigations resulting from the inability to access encrypted data; this problem is known as "going dark." FBI Director, James Comey, gave a speech at the Brookings Institute in October 2014 calling for legislation to compel the "assistance and cooperation" from technology companies in law enforcement investigations.[25] He proposed legislation

19. *What is Encryption, and Why Are People Afraid of It?*, How-To Geek, http://www.howtogeek.com/234642/what-is-encryption-and-why-are-people-afraid-of-it/ (last visited Sept. 19, 2016).

20. *Id.*

21. *Id.*

22. *See* Apple Inc. Response to Court's October 9, 2015 Memorandum and Order, *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 15-MS-1902 (E.D.N.Y. 2015), ECF No. 11.

23. Nate Raymond, *Apple Tells U.S. Judge 'Impossible' to Unlock New iPhones*, Reuters (Oct. 20, 2015), http://www.reuters.com/article/us-apple-court-encryption-idUSKCN0SE2NF20151020.

24. *Id.*

25. *See* Comey, *supra* note 1.

that would require companies to create products with a "front door" (as opposed to a "back door") key. The key would be held or accessible by government officials and available for use only after proper judicial review. It would allow officials to search the contents of seized, encrypted information.[26] The aim is to prevent information from "going dark" by proscribing the distribution of unbreakable encryption.

Director Comey classified two types of data: "data at rest" and "data in motion." Data at rest describes information stored on devices[27] and is usually encrypted through some variation of the conventional method described above.[28] In contrast, data in motion is information sent through a network (e.g., a text message sent through a wireless carrier network).[29] This type of data is vulnerable to interception before reaching its recipient. Accordingly, data in motion is usually encrypted before leaving the originator's device. The method used is often a more complex version of encryption called public-key cryptography, which involves the use of multiple keys.[30] Under Director Comey's plan, technology companies would likely provide cryptography in which the company also holds an additional key to both data at rest and data in motion.

D. Technology Companies Actively Support Strong Encryption

Technology industry leaders are prepared to oppose efforts aimed at disabling privacy-enabling encryption. Speaking at WSJDLive in October 2015, Apple CEO, Tim Cook, said, "I don't know a way to protect people without encrypting."[31] He further added, "You can't have a back door that's only for the good guys."[32] The Information Technology Industry Council (ITI)—members include Apple, Dell, Facebook, Google, Microsoft, IBM, Intel, and

26. *See id.*

27. *Id.*

28. *How PGP Works*, THE INT'L PGP HOME PAGE, http://www.pgpi.org/doc/pgpintro/ (last visited Sept. 19, 2016).

29. *See id.*

30. *Id.* ("The primary benefit of public key cryptography [over the conventional method described above] is that it allows people who have no preexisting security arrangement to exchange messages securely." Public key cryptography involves the use of two keys: a public key known to all and a private key known only to the recipient. The two keys are mathematically related in a way that is too complicated for even the most powerful computers to discern. That relationship, however, allows a message encrypted with the publicly known key to be decrypted only with knowledge of the private key. This method is increasingly becoming more common for networked communications.). *Id.*

31. Morgan, *supra* note 2.

32. *Id.*

Twitter—speaks globally for the technology sector.[33] ITI sent a letter to President Obama on June 8, 2015 that urged him to refrain from pursuing "any policy or proposal that would require or encourage companies to weaken [encryption]."[34] On November 19, 2015, ITI President and CEO, Dean Garfield, released the following statement:

> Encryption is a security tool we rely on every day to stop criminals from draining our bank accounts, to shield our cars and airplanes from being taken over by malicious hacks, and to otherwise preserve our security and safety. We deeply appreciate law enforcement's and the national security community's work to protect us, but weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys, which would almost certainly cause serious physical and financial harm across our society and our economy. Weakening security with the aim of advancing security simply does not make sense.[35]

In addition to the technology industry, equally important pushbacks have come from various security branches of the U.S. government. Speaking to the Atlantic Counsel in January 2016, NSA Director, Admiral Michael S. Rogers, said, "encryption is foundational to the future."[36] To quibble that "encryption is bad and we ought to do away with it [is] a waste of time."[37] Rather, the more important question is, "what's the best way for [security officials] to deal with it?"[38] "General Michael Hayden, former director of both the CIA (2006 to 2009) and the NSA (1999 to 2005) says FBI Director James Comey is wrong about encryption, and that America and the American people will be 'more secure' with unbreakable, end-to-end encryption."[39] The statements reflect the growing tension over the debate.

---

33. *Id.*

34. *Tech Industry Warns President of Risks in Compromising Encryption*, INFO. TECH. INDUS. COUNCIL (June 9, 2015), http://www.itic.org/news-events/news-releases/tech-industry-warns-president-of-risks-in-compromising-encryption.

35. *Tech Responds to Calls to Weaken Encryption*, INFO. TECH. INDUS. COUNCIL (Nov. 19, 2015), https://www.itic.org/news-events/news-releases/tech-responds-to-calls-to-weaken-encryption.

36. Michael S. Rogers, Dir., Nat'l Sec. Agency, *U.S. Cybercom and the NSA: A Strategic Look with ADM Michael S. Rogers* (Jan. 21, 2016), https://www.youtube.com/watch?v=WNTGO6OFgCo&feature=youtu.be&t=1532.

37. *Id.*

38. *Id.*

39. Bryan Chaffin, *Former Director of CIA and NSA Says FBI Is Wrong About Apple's Encryption*, THE MAC OBSERVER (Feb. 19, 2016, 2:38 PM), http://www.macobserver.com/tmo/article/former-director-of-cia-and-nsa-says-fbi-is-wrong-about-apples-encryption.

In February 2016, tensions grew even stronger between technology companies and the U.S. government when a U.S. District Court for the Central District of California ordered Apple, Inc. to unlock an encrypted iPhone.[40] At the request of the FBI, and under the authority of the All Writs Act of 1789, the Magistrate Judge ordered Apple to build "a version of iOS that bypasses security [in a way that] would undeniably create a backdoor."[41] Intending to oppose the order, Apple warned, "while the government may argue that its use would be limited to this case, there is no way to guarantee such control."[42] Apple cited privacy as its guiding concern:

> The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.[43]

The order, described by Apple as "unprecedented," comes under unusually compelling circumstances.[44] The iPhone targeted by the order was used by Syed Rizwan Farook, the terrorist who "carried out the San Bernardino shootings that killed 14 people and wounded 22 others at a holiday party."[45] The shooting had a "large emotional impact while also demonstrating the danger posed by armed militants."[46] More compelling, the iPhone's owner is Farook's former employer, a local government that consents to the search of the phone.[47] These sympathetic facts make a strong case in favor of the unprecedented order.[48]

Unsurprisingly, the order and Apple's public response have heightened the attention U.S. news media circles are giving to the encryption debate. The

40. *See* David Ingram & Dan Levine, *Apple Likely to Invoke Free-speech Rights in Encryption Fight*, REUTERS (Feb. 19, 2016, 1:21 AM), http://www.reuters.com/article/us-apple-encryption-freespeech-idUSKCN0VS025.

41. *What is Encryption, and Why Are People Afraid of It?*, HOW-TO GEEK, http://www.howtogeek.com/234642/what-is-encryption-and-why-are-people-afraid-of-it/ (last visited Sept. 19, 2016).

42. *Id.*

43. *Id.*

44. *Id.*

45. Ingram & Levine, *supra* note 40.

46. *Id.*

47. *Id.*

48. *See id.*

topic has even spread into the 2016 Presidential race.[49] Candidates, usually careful to avoid commitment, face direct questions regarding the issue, and their various positions are not easily categorized along party lines.[50] But candidates who take a strong stance risk being labeled anti-privacy or pro-terrorist.

Proponents of Director Comey's plan essentially describe the problem as a classic case of merely balancing the "friction between individual liberty and collective security."[51] The thrust of their argument is that the pervasive use of encryption—"going dark"—"creates an unacceptable obstacle to lawful searches and surveillance that are necessary to protect the public from criminal and national security threats."[52] They argue that, when reasonable, the Fourth Amendment authorizes governmental search and surveillance,[53] but the use of encryption acts as an absolute restriction on this vested governmental right. But does it? Does the right to search and surveil include the power to compel all citizens to communicate and record information in a way such that their words can be heard and their actions be seen? Does the interest in searching and surveilling empower Congress, the President, or the Courts to place burdens upon those who seek to preserve privacy? May they forbid whispering?

III. CONSTITUTIONAL ANALYSIS

Proponents have tailored the plan to ban the distribution of encryption to circumvent the Fourth Amendment's purpose without violating its black-letter text. At first glance, the plan appears to suggest clever means of aiding law enforcement and national security officials without violating the technicalities of the Constitution. But a more careful examination suggests otherwise.

Notwithstanding the aim of the Comey plan, it likely still violates the Fourth Amendment right to be secure against unreasonable searches and seizures. The plan also likely violates the fundamental right to privacy. Even worse, these violations may not be redressable. Accordingly, this analysis begins with a discussion of standing requirements.

---

49. *See* Michael Morisy, *Where Do the Presidential Candidates Stand on Encryption?*, WINDOWS IT PRO (Feb. 18, 2016), http://windowsitpro.com/security/where-do-presidential-candidates-stand-encryption.

50. *See id.*

51. *See* Geoffrey S. Corn, *Averting the Inherent Dangers of "Going Dark": Why Congress Must Require A Locked Front Door to Encrypted Data*, 72 WASH. & LEE L. REV. 1433 (2015).

52. *Id.* at 1434.

53. *Id.*

A. If a Legislative Ban on the Distribution of Strong Encryption Is Unconstitutional, Abuse Is Likely Not Redressable

The Fourth Amendment provides that "[t]he right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon *probable cause* . . . ."[54] FBI Director Comey calls for tailoring legislation in such a way as to defeat the Fourth Amendment's purpose without violating the specific requirements typically at issue in Fourth Amendment cases and controversies.

To circumvent the Fourth Amendment, Congress would ban technology companies (e.g., Apple and Google) from distributing strong encryption capabilities. These companies would be required to maintain access to all the devices they sell. With a search warrant, the government could compel companies to provide access to information contained on any device. Thus, the potential legislation would essentially conscript technology companies to seize information so the government could then search the information after a court's approval. Such a situation would be similar to the leaked FISA court order allowing the search of Verizon's U.S. customers' phone records.[55]

While this legislation seems tentatively permissible, it still begs the question: is it constitutional? In 2013, *Clapper v. Amnesty International USA* asked a similar question.[56] In a 5-4 decision, the U.S. Supreme Court held the complaining party did not have standing to sue.[57] Ordinarily, if legislation oversteps the constitutional limits of congressional authority, Article III Courts can strike down the legislation.[58] Authority to do so, however, is limited to actual cases and controversies.[59] "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue."[60] Standing requires an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[61] After establishing standing, the case can move on to discovery where the parties have the ability to ascertain the evidence necessary to prove their case.[62]

---

54. U.S. CONST. amend. IV (emphasis added).

55. *See* Greenwald & MacAskill, *supra* note 9.

56. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1142 (2013).

57. *Id.* at 1142–43.

58. Marbury v. Madison, 5 U.S. 137, 178 (1803).

59. U.S. CONST. art. III, § 2, cl. 1.

60. *Amnesty Int'l*, 133 S. Ct. at 1146 (citations omitted) (internal quotation marks omitted).

61. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010).

62. Lujan v. Nat'l Wildlife Fed'n, 497 U.S. 871, 906 (1990).

Where the injury is an invasion of privacy, showing injury, whether actual or imminent, proves to be prohibitively difficult,[63] and "[a]ll too often the invasion of privacy itself will go unknown."[64] This was the case in *Amnesty International*,[65] in which the plaintiffs challenged the constitutionality of a 2008 amendment to FISA that "established a new and independent source of intelligence collection authority, beyond that granted in traditional FISA."[66] The amendment removed the requirement that the government must "demonstrate *probable cause* that the target of the electronic surveillance is a foreign power or agent of a foreign power."[67] The original FISA of 1978 included the requirement, and removal of the requirement seems a blatant defiance of the Fourth Amendment text mandating that search warrants may only issue upon a showing of "probable cause."[68] For this reason, the plaintiffs contended that the legislation was unconstitutional.[69] However, the case was never heard on its merits due to lack of standing.[70]

To show actual and imminent injury, plaintiff Scott McKay pleaded that as a lawyer he represented several suspected international terrorists, such as Khalid Sheik Mohammed.[71] Among McKay's clients were suspected terrorists formerly detained at Guantánamo Bay, who had since been acquitted of charges against them.[72] Prior to 2008, the U.S. government had intercepted about "10,000 telephone calls and 20,000 email communications" involving one of McKay's clients.[73] Knowing this, McKay believed that it was highly likely the government would monitor his telephone communications with his clients under the authority of the 2008 FISA amendment, but in violation of the Fourth Amendment.[74] Accordingly, to avoid violations of confidentiality, McKay would not communicate unless a matter was urgent, and then he would only communicate in person, which involved expensive and time-consuming travel arrangements.[75] In a 5-4 ruling characterizing the injury as

63. *See Amnesty Int'l*, 133 S. Ct. at 1138.

64. Bartnicki v. Vopper, 532 U.S. 514, 549 (2001) (Rehnquist, J., dissenting).

65. *Amnesty Int'l*, 133 S. Ct. at 1143.

66. *Id.* at 1144 (citations omitted).

67. *Id.* (emphasis added).

68. *Id.* at 1143; *see* U.S. CONST. amend. IV.

69. *Amnesty Int'l*, 133 S. Ct. at 1142.

70. *Id.* at 1143.

71. *Id.* at 1156–57 (Breyer, J., dissenting).

72. *Id.* at 1157 (Breyer, J., dissenting).

73. *Id.* (Breyer, J., dissenting) (citations omitted).

74. *Id.* (Breyer, J., dissenting).

75. *Amnesty Int'l*, 133 S. Ct. at 1164 (Breyer, J., dissenting).

"speculative," the Court held that McKay did not meet the injury requirement requisite for standing.[76]

Warrantless wiretaps are, by their nature, designed to go undetected. Some may consider it a lesser problem if the victim is unaware, but "[i]f anything, [the violation] is more offensive because the [victim] is completely unaware of the invasion of privacy."[77] Because the violation is clandestine, to challenge the constitutionality of a congressional act that permits unconstitutional violations of privacy, the challenger must rely on a showing of imminent injury (rather than actual injury) in order to proceed to discovery, where he or she may gather evidence to show actual injury.[78] But the standing requirements, as applied in *Amnesty International*, are so prohibitive that perhaps nobody can satisfy them. After all, who is more likely to be the subject of a warrantless wiretap than an attorney for suspects of international terrorism?

If Scott McKay cannot show that violation of his Fourth Amendment rights is imminent, it seems doubtful that anyone can without first having concrete evidence. However, such proof was provided in a subsequent case heard by the Second Circuit, *American Civil Liberties Union v. Amnesty International*.[79] That case was an action seeking to enjoin the NSA from further collection of data. The plaintiffs in the case claimed to be actually injured because they were Verizon customers and the Snowden leaks evidenced that the NSA had violated their Fourth Amendment.[80] The court held in their favor that standing was conferred, because these plaintiffs "need not speculate that the government has collected, or may in the future collect, their call records. To the contrary, the government's own orders demonstrate that appellants' call records are indeed among those collected as part of the telephone metadata program."[81] In other words, without a government whistleblower, like Snowden, plaintiffs like these or Scott McKay have very little chance of seeking redress for statutes that blatantly call for violations of the Fourth Amendment.

Director Comey proposes that Congress restrict technology companies' ability to distribute strong encryption capabilities. Proponents of this proposal argue it conforms to the Fourth Amendment. However, if the plan does violate the Constitution, courts will likely never have the occasion to rule on the law. Under *Amnesty International*'s standing requirements, the political process may serve as the only means of protecting privacy rights. The President and all of Congress have sworn to uphold the Constitution. As the only

76. *Id.* at 1143.

77. Berger v. N.Y., 388 U.S. 41, 65 (1967).

78. *See Amnesty Int'l*, 133 S. Ct. at 1143.

79. Am. Civil Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015).

80. *Id.* at 799.

81. *Id.* at 801.

line of defense, these elected officials would be derelict not to consider the constitutional perspectives below. "Only by striking at all aspects of the problem can privacy be adequately protected."[82]

B. To Regulate Against the Distribution of Strong Encryption Would Directly Violate The Fourth Amendment

"'It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property' that violates the Fourth Amendment."[83]

1. History and Text of the Fourth Amendment

The Fourth Amendment's text "reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant."[84] In 1761, nearly twenty years before drafting the Fourth Amendment's precursor, as a young lawyer, John Adams took courtroom notes while James Otis argued against general warrants and proposed an alternative model to measure the propriety of such intrusions.[85] Throughout his life, John Adams "repeatedly referenced the importance of Otis's arguments."[86]

> The hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws. They were denounced by James Otis as "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book," because they placed "the liberty of every man in the hands of every petty officer." The historic occasion of that denunciation, in 1761 at Boston, has been characterized as "perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country." "Then and there," said John Adams, "then and there was the first scene of the first act of opposition to the arbitrary claims

82. Bartnicki v. Vopper, 532 U.S. 514, 549 (2001) (Rehnquist, J., dissenting) (citations omitted).

83. Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307 (1998) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)) (internal quotations omitted).

84. Stanford v. Texas, 379 U.S. 476, 481 (1965) (quoting U.S. CONST. amend. IV).

85. Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 980–81 (2011).

86. *Id.*

> of Great Britain. *Then and there the child Independence was born.*"[87]

During the American Revolution, the widely held disdain for the abusive use of general warrants culminated in many state governments adopting laws protecting against unreasonable searches and seizures.[88] "Those protections, embodied in the constitutions of the various states after declaring their independence, typically addressed only abuses associated with general warrants."[89] However, the Massachusetts Constitution, drafted by John Adams in 1779, offered a different model.[90] Rather than merely abolish the practice of general warrants, John Adams's provision preceded with the specific declaration of the right to be secure.[91] Article 14 provided:

> Every subject has a right to be secure from all unreasonable searches and seizures of his person, his house, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the person or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.[92]

"Although Adams consulted other state constitutions, Article 14 had significant innovations: the words 'secure' and 'unreasonable' to define the quality and scope of the right protected were new to search and seizure provisions."[93] Moreover, rather than merely prohibiting general warrants, the first sentence justified the prohibition by articulating the underlying right to be secure against unreasonable searches and seizures.[94] Although James Madison is credited with drafting the Fourth Amendment, he adopted Adams's unique model as the format.[95]

There is consensus among historians that general warrants were the specific target of the Fourth Amendment.[96] Arguing the necessity of the Fourth

87. *Stanford*, 379 U.S. at 481–82 (emphasis added).

88. Clancy, *The Framers' Intent*, *supra* note 83, at 1027.

89. *Id.*

90. *Id.*

91. *Id.* at 1028.

92. *Id.*

93. *Id.*

94. Clancy, *The Framers' Intent*, *supra* note 83, at 1028.

95. *Id.* at 1029.

96. *Id.* at 1046.

Amendment before the House of Representatives, James Madison asserted that because the Federal government may reasonably consider general warrants "necessary and proper" to carry its powers into execution, general warrants must be constitutionally forbidden.[97] While his aim was to forbid general warrants, Madison chose Adams's abstract method for doing so, copying almost verbatim the essential elements of Adams's declaratory statement, declaring first, the broad right of the people to be "secure," and then particularly against "unreasonable" searches and seizures.[98] This format persisted through final form and harmonizes with the view that "the framers intended not only to prohibit the specific evils of which they were aware but also, based on the general terms they used, to give the Constitution enduring value beyond their own lifetimes."[99] In final form:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[100]

2. Development of Fourth Amendment Jurisprudence

"The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society. It is therefore implicit in 'the concept of ordered liberty' . . . ."[101] While the text and history of the Fourth Amendment show intention to protect the *broad* right to be "secure," its specific prohibition—against unreasonable searches and seizures—may seem like the only justiciable manifestation of a violation of the right to be secure. Indeed, a review of cases implicating the Fourth Amendment suggests that before there can be a violation there must be an actual search or seizure. And common explanations of the Amendment, like the one found at the U.S. Courts' website, suggest its purpose is to "protect[ ] people from unreasonable searches and seizures by the government."[102] Both lines of evidence indicate the generally accepted principle that the Fourth Amendment is implicated only after performance of a search or seizure.

---

97. *Id.*

98. *Id.*

99. *Id.* at 988.

100. U.S. CONST. amend. IV.

101. Wolf v. Colorado, 338 U.S. 25, 27 (1949), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961).

102. *What Does the Fourth Amendment Mean?*, U.S. COURTS, http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 (last visited Sept. 19, 2016).

If there has been a search or seizure, Fourth Amendment analysis then turns on whether the search or seizure was lawful. A violation requires that "the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place."[103] To establish that a legitimate expectation of privacy exists involves two inquiries: there must first be shown "a subjective expectation of privacy in the area searched, and second, that the expectation must be one that society is prepared to recognize as reasonable."[104]

Upon establishing a legitimate expectation of privacy, "[a]s the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is reasonableness."[105] Warrantless searches and seizures are per se unreasonable and "subject only to a few specifically established and well-delineated exceptions."[106] Even with proper procedure, the reasonableness of a search and seizure depends upon balancing, "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[107] To be reasonable, a search usually requires "some quantum of individualized suspicion."[108]

3. FBI Director Comey Tailored his Plan to Circumvent Fourth Amendment Jurisprudence

At first blush, the plan proposed by FBI Director Comey seems, for three reasons, a clever circumvention of the Fourth Amendment. First, under the plan, encrypted content would purportedly only be searched under lawful conditions.[109] Director Comey says, "[i]n the past, conducting electronic surveillance was more straightforward. We identified a target phone being used by a bad guy, with a single carrier. We obtained a court order for a wiretap, and, under the supervision of a judge, we collected the evidence we needed for prosecution."[110] Presumably, the suggested "front door" key is to be used only for conducting these types of lawful searches—reasonable, warranted

103. Rakas v. Illinois, 439 U.S. 128, 143 (1978).

104. United States v. Anderson, 154 F.3d 1225, 1229 (10th Cir.1998) (citations omitted) (internal quotation marks omitted).

105. Maryland v. King, 133 S. Ct. 1958, 1969 (2013) (internal quotation marks omitted).

106. Katz v. United States, 389 U.S. 347, 357 (1967).

107. Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

108. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 674 (1995) (citations omitted) (internal quotation marks omitted).

109. Comey, *supra* note 1.

110. *Id.*

searches. Although, if abused, a plaintiff would likely lack proof and even the ability to discover evidence to seek redress.[111]

Second, rather than suggesting a back door, Director Comey "want[s] to use the front door, with clarity and transparency."[112] The figurative distinction between front and back door seems to preempt any reasonable expectation of privacy, a requisite element of an unlawful search and seizure.[113] For example, a Fourth Amendment claim could not prevail when the Tenth Circuit held that a university professor had no reasonable expectation of privacy on his office computer because the university had a computer and internet usage policy that allowed the employer a right of access on a need to know basis.[114] Accordingly, no reasonable expectation of privacy would exist if the FBI and technology companies publicize that they are able—and contract for the ability—to access information stored and transmitted using electronic devices. With no reasonable expectation of privacy, the government may not even need a warrant to lawfully search the devices. However, there would seem an unacceptable irony if the only reason one had no reasonable expectation of privacy is because the government proscribed measures to attain privacy.

Third, under the plan, technology companies, not the government, might routinely and incidentally "seize" encrypted information transmitted through their systems. However, the government should only search the information when it is properly warranted. Accordingly, even if a reasonable expectation of privacy existed, the government would have had no part in either seizing or searching until after complying with proper procedure. Of course, if the government were also seizing and searching without proper judicial oversight, the public would have no way of knowing. Assuming no abuse occurs, Director Comey's plan appears, at first glance, to comply with the Fourth Amendment. In practice, electronics users would have no reasonable expectation of privacy that demands a warrant for search. Seizing of information would routinely be performed by technology companies that are not restrained by the Fourth Amendment, and government searches would be performed only after obtaining unnecessary warrants that serve primarily to portray propriety.

4. Careful Consideration Indicates Banning the Distribution of Encryption Technology is a Blatant Violation of the Fourth Amendment

A cursory review might suggest that Director Comey's plan complies with the Fourth Amendment's legal requirements, but a deeper review of the text and the Framers' intent reveals otherwise. The cases forming Fourth

111. *See generally* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

112. Comey, *supra* note 1.

113. *See* Rakas v. Illinois, 439 U.S. 128, 143 (1978).

114. United States v. Angevine, 281 F.3d 1130, 1133 (10th Cir. 2002).

Amendment jurisprudence deal almost entirely with searches and seizures actually performed. Nonetheless, it is a mistake to conclude that an actual search or seizure is required to violate the Fourth Amendment.

The plain language of the Fourth Amendment text protects the *right to be secure* against unreasonable searches and seizures; the right "shall not be violated."[115] Now, just as at the time of drafting, it may be difficult to contemplate a circumstance in which a violation occurs without an actual search and seizure. Notwithstanding, however, the history of its drafting shows the Framers chose the specific language to protect even against uncontemplated violations of the broader right to be "secure."[116]

"Adams and his contemporaries repeatedly used the concept of 'security' to describe the quality of the right protected as to each person's life, liberty, and property."[117] As a young lawyer sitting in on the arguments of James Otis, Adams recorded Otis's assertion that general warrants violate "fundamental Principles of Law . . . . A Man, who is quiet, is as secure in his House, as a Prince in his Castle . . . ."[118] Otis's own account asserted that the evil caused by a law permitting general warrants was that "every hous[e]holder . . . will necessarily become *less secure* than he was before [the law]."[119] "Recalling Otis's argument many years later, Adams said in a letter to William Tudor that Otis examined the acts of trade and demonstrated that 'they destroyed all our security of property, liberty, and life.'"[120] Similarly, in Madison's address to the House of Representatives, he "repeatedly used variations on the concept of 'security' as the underlying concern."[121] Hence, he asserted, "amendments were needed to 'expressly declare the great rights of mankind secured under this Constitution.'"[122] Madison argued that the Bill of Rights would "provide those securities for liberty which are required by a part of the community" and that the amendments would "incorporate those provisions for the security of rights."[123]

Otis chose not to argue a particular injury caused by any particular search or seizure. Instead, Otis argued broadly that every person was injured by the law, itself, which prescribed general warrants—it was the law that

115. U.S. CONST. amend. IV.

116. *See* Clancy, *The Framers' Intent*, *supra* note 83, at 988–89.

117. *Id.* at 1059.

118. *Id.* at 996.

119. *Id.* at 994 (emphasis added).

120. *Id.* at 1059.

121. *Id.* at 1061; James Madison, Speech at the First Congress, First Session: Amendments to the Constitution (June 8, 1789), *in* 5 WRITINGS OF JAMES MADISON at 230 (Gaillard Hunt ed., 1904), http://lf-oll.s3.amazonaws.com/titles/1937/Madison_1356-05_EBk_v6.0.pdf.

122. Clancy, *supra* note 83, at 1061.

123. *See id.*; Madison, *supra* note 121, at 374.

made people "less secure."[124] Even without a search, such a law indiscriminately violates the rights of all, specifically, the *right to be secure* against such arbitrary and unreasonable searches.[125] "[O]ur Revolution sprang" directly out of the violation of this right.[126] The record of these events indicates that the Framers intentionally drafted the Fourth Amendment to protect the broad right to be secure from unreasonable searches and seizures, rather than merely prohibit general search warrants. Accordingly, notwithstanding ordinary Fourth Amendment analysis, neither search nor seizure is required for a violation to occur. Rather, as Otis argued, Adams expounded, and Madison agreed, the denial of security is the true violation.

In light of the Framers' intent, Director Comey's proposal does not withstand Fourth Amendment analysis. Director Comey's plan is nothing more than a novel approach to make the people *insecure* against unreasonable searches. Absent cases involving actual searches, no challenges exist regarding a violation of the right to be secure from unreasonable searches. Similarly absent are cases challenging government violations of the Third Amendment by quartering soldiers in private homes. But that there has been no occasion to assert these rights does not make them any less substantive. To the contrary, that these rights have survived centuries unviolated indicates importance of the highest magnitude.[127] Regulatory measures aimed at exposing every person's communications and records to arbitrary search would ordinarily seem too absurd to attempt. But because the use of technology has advanced without the ability to secure privacy, banning encryption may seem an acceptable measure to maintain the status quo. Careful analysis, however, reveals that banning encryption violates the Fourth Amendment in a manner so audacious that similar attempts have not been made since before the states won their independence. Just as the government would never attempt to ban the sale of lock and key diaries, paper shredders, matches, or safes—all of which certainly interfere with reasonable searches—our government must refrain from proscribing the distribution of strong encryption technology. The Fourth Amendment forbids such.

C. Court Test Will Likely Hold The Fundamental Right of Privacy Includes The Right To Pursue The Security of Privacy

Both the Fifth and Fourteenth Amendments provide that government may deprive no person of "life, liberty, or property, without due process of

124. *See* Clancy, *The Framers' Intent*, *supra* note 83, at 994.

125. *See id.* (emphasis added).

126. Berger v. New York, 388 U.S. 41, 64 (1967) (Douglas, J., concurring).

127. For more than two centuries, the United States has not attempted to quarter soldiers in the homes of citizens, nor has its legislature attempted to outlaw whispering, or the keeping of secrets. The rights implicated by doing so are so basic and important that no official would dare violate them.

law."[128] The Fifth Amendment protects individuals from infringements by the federal government and the Fourteenth by the state.[129] Due Process review, however, is the same for both Amendments.[130]

Due Process demands "more than fair process, and the 'liberty' it protects includes more than the absence of physical restraint."[131] In addition to a procedural analysis, Due Process review includes a substantive analysis that protects personal liberty from government actions.[132] Certain liberties—fundamental rights—receive heightened protection against government interference under the Due Process Clause.[133]

In addition to those enumerated in the Bill of Rights, some unenumerated rights receive heightened constitutional protection. The liberty protected by Due Process includes a broad fundamental right of privacy.[134] Protected privacy interests tend to fall into two categories: the "individual interest in avoiding disclosure of personal matters" and the interest in autonomy in making certain kinds of important decisions.[135] The Court has not marked the outer limits of the fundamental right to privacy.[136] Precedent informs us, though, that the right specifically includes the rights to marry, have children, direct the upbringing of those children, marital privacy, use contraception, maintain bodily integrity, and receive an abortion.[137] The Supreme Court has alluded that the right might include a broad fundamental right to informational privacy, but the Court has not specifically held such.[138] Proscribing the distribution of encryption technology would violate interests that fall within the fundamental right to privacy.

The Court is careful when specifically defining fundamental rights to avoid injecting its personal policy preferences into the Constitution where the political process should govern.[139] Accordingly, the Court specifically deems

128. U.S. CONST. amend. V, XIV § 1.

129. *See* Malinski v. New York, 324 U.S. 401, 415 (1945) (Frankfurter, J., concurring).

130. *Id.* ("To suppose that 'due process of law' meant one thing in the Fifth Amendment and another in the Fourteenth is too frivolous to require elaborate rejection.").

131. Washington v. Glucksberg, 521 U.S. 702, 719 (1997).

132. *Id.* at 720.

133. *Id.*

134. Zablocki v. Redhail, 434 U.S. 374, 384 (1978) (citing Griswold v. Connecticut, 381 U.S. 479, 486 (1965)).

135. Whalen v. Roe, 429 U.S. 589, 599–600 (1977).

136. *Zablocki*, 434 U.S. at 385.

137. Washington v. Glucksberg, 521 U.S. 702, 720 (1997).

138. Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 147 (2011).

139. *Glucksberg*, 521 U.S. at 720.

rights as fundamental only by carefully describing the right, and only when the right is deeply rooted in the Nation's history and traditions and "implicit in the concept of ordered liberty," such that "neither liberty nor justice would exist if they were sacrificed."[140] Government may only infringe upon fundamental rights through actions narrowly tailored to serve a compelling governmental interest.[141]

1. The Privacy Right at Stake is Carefully Described as the Right to Pursue the Security of Informational Privacy

The Framers drew heavily on the work of the philosopher, John Locke,[142] who asserted that the purpose of government is to protect individual life, liberty, and property.[143] Accordingly, the Fifth and Fourteenth Amendments provide that deprivation of these demands Due Process.[144] Interestingly, however, when Thomas Jefferson penned the Declaration of Independence, he changed the third prong, "property," to "the *pursuit* of happiness."[145] In the 2006 American film, *The Pursuit of Happyness*, Christopher Gardner, in the story based on his life, questioned how Thomas Jefferson "kn[ew] to put the pursuit part in there."[146] He pondered, "maybe happiness is something that we can only pursue."[147] Whether a person can attain happiness is far outside the scope of this comment. The distinction, however, between an unalienable right to happiness and an unalienable right to *pursue* happiness is illustrative of the care taken to describe the right at stake through regulation of encryption—the right to pursue the security of informational privacy.

Locke also coined the phrase, "pursuit of happiness," when he wrote, "the necessity of pursuing happiness [is] the foundation of liberty."[148] It logi-

140. *Id.* at 720–21. Sometimes, it seems that the Court requires a lower standard before nominating a right as fundamental, but for the purpose of this comment, the most stringent test will be used.

141. *Glucksberg*, 521 U.S. at 721.

142. *See* Obergefell v. Hodges, 135 S. Ct. 2584, 2613 (2015) (Roberts, J., dissenting).

143. *See* JOHN LOCKE, TWO TREATISES OF GOVERNMENT § 87, at 59 (1698) (justifying political society on the basis of a power that man "hath by Nature . . . to preserve his Property, that is, his Life, Liberty and Estate"), http://socserv2.socsci.mcmaster.ca/econ/ugcm/3ll3/locke/government.pdf.

144. *See* U.S. CONST. amend. V, XIV § 1.

145. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).

146. *The Pursuit of Happyness, Quotes*, IMDB, http://www.imdb.com/title/tt0454921/quotes (last visited Sept. 19, 2016).

147. *Id.*

148. *Locke and Happiness*, PURSUIT OF HAPPINESS, INC., http://www.pursuit-of-happiness.org/history-of-happiness/john-locke/ (last visited Sept. 19, 2016).

cally follows that when Jefferson replaced "property" with "pursuit of happiness," he likely intended to artfully emphasize that the states were declaring their independence due to loftier notions of liberty rather than mere property rights. Regardless of Jefferson's reasons, the inclusion of the phrase provides insight into the meaning behind the Liberty protected by Due Process. Happiness is fleeting, and to suggest a guarantee of happiness seems an absurd contradiction to the human condition. While few legal protections exist for disruption of happiness (e.g., actionable torts for inflicting of emotional distress), the government surely need not narrowly tailor its actions, and only for compelling interests, before upsetting individual happiness. Nonetheless, Locke's liberty, at its most fundamental level, includes the right to *pursue* happiness.

While privacy is certainly more attainable than happiness, information intended to remain private is always susceptible to public exposure. Even a whisper can be incidentally overheard, and once overheard privacy is lost. "Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press."[149] Perhaps this explains the Court's reluctance to include the right to private information within the fundamental right of privacy.[150]

The Court may fear that recognition of a broad fundamental right to informational privacy might unacceptably protect even those communications intended to be private but somehow exposed through passive incidents of life. All three Supreme Court cases that considered whether the fundamental right to privacy includes the right to informational privacy involved information already exposed and known. In 1977, *Whalen v. Roe* considered whether a New York law requiring doctors to provide the names and addresses of patients prescribed certain drugs violated their right to privacy.[151] In the same year, *Nixon v. Administrator of General Services* considered whether a right to informational privacy protected President Nixon's documents and tape recordings.[152] Finally, in 2011, *National Aeronautics & Space Administration v. Nelson* assumed a significant constitutional right to informational privacy but decided that background checks performed by NASA would not violate that right even under the most deferential standard of review.[153]

149. Bartnicki v. Vopper, 532 U.S. 514, 534 (2001) (quoting Time, Inc. v. Hill, 385 U.S. 374, 388 (1967)).

150. *See* Whalen v. Roe, 429 U.S. 589, 600 (1977); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 465 (1977); Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 138 (2011).

151. *Whalen*, 429 U.S. at 591.

152. *Nixon*, 433 U.S. at 429.

153. *Nat'l Aeronautics & Space Admin.*, at 562 U.S. 147.

In all three cases the Court discussed the right to informational privacy through *Bartnicki v. Vopper*'s "risk of exposure" framework. None of the opinions, however, discuss the right in terms of the liberty to mitigate the risk of exposure. To draw a subtle distinction, these cases consider rights intended to protect information already exposed but not the right to prevent exposure. The latter is the specific privacy right at stake under Director Comey's proposal. It is the right to *pursue* the security of informational privacy—i.e. the right to whisper.

2. The Liberty to Pursue the Security of Informational Privacy is Deeply Rooted in the History And Traditions of the United States

Millar v. Taylor is the famous 1769 English case that established a perpetual common law copyright by proclaiming, "[i]t is certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends."[154] "The aim of [copyright law] is to secure to the author, composer, or artist the entire profits arising from publication; but the common-law protection enables him to control absolutely the act of publication, and in the exercise of his own discretion, to decide whether there shall be any publication at all . . . ."[155] Copyright law is designed to protect property rights, but its application embraces the individual right to secure informational privacy.[156]

The common law tort of nuisance protects the right to secure privacy under the right of quiet enjoyment of property. Nuisance law condemned the ancient practice of eavesdropping.[157] Eavesdropping was indictable under common law in both England and the United States.[158] While copyright and nuisance laws protect property, the premise for both is that individual liberty includes the right to secure informational privacy. Indeed, the common law provides redress for violation of the right.

The law of agency *requires* individuals to pursue the security of informational privacy.[159] Agents often have a fiduciary duty to maintain the confidentiality of their principals. Agency law requires attorneys to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or

154. Millar v. Taylor, 4 Burr. 2303, 2379 (1769) (Yates, J.).

155. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 200 (1890).

156. *See id.*

157. Berger v. New York, 388 U.S. 41, 45 (1967) (citing 4 BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 168 (1769)). Eavesdropping was so named after the practice of listening "under the eaves of houses or their windows, or beyond their walls seeking out private discourse." *Id.*

158. 1 BISHOP, COMMENTARIES ON THE CRIMINAL LAW 670 (1882).

159. *See* RESTATEMENT (FIRST) OF AGENCY § 395 (1933).

unauthorized access to, information relating to the representation of a client."[160] The Federal Health Insurance Portability and Accountability Act (HIPAA) sanctions failures in maintaining the privacy of medical records and communications—HIPAA requires encryption.[161] The privacy requirements within historical agency law and its modern developments demonstrate that the right to pursue the security of informational privacy is deeply rooted in the history and tradition of U.S. jurisprudence.

In addition to the ample evidence in legal history, the right to pursue the security of informational privacy is so self-evident that to suggest otherwise seems absurd. Perhaps this is why opponents of encryption seek such a roundabout method of restricting its usage. Perhaps they fear that the public would never tolerate direct proscription of encryption—much like the public might not tolerate a direct proscription of mathematics or behind-closed-doors meetings.

3. The Right to Pursue the Security of Informational Privacy is so Implicit in the Concept of Ordered Liberty that Neither Justice nor Liberty Would Exist if the Right were Sacrificed

In *Griswold v. Connecticut*, Justice Douglas wrote for the majority and held that unenumerated fundamental rights are an articulation of rights found within the "penumbra" and "emanations" of the Bill of Rights.[162] The lasting test, however, came from Justice Harlan's concurrence. Justice Harlan reasoned that the Due Process clause "stands . . . on its own bottom."[163] When determining whether a right is fundamental, one inquiry is whether the right is "implicit in the concept of ordered liberty."[164] In accordance with this view, the Court has held that "[t]he security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society. It is therefore implicit in 'the concept of ordered liberty' . . . ."[165]

While Justice Harlan disagreed with the amorphous penumbra-and-emanations test, he agreed that the "relevant inquiry may be aided by resort to

160. MODEL RULES PROF'L CONDUCT R. 1.6(c) (1983).

161. *See* Sarah S. Mir, *HIPAA Privacy Rule: Maintaining the Confidentiality of Medical Records, Part I A Detailed Look at the Evolution of HIPAA Privacy and How It Impacts Those It Touches*, 13 J. HEALTH CARE COMPLIANCE 5, 6 (2011).

162. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

163. *Id.* at 500 (Harlan, J., concurring).

164. *Id.*

165. Wolf v. Colorado, 338 U.S. 25, 27 (1949), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961).

one or more of the provisions of the Bill of Rights."[166] Accordingly, both Justices found a fundamental right to privacy implicit within the First, Fourth, and Fifth Amendments.[167] For similar reasons, the concept of ordered liberty must also include the right to pursue the security of informational privacy.

a. The First Amendment Suggests the Fundamental Right to Privacy Includes the Right to Pursue the Security of Informational Privacy

"At the heart of the First Amendment lies the principle that each person should decide for himself or herself the ideas and beliefs deserving of expression, consideration, and adherence."[168]

> The First Amendment reflects a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open. . . . That is because speech concerning public affairs is more than self-expression; it is the essence of self-government. . . . Accordingly, speech on public issues occupies the highest rung of the hierarchy of First Amendment values, and is entitled to special protection.[169]

Personal privacy also includes "the interest in fostering private speech."[170] "Privacy of communication is an important interest . . . . Moreover, the fear of public disclosure of private conversations might well have a chilling effect on private speech."[171]

> In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, even without the reality of such activity, can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.[172]

The plan advocated by FBI Director Comey would place a heavy burden on citizens seeking private communication. Knowledge that electronic communications are subject to unintended exposure would have a chilling effect on all private communications, even those communications that make up the

166. *Griswold*, 381 U.S. at 500 (Harlan, J., concurring).

167. *See id.*

168. Bartnicki v. Vopper, 532 U.S. 514, 553 (2001) (Breyer, J., concurring).

169. Snyder v. Phelps, 562 U.S. 443, 452 (2011) (internal quotation marks omitted).

170. *Bartnicki*, 532 U.S. at 536 (Breyer, J., concurring) (internal quotation marks omitted).

171. *Id.* at 532–33.

172. *Id.* at 533 (citation omitted).

very essence of self-government. Whether by whispering or encrypting, the rationale behind the First Amendment's protection of speech suggests the right to pursue informational privacy is so implicit in the concept of ordered liberty that neither justice nor liberty could exist if it was sacrificed.

b. The Fourth Amendment Suggests the Fundamental Right to Privacy Includes the Right to Pursue the Security of Informational Privacy

The Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion."[173] It provides that people are to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[174] In defining Fourth Amendment privacy rights, early American jurisprudence extended protection only to physical intrusion of physical things and locations, such as homes and actual papers.[175] Before the advent of telephonic and electronic eavesdropping, this body of law served as a workable protection of Fourth Amendment rights. However, the physical limitations proved insufficient as technological advancements enabled searches and seizures without physical intrusion.

In 1967, *Katz v. United States* considered whether law enforcement's warrantless use of an electronic listening device attached to the outside (as opposed to inside) of a telephone booth constituted a search and seizure in violation of the Fourth Amendment.[176] Precedent suggested that a search warrant was unnecessary because the listening device did not physically penetrate the telephone booth.[177] Citing to its own opinion authored only six years prior, the Supreme Court broadened Fourth Amendment protection and held that the Fourth Amendment "governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any technical trespass . . . ."[178] The Court departed from precedent by extending Fourth Amendment protection to non-physical things, such as conversations and forgoing a requirement that the invasion be physical in nature.[179] Accordingly, the unwarranted recording violated the Fourth Amendment.[180]

---

173. Katz v. United States, 389 U.S. 347, 350 (1967).

174. U.S. CONST. amend. IV.

175. *See Katz*, 389 U.S. at 362 (Harlan, J., concurring).

176. *Id.* at 349.

177. *Id.* at 352 (citations omitted).

178. *Id.* at 353 (internal quotation marks omitted).

179. *Id.* at 359.

180. *Id.*

In arriving at this holding, the Court articulated the proper perspective of the Fourth Amendment: "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[181]

> For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he *seeks to preserve as private*, even in an area accessible to the public, may be constitutionally protected.[182]

Thus, whether the Fourth Amendment protects a person's privacy may turn on whether the person subject to search or seizure affirmatively sought to preserve privacy. The rule implies that deeply rooted within our concept of ordered liberty exists the individual *right to pursue the security of informational privacy*. Absent this right, the Fourth Amendment would serve frivolously to secure only those who happened upon privacy. Banning or weakening encryption will place a broad and heavy burden on the exercise of this right.

c. The Fifth Amendment Suggests the Fundamental Right to Privacy Includes the Liberty to Pursue the Security of Informational Privacy

Under the Fifth Amendment, no person "shall be compelled in any criminal case to be a witness against himself."[183] The privilege against self-incrimination "is so fundamental to our system" that "if a person in custody is to be subjected to interrogation, he must first be informed in clear and unequivocal terms that he has the *right to remain silent*."[184] Moreover, the privilege demands informing the accused of "the right to the presence of an attorney, and that if he cannot afford an attorney one will be appointed for him prior to any questioning if he so desires."[185] The detained must be permitted to confer with counsel, *in private*.[186]

The privilege against self-incrimination "has come rightfully to be recognized in part as an individual's substantive right, a right to a private enclave where he may lead a private life. That right is the hallmark of our democracy."[187] Our concept of ordered liberty requires the guarantee of the privilege to not self-incriminate. Implicit within the privilege is the right to pursue the security of informational privacy. For the accused, this right

181. *Katz*, 389 U.S. at 359.

182. *Id.* at 351–52 (emphasis added) (citations omitted).

183. U.S. CONST. amend. V.

184. Miranda v. Arizona, 384 U.S. 436, 467–68 (1966) (emphasis added).

185. *Id.* at 479.

186. *Id.* at 485.

187. *Id.* at 460 (internal quotation marks omitted).

manifests itself through the right to remain silent and the guarantee of private conference with counsel. Neither justice nor liberty could be done if the underlying right to seek to preserve privacy were sacrificed.

4. Banning the Distribution of Strong Encryption will not Withstand Strict Scrutiny

With little exception, under strict scrutiny, the government may only infringe upon fundamental rights to serve "compelling" governmental ends, and then only by means "narrowly tailored" to further those ends.[188] "[O]ne of the most quoted lines in legal literature" is attributed to legal scholar, Gerald Gunther, who observed that strict scrutiny is "'strict' in theory and fatal in fact."[189]

The two-pronged strict scrutiny analysis begins with a determination of the ends sought, which must be compelling.[190] "'[T]he Court uses compelling in the vernacular to describe [the] societal importance' of the government's reasons for enacting the challenged law."[191] "Because the government is impinging upon someone's core constitutional rights, only the most pressing circumstances can justify the government action."[192] Broadly speaking, a compelling government interest exists in matters of great importance are at stake, such as national security, public safety, and crime investigation. However, strict scrutiny may require a strong nexus between the specific end of performing proper searches and seizures and the general ends of national security and public safety. Nonetheless, this comment assumes the government interest is compelling.

The second prong considers whether the means are narrowly tailored to serve the compelling interest.[193] Narrow tailoring requires that the law capture within its reach the "least restrictive" means available to pursue those

188. Washington v. Glucksberg, 521 U.S. 702, 721 (1997). *But see* Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 874 (1992) (introducing an undue burden test that departs somewhat from traditional strict scrutiny).

189. Gerald Gunther, *Foreword: In Search of Evolving Doctrine on A Changing Court: A Model for A Newer Equal Protection*, 86 HARV. L. REV. 1, 8 (1972); Kathleen M. Sullivan, *Gerald Gunther: The Man and the Scholar*, 55 STAN. L. REV. 643, 645 (2002).

190. *See Glucksberg*, 521 U.S. at 721.

191. Adam Winkler, *Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts*, 59 VAND. L. REV. 793, 800 (2006) (quoting HANS A. LINDE, WHO MUST KNOW WHAT, WHEN, AND HOW: THE SYSTEMIC INCOHERENCE OF "INTEREST" SCRUTINY, IN PUBLIC VALUES IN CONSTITUTIONAL LAW 221 (Stephen E. Gottlieb ed., 1993)).

192. *Id.*; *see* Korematsu v. U.S., 323 U.S. 214, 216 (1944) (opining that constitutional rights are not absolutes and that "[p]ressing public necessity" may warrant interference).

193. Winkler, *supra* note 191, at 800.

ends.[194] This is where government actions often fail strict scrutiny review. Banning the distribution of encryption technology is not "narrowly tailored" because it is too broad.

The Comey plan heavily burdens access to privacy-enabling technology. Doing so will, no doubt, aid law enforcement investigations, but by broadly denying a most basic right.

> If a statute were to authorize placing a policeman in every home or office where it was shown that there was probable cause to believe that evidence of crime would be obtained, there is little doubt that it would be struck down as a bald invasion of privacy . . . . I can see no difference between such a statute and one authorizing electronic surveillance, which, in effect, places an invisible policeman in the home. If anything, *the latter is more offensive because the homeowner is completely unaware of the invasion of privacy.*[195]

The statute considered in *Berger* authorized surveillance where less than probable cause existed to believe that any particular offense had occurred.[196] The statute did not withstand strict scrutiny because "the language of New York's statute is too broad in its sweep resulting in a trespassory intrusion into a constitutionally protected area."[197] Rather than directly intruding into private areas, banning the distribution of encryption technology will prohibitively burden ordinary citizens in their pursuit to secure privacy. Rather than targeting a *few* with probable cause, the plan openly invades the privacy rights of *all*, by creating a "front door" for the government to surveil all electronic information. The untailored proposal infringes upon everyone; its breadth would eviscerate privacy rights.

IV. PRUDENTIAL CONSIDERATION

Our nation's history and traditions suggest that mistrust of government is more than ample justification to seek informational privacy. Beyond trust, however, the government should promote, rather than discourage, the use of strong encryption—weakening encryption will cause more crime and national security threats than it rectifies.

194. *Id.* at 800–01; *see* Thomas v. Review Bd. of Ind. Emp't Sec. Div., 450 U.S. 707, 718 (1981) ("The state may justify an inroad on religious liberty by showing that it is the least restrictive means of achieving some compelling state interest.").

195. Berger v. New York, 388 U.S. 41, 65 (1967) (emphasis added).

196. *Id.* at 59.

197. *Id.* at 44.

A. Weakening Encryption Will Lead to More Crime

Informational insecurity wreaks havoc on modern society. Just two months before Director Comey's speech, Apple suffered a security breach where hackers accessed and released private images of several female celebrities.[198] "Private images of Jennifer Lawrence, Kate Upton, Rihanna and others were widely distributed on the internet . . . in the largest celebrity hacking scandal in history."[199] Victims who had their private photos published on the internet threatened to sue Google for damages of over $100 million for "profiting from the victimization of women."[200] Within hours, Google scrambled to remove links to "tens of thousands of pictures" published through no fault of their own.[201]

In April 2015, as a result of a Federal Communications Commission (FCC) investigation of consumer data breaches, AT&T agreed to pay a $25 million civil penalty.[202] The "AT&T data breaches exposed about 280,000 U.S. customers' names and . . . Social Security numbers."[203] The data was targeted in order to unlock stolen mobile devices for sale on secondary markets.[204] In response to the breach, Tom Wheeler, Chairman of the FCC said, "[a]s the nation's expert agency on communications networks, the [FCC] cannot—and will not—stand idly by when a carrier's lax data security practices expose the personal information of hundreds of thousands of the most vulnerable Americans to identity theft and fraud."[205]

The year 2014 proved to be one of the worst for security breaches. A string of attacks began in December 2013, when several news outlets reported that hackers stole "40 million credit and debit cards and 70 million

198. Edwin Chan & Christina Farr, *Apple Says Its Systems Not to Blame for Celebrity Photo Breach*, REUTERS (Sept. 3, 2014, 2:59 PM), http://www.reuters.com/article/us-entertainment-photos-apple-idUSKBN0GX29D20140903.

199. Alex Hern & Dominic Rushe, *Google Threatened With $100m Lawsuit Over Nude Celebrity Photos*, THE GUARDIAN (Oct. 2, 2014, 8:21 AM), http://www.theguardian.com/technology/2014/oct/02/google-lawsuit-nude-celebrity-photos.

200. Emily Smith, *Hacked Celebs' Lawyers Threaten to Sue Google*, PAGE SIX (Oct. 1, 2014, 11:04 PM), http://pagesix.com/2014/10/01/lawyers-for-hacked-celebs-sue-google-for-failing-to-removing-nude-pics.

201. Samuel Gibbs, *Google Removes Results Linking to Stolen Photos of Jennifer Lawrence Nude*, THE GUARDIAN (Oct. 20, 2014, 9:01 AM), http://www.theguardian.com/technology/2014/oct/20/google-search-results-linking-stolen-nude-photos-jennifer-lawrence.

202. Everett Rosenfeld, *AT&T Data Breaches Revealed: 280K US Customers Exposed*, CNBC (Apr. 8, 2015, 1:19 PM), http://www.cnbc.com/2015/04/08/att-data-breaches-revealed-280k-us-customers-exposed.html.

203. *Id.*

204. *Id.*

205. *Id.*

personal records" from Target stores.[206] Target ultimately agreed to pay $39 million to settle claims from the breach.[207] Subsequently, hackers breached Home Depot and accessed 56 million credit cards and 53 million email addresses.[208] Similar breaches occurred at Kmart, Dairy Queen, and Albertsons.[209] Additionally, JPMorgan Chase & Co. announced hackers accessed information covering 76 million households and seven million small businesses.[210]

These attacks impose huge costs on society. In June 2014, the Center for Strategic and International Studies (CSIS), a Washington think tank, estimated that data breaches cost the world economy more than $445 billion annually—or almost one percent of global income.[211] President Obama cited an even higher figure of $1 trillion annual economic cost resulting from data breaches.[212] These costs have elevated the problem of data security to high priority for the world economy.

Despite growing security concerns, progress continues. Mobile device users increasingly manage business and finances with their computers and smartphones.[213] Major banks and investment brokers enable customers to manage accounts through web-access and apps installed on mobile devices.[214] Both Apple and Google have implemented mobile payment func-

206. *E.g.*, Tali Arbel, *Top Business Stories of 2014: US Grows, World Slows*, YAHOO! FINANCE (Dec. 22, 2014, 5:39 PM), http://finance.yahoo.com/news/top-business-stories-2014-us-grows-world-slows-185010987—finance.html.

207. Ahiza Garcia, *Target Settles for $37 Million Over Data Breach*, CNN MONEY (Dec. 2, 2015, 5:48 PM), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/.

208. Arbel, *supra* note 206.

209. *Id.*

210. *Id.*

211. Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and Espionage Costs $445 Billion Annually*, THE WASH. POST, June 9, 2014, https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

212. *Id.*

213. *See Consumers and Mobile Financial Services 2015*, BD. OF GOVERNORS OF THE FED. RES. SYST. (Mar. 2015), http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf.

214. *See* MOBILE SOLUTIONS, CAPITAL ONE, https://www.capitalone.com/online-banking/mobile/ (last visited Mar. 14, 2016); *Seize Opportunity Anywhere with Mobile Trading*, TD AMERITRADE, https://www.tdameritrade.com/tools-and-platforms/mobile-trading.page (last visited Sept. 19, 2016).

tions on their smartphones, making it possible to pay at storefront points of sale with just a mobile device.[215]

As technological progress continues, vulnerabilities grow. Given these vulnerabilities, technology companies have responsibly made device security a top priority by putting strong encryption as a default setting on mobile devices.[216] Technology companies cannot jeopardize security with a back or front door (i.e. weaknesses) for criminals to attack. To do so would exacerbate an already enormous problem.

B. Weakening Encryption Will Lead to Greater National Security Threats

Data breaches are not always profit-driven; there is a brand of hackers, "hacktivists," motivated by political ends. On November 24, 2014, Sony Pictures Entertainment (Sony) fell victim to hacktivists.[217] Sony was preparing to release the film, *The Interview*, a comedy depicting a plotted assassination of North Korean dictator Kim Jong-un.[218] Threatening negative repercussions should Sony release the film, these hacktivists—presumably North Korean hackers—leaked numerous confidential Sony documents: employee addresses, social security numbers, performance reviews, and embarrassing emails.[219] The news media knowingly continued to propagate the illegally obtained data, causing irreparable harm to Sony's reputation and business relationships.[220] Problematically, Sony may be without remedy against those outlets due to First Amendment defenses.[221] Accordingly, tightening security to prevent future occurrences seems to be Sony's only available "remedy."

National security experts are concerned with greater threats involving politically motivated data breaches. "A study conducted in April [2015] by Symantec Corp., the world's biggest cybersecurity firm, found that computer-system invaders attacked 43 percent of global mining, oil and gas com-

215. *See Apple Announces Apple Pay*, APPLE (Sept. 9, 2014), https://www.apple.com/pr/library/2014/09/09Apple-Announces-Apple-Pay.html; *MasterCard Powers Android Pay, Bringing Mobile Payments to Android Device Owners*, MASTERCARD (May 28, 2015), http://newsroom.mastercard.com/press-releases/mastercard-powers-android-pay-bringing-mobile-payments-to-android-device-owners/.

216. *See* Comey, *supra* note 1.

217. Samuel C. Cole, Comment, *You Took the Words Right Out of My Database: Is There First Amendment Protection for Media Outlets Publishing Business Data Stolen by Hackers?*, 18 SMU SCI. & TECH. L. REV. 111 (2015).

218. *Id.*

219. *Id.* at 112.

220. *Id.*

221. *See id.* (presents a constitutional interpretation that allows protection, notwithstanding common understanding).

panies at least once" in the previous year.[222] Experts fear that attackers, by targeting these companies, are exploring the potential to create blackouts or oil spills.[223] Given the interconnectivity of major military and industrial operations, very little imagination is required to envision horrific national security incidents due to cyber security failures, even those from smart phone breaches. Unsurprisingly, President Obama believes "[c]yber threats pose one [of] the gravest national security dangers that the United States faces."[224]

> America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas.[225]

Perhaps this is why the White House chose not to pursue anti-encryption legislation.[226] Constitutional considerations aside, justifying measures to ban strong encryption could pose an irreconcilable contradiction with stated ends.

C. The People of the United States Have Never Trusted Their Democratically Elected Government with the Power Suggested

Speaking to the Brookings Institute, Director Comey acknowledged, "[t]his country was founded by people who were worried about government power—who knew that you cannot trust people in power."[227] Ironically, in the same speech, he suggests, "the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust."[228] Appealing to the crowd, he asked, "[a]re we so mistrustful of government—and of law enforcement—that we are willing to let bad guys walk away . . . willing to

222. Isaac Arnsdorf, *Hackers' Favorite Target: Big Oil and All That Deadly Equipment*, BLOOMBERG (June 15, 2015, 6:00 PM), http://www.bloomberg.com/news/articles/2015-06-10/hackers-favorite-target-big-oil.

223. *Id.*

224. Statement by the President on the Cybersecurity Framework, 2014 DAILY COMP. PRES. DOC. 88 (Feb. 12, 2014), https://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework.

225. *Id.*

226. James B. Comey, Dir., Fed. Bureau of Investigation, *Statement Before the Senate Committee on Homeland Security and Governmental Affairs* (Oct. 8, 2015), https://www.fbi.gov/news/testimony/threats-to-the-homeland.

227. Comey, *supra* note 1.

228. *Id.*

leave victims in search of justice?"[229] In the United States, the answer to those questions has always been a resounding "yes!" Since its founding, the people of the United States have vested their government with *limited* powers precisely because they distrust.

The law provides numerous examples where society is unwilling to pay with liberties the cost of convicting every criminal for every crime.[230] Law enforcement could convict more criminals without the Fifth Amendment privilege against self-incrimination. Likewise, unwarranted searches and seizures would aid in criminal convictions. Indeed, "[a]t every level of our legal system—from the Constitution,[231] to our statutes,[232] common law,[233] [and] rules[234] . . . —society has acted to preserve certain rights at the expense of burdening law enforcement's interest in investigating crimes and bringing criminals to justice."[235] It should be no surprise that the people may wish to continue in this legal tradition, a tradition that opposes legislation that would trounce on rights fundamental to their liberty.

Director Comey is no doubt well intentioned. In his struggle to punish crime, he wishes to leave no stone unturned. However, our Nation has never given the sort of trust he proposes. That Snowden revealed instances of abuse changes nothing. There is no "pendulum" of trust; the Constitution has always protected the right to encrypt.

V. CONCLUSION

Apart from recent history, searching a criminal suspect's communications has generally been an unrealistic possibility. Before technological advancements, individuals conducted almost all communications in private, unsearchable contexts. Apart from written text, communications were undis-

229. *Id.*

230. Apple Inc. Motion to Vacate Order Compelling Apple, Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistance, In 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 35KDG203, No. 16-CM-10 (C.D. Cal. Feb. 25, 2016), ECF No. 16, at 46 [hereinafter Apple Inc. Motion to Vacate Order].

231. *See, e.g.*, U.S. CONST. amend. IV (limitations on searches and seizures), amend. V (limitations on charging; prohibition on compelling testimony of accused).

232. *See, e.g.*, 18 U.S.C. § 3282 (prohibition on prosecuting crimes more than five years old); Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (2014) (limitations on ability to intercept communications).

233. *E.g.*, attorney-client privilege, spousal privilege, reporter's privilege, and priest-penitent privilege, all of which limit the government's ability to obtain evidence.

234. *See, e.g.*, FED. R. EVID. 404 (limitations on use of character evidence); FED. R. EVID. 802 (limitations on use of hearsay).

235. Apple Inc. Motion to Vacate Order, *supra* note 230, at 46.

coverable. As society increasingly relies on technology to communicate, the government's ability to search and surveil has substantially expanded.

Law enforcement has become accustomed to heightened search abilities in this era coined "the golden age of surveillance."[236] People are increasingly communicating via mediums that travel through public channels. For convenience, a great percentage of the population carries devices that track many details of their life: conversations, finances, friends, calendars, and even location. As a result, law enforcement officials have grown accustomed to new investigation capabilities not possible just several decades prior; they may even feel entitled to these abilities.

That people have sacrificed some privacy for convenience does not mean they have waived their constitutional rights. Just as technological advancements created the "golden age of surveillance," further advancements are now serving to restore privacy. Encryption reduces some capabilities recently enjoyed by law enforcement, and this development frustrates those tasked with investigating crime and securing the nation. Nonetheless, it is the right of the people to be secure from unreasonable searches and seizures and to pursue the security of their informational privacy.

Aside from the constitutional right to encrypt, efforts to prevent the use of encryption, while well-meaning, seem ill-considered. Financial crimes involving technological security breaches result in enormous economic loss; encryption is the best means to combat these crimes. Cyber threats pose one of the greatest dangers to our national security; encryption serves to defend against these threats. To hinder the use of encryption will likely cause more harm than it helps.

Given the revelations made by Edward Snowden along with the unattainable standing requirements to challenge Fourth Amendment violations, many individuals perceive unlawful searches to be widespread, yet entirely un-redressable. Encryption, accordingly, may serve as the only means of securing fundamental constitutional rights involving informational privacy. This comment urges discontinuation of attempts to stifle the use of strong encryption. "The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[237]

236. *See* Peter Swire, *The Golden Age of Surveillance*, SLATE (July 15, 1015, 4:12 PM), http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

237. Olmstead v. United States, 277 U.S. 438, 479 (1928) (J. Brandeis, dissenting).


SOUTHERN METHODIST UNIVERSITY
DALLAS, TEXAS

NON PROFIT ORGANIZATION

Southern Methodist University
P.O. Box 750116
Dallas, Texas 75275-0116

SMU Science and Technology Law Review

An Official Publication of
Southern Methodist University Dedman School of Law

TO: