Loyola of Los Angeles Law Review

Volume 50 | Number 4 Article 7

2017

Decrypting the Fourth Amendment: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Encryption Technologies

Candice Gliksberg
Loyola Law School, Los Angeles

Decrypting the Fourth Amendment: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Encryption Technologies

Cover Page Footnote

J.D. Candidate, May 2018, Loyola Law School, Los Angeles; B.A., Comparative Literature, University of California, Los Angeles. I wish to thank Professor Karl Manheim for his guidance, encouragement, and patience, and for explaining the complexities of quantum computing simply. Special thanks to Professor Cadra, Sigourney Haylock, Michaela Goldstein, and the other editors of the Loyola of Los Angeles Law Review for their helpful suggestions. Most importantly, I would like to thank my family, especially my mother, Dina, and my brother, Richard, for their constant love and support.

DECRYPTING THE FOURTH AMENDMENT: APPLYING FOURTH AMENDMENT PRINCIPLES TO EVOLVING PRIVACY EXPECTATIONS IN ENCRYPTION TECHNOLOGIES

*Candice Gliksberg**

I. INTRODUCTION

A legal battle is brewing between the U.S. government and technology companies over whether the government has the right to place limits on digital security measures like encryption.[1] The debate over encryption and government access to digital communications dates back decades, but for many Americans it came to the fore following the December 2015 terrorist attack in San Bernardino,[2] when the FBI attempted to compel the unlocking of an encrypted iPhone.[3] At the same time, the Senate was considering legislation that would require technology companies and communications service providers to weaken their encryption technologies and provide the government "backdoor" access into consumer devices.[4]

---

* J.D. Candidate, May 2018, Loyola Law School, Los Angeles; B.A., Comparative Literature, University of California, Los Angeles. I wish to thank Professor Karl Manheim for his guidance, encouragement, and patience, and for explaining the complexities of quantum computing simply. Special thanks to Professor Cadra, Sigourney Haylock, Michaela Goldstein, and the other editors of the Loyola of Los Angeles Law Review for their helpful suggestions. Most importantly, I would like to thank my family, especially my mother, Dina, and my brother, Richard, for their constant love and support.

1. Sarah Sorcher, *The Battle Between Washington and Silicon Valley Over Encryption*, CHRISTIAN SCI. MONITOR (July 7, 2015), http://www.csmonitor.com/World/Passcode/2015/0707/The-battle-between-Washington-and-Silicon-Valley-over-encryption.

2. Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?*, NPR (Dec. 3, 2016, 1:00 PM), http://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption.

3. Amy Davidson, *The Dangerous All Writs Act Precedent in the Apple Encryption Case*, THE NEW YORKER (Feb. 19, 2016), www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case.

4. *See* Compliance with Court Orders Act of 2016 (Discussion Draft 2016), https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf.

At the core of the debate is the balance between individual privacy and national security.[5]

The proliferation of the Internet,[6] wireless communication,[7] portable electronic storage ("e-storage"), electronic commerce ("e-commerce),[8] social media,[9] and cloud computing[10] has changed the way we live and work. We send personal communications, conduct financial transactions, and store our personal information (images, videos, audio recordings, and other private data) in cyberspace. e-storage has not only made it possible, but commonplace, to carry entire photo albums, video libraries, written communications, address books, and the like in one's pocket, whereas previously these records would only be found in the home.[11] With the shift in Internet usage from consumption to participation,[12] our interactions with cyberspace can reveal the most intimate details of our lives.[13] Simply using a navigation application on your phone can reveal where you are, where you have been, and where you are going.[14] Electronic safeguards such as encryption offer a way to protect this information from prying eyes by locking out anyone who is not authorized to view it.[15] The government's concern is that encryption affords the

5. *The Encryption Tightrope: Balancing Americans' Security and Privacy*: *Hearing Before the H. Comm. on the Judiciary*, 114th Cong., 6 (2016) (statement of James B. Comey, Director, Federal Bureau of Investigation), https://judiciary.house.gov/wp-content/uploads/2016/02/114-78_98899.pdf.

6. *Internet/Broadband Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017) http://www.pewinternet.org/fact-sheet/internet-broadband.

7. *Mobile Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017) http://www.pewinternet.org/fact-sheet/mobile.

8. *Number of Digital Shoppers in the United States Since 2009*, STATISTA, https://www.statista.com/statistics/183755/number-of-us-internet-shoppers-since-2009 (last visited Feb. 6, 2017).

9. *Social Media Fact Sheet*, PEW RES. CTR. (Jan. 12, 2017) http://www.pewinternet.org/fact-sheet/social-media.

10. *See, e.g.*, *Google Drive*, GOOGLE, https://www.google.com/drive (last visited Feb. 6, 2017).

11. Riley v. California, 134 S. Ct. 2473, 2491–93 (2014).

12. Daniel Nations, *What Does 'Web 2.0' Even Mean? How Web 2.0 Completely Changed Society*, LIFEWIRE (Dec. 1, 2016), https://www.lifewire.com/what-is-web-2-0-p2-3486624.

13. *See, e.g.*, David Nield, *How to See Everything Your Browser Knows About You*, GIZMODO (Dec. 1, 2016, 8:30 AM), http://fieldguide.gizmodo.com/how-to-see-everything-your-browser-knows-about-you-1789550766; Geoff Duncan, *7 Ways Your Apps Put You at Risk, and What You Can Do About It*, DIGEST TRENDS (Feb. 26, 2014, 9:22 AM), http://www.digitaltrends.com/mobile/seven-ways-apps-put-risk-cant-really.

14. *See* Duncan, *supra* note 13.

15. Sean J. Edgett, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339, 340 (2003).

same protection to criminal entities and terrorists.[16] The very same encryption that protects our information from prying eyes also prevents detection of malicious activity by watchful eyes.[17] However, ever since the whistleblower Edward Snowden revealed that the National Security Agency was collecting troves of Americans' communications records and hacking into the Internet backbone, there has been widespread mistrust of the government and its surveillance powers.[18] Thus, any legislation proposing to regulate encryption will likely receive pushback and criticism from companies and the American public.[19]

This Note addresses the possible limitations that the Fourth Amendment[20] places on the government's ability to regulate electronic security technologies, particularly limitations upon the use of digital encryption.[21] This Note takes the position that encryption creates a reasonable expectation of privacy in one's encrypted information, and thus, encrypted information should be afforded Fourth Amendment protection. Thus, if regulation effectively limits or eliminates the ability to encrypt a digital file, it will violate the Fourth Amendment's proscription of unreasonable searches and seizures. Part II of this Note gives a general overview of encryption. Part III explains the history and contours of the Fourth Amendment's warrant requirement. Part III also defines the reasonable expectation of privacy doctrine and provides a foundation for why the Fourth

16. *See generally Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy: Hearing before the S. Comm. on the Judiciary*, 114th Cong. (2015) (joint statement of James B. Comey, Director, Federal Bureau of Investigation, and Sally Quillian Yates, Deputy Attorney General), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Yates%20and%20Comey%20Joint%20Testimony1.pdf.

17. *Id.*

18. Sorcher, *supra* note 1.

19. Michael Heller, *Burr-Feinstein Bill Still Looks to Force Companies to Break Encryption*, TECHTARGET (Sept. 13, 2016), http://searchsecurity.techtarget.com/news/450304183/Burr-Feinstein-bill-still-looks-to-force-companies-to-break-encryption.

20. U.S. CONST. amend. IV.

21. Though beyond the scope of this paper, it is important to note that restrictions and regulations on encrypted communications also raise First and Fifth Amendment concerns. For example, laws regulating the dissemination and use of encryption have been criticized as an unconstitutional suppression of free speech for inhibiting the free flow of ideas of people who wish to communicate using encrypted communications. Norman Andrew Crain, *Bernstein, Karn, and Junger: Constitutional Challenges to Cryptographic Regulations*, 50 ALA. L. REV. 869, 870 (1999). Similarly, commentators have noted that compelling an individual to produce his or her encryption key may violate the Fifth Amendment Privilege against self-incrimination. Scott Brady, *Keeping Secrets: A Constitutional Examination of Encryption Regulation in the United States and India*, 22 IND. INT'L & COMP. L. REV. 317, 325–26 (2012).

Amendment's evolution will encompass encrypted data. Part IV evaluates the arguments for and against encryption triggering Fourth Amendment protection and examines whether case law indicates a resolution of the matter. Part V examines the effects of the notorious "third-party doctrine" on encrypted communications. Part VI proposes that the courts should recognize encryption as a virtual-concealment effort that creates a reasonable expectation of privacy in the contents of encrypted files. Lastly, Part VII concludes that any legislation attempting to regulate virtual security measures like encryption should be analyzed under the Fourth Amendment and likely will receive criticism on Fourth Amendment grounds.

II. ENCRYPTION GENERALLY

It is important to understand the encryption process in order to understand the amount of privacy and security that is afforded by this cyber technology. In general, the process of encryption scrambles or encodes the contents of a digital file, making it unreadable to any computer or person that does not possess the correct decryption key.[22] Once a file has been encrypted, it can be transmitted through the Internet, shared with other users over a network, or left on a personal computer, all with the owner of the document retaining control over who can access the file's contents.[23]

A. The Encryption Process

Non-electronic based encryption can be exceedingly simplistic and far less sophisticated than the advanced digital encryption used today.[24] However, its process is useful for understanding how encryption works. Encryption works by employing an algorithm to mix characters of a message with other characters or values in a seemingly nonsensical way.[25] An algorithm can be as simple as substituting numbers for letters or shifting the letters of the Alphabet in a given direction by a given number.[26] For example, with a shift of

22. *See, e.g.*, SIMON SINGH, THE CODE BOOK: THE EVOLUTION OF SECRECY FROM MARY, QUEEN OF SCOTS, TO QUANTUM CRYPTOGRAPHY 6, 11 (Anchor Books, 1999).

23. Edgett, *supra* note 15, at 342.

24. *Ciphers*, PRAC. CRYPTOGRAPHY, http://practicalcryptography.com/ciphers/caesar-cipher (last visited Feb. 6, 2017).

25. *See generally* Singh, *supra* note 22 (describing the fundamentals of encryption).

26. *Ciphers*, *supra* note 24.

1, "A" would become "B", "B" would become "C", and so on.[27] Thus, the word "SECRET" would be written "TFDSFU". To decrypt the message, the recipient would need to know the key, in this case, the number of characters to shift the alphabet. Since only the intended recipient of the message would ordinarily know the key, anyone else who intercepts the message would see only unintelligible gibberish ("ciphertext").[28] However, since in this example there are only a limited number of possible shifts or combinations (e.g., 26 letters in the English alphabet), each combination can be tested in turn in a short time, even by hand.[29] This would be an example of a "brute force" attack.[30]

Computer encryption works similarly, but because the algorithms are being executed by a computer, they can be much more complex. The strength of encryption is usually measured by key size, which in turn determines how long it would take a computer to decrypt the data by brute force attack (i.e., simply trying every possible combination in order to find the right key).[31] Because computers process information using bits, a brute force attack could take millennia.[32] Each bit is a unit of data that possesses a single binary value, either a 0 or 1 (i.e., two possibilities).[33] This means that a 128-bit key has 2^{128} possible combinations, or more than 300 decillion (300,000,000,000,000,000,000,000,000,000,000,000) possible combinations,[34] which would take multiple supercomputers several millennia to crack.[35] Thus, it is virtually unbreakable by brute force attack.

27. *Id.*

28. Ciphertext is the encrypted form of the original text and is meant to be unintelligible without the encryption key. The original, unencrypted text is known as plaintext. *See* Singh, *supra* note 22, at 11.

29. *Id.*

30. TONY HOWLETT, *Types of Encryption*, *in* OPEN SOURCE SECURITY TOOLS: A PRACTICAL GUIDE TO SECURITY APPLICATIONS (2004) (ebook), http://books.gigatux.nl/mirror/securitytools/ddu/ch09lev1sec1.html.

31. *Id.*

32. *Id.*

33. Nick Parlante & Julie Zelenski, *Computer Memory: Bits and Bytes*, STANFORD (Apr. 4, 2008), https://see.stanford.edu/materials/icsppcs107/06-Computer-Architecture.pdf.

34. Thom Patterson, *Spies Among Us: Get a Peek at Their Playbook*, CNN (July 20, 2016), http://www.cnn.com/2016/07/20/us/declassified-spycraft-espionage-gear-techniques.

35. Edgett, *supra* note 15, at 343.

B. The Importance of the Key

The encryption key is a unique code that keeps a digital file protected. This makes the key the most important part of the process.[36] The strength of the encryption is dependent upon the key and not the algorithm used to encode the file or message.[37] Knowing the algorithm without the key is worthless because the key is the only thing that can decrypt the message.[38] This is why decryption is analogized to a lock and key in the physical world.[39] It is also important to keep the description of the encryption process in mind when evaluating whether or not the entire process seems to create a reasonable expectation of privacy, which would trigger Fourth Amendment protection. Analyzing case law with this framework in mind will demonstrate that courts may be on the path to finding that encrypting documents creates Fourth Amendment protection.

III. THE FOURTH AMENDMENT SHIELD AGAINST UNREASONABLE SEARCHES AND SEIZURES

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[40]

The amendment was adopted as a response to the English Crown's use of general warrants, which allowed British officers to seize whomever and whatever they pleased while conducting unrestrained searches for evidence of criminal activity.[41] This abuse of power and unrestricted invasion of privacy was one of the driving forces behind the American Revolution itself.[42] It is unsurprising then, that the Supreme Court recognized the Fourth Amendment's significance as

36. *Id.* at 344.
37. *Id.*
38. *Id.*
39. *Id.*
40. U.S. CONST. amend. IV.
41. Riley v. California, 134 S. Ct. 2473, 2494 (2014); *see also* Ashcroft v. al-Kidd, 563 U.S. 731, 131 (2011).
42. *Riley*, 134 S. Ct. at 2494.

a safeguard against abuses by the government,[43] and that our courts take care to uphold it.[44] Because the Fourth Amendment is meant to restrict the government's power to investigate its citizenry, governmental limitations on one's ability to keep digital files and communications private should be analyzed under the Fourth Amendment.

A. The Requirement of a Reasonable Expectation of Privacy

The Fourth Amendment warrant requirement is triggered whenever a search would infringe upon an individual's reasonable expectation of privacy.[45] However, that expectation must be reasonable from both a subjective and objective point of view. The standard requires "first, that a person exhibit[] an actual or subjective expectation of privacy and second, that the expectation be one that society is prepared to recognize as reasonable."[46]

Because it is difficult to contest a defendant's claim to a subjective expectation of privacy,[47] the primary focus of the test is what makes an expectation of privacy objectively "reasonable."[48] An expectation of privacy is constitutionally "reasonable" when it is backed by an enforceable, extra-constitutional right to enjoin the government's invasion of privacy.[49] That is, the legitimacy of the expectation "must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."[50]

---

43. United States v. Rabinowitz, 339 U.S. 56, 69 (1950).

44. *E.g.*, United States v. Most, 876 F.2d 191, 200 (D.C. Cir. 1989) ("We do not believe that strict enforcement of the fourth amendment will . . . preclude effective law enforcement. Candor compels us to acknowledge, however, that some crimes escape detection . . . as a result of our vigilant commitment to constitutional norms. Enforcement of these norms is not, on such occasions, a pleasant duty; but it is a duty from which judges may not shrink.").

45. Rakas v. Illinois, 439 U.S. 128, 151 (1978).

46. 117 AM. JUR. Trials 193 §2 (2012). This two-part test was first articulated in a concurring opinion by Justice Harlan. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (stating that the reasonable expectation of privacy test "has come to mean the test enunciated by Justice Harlan's separate concurrence in *Katz*.").

47. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create A "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 507 (2001).

48. *Id.* at 507.

49. *Id.*; *see, e.g.*, *Rakas*, 439 U.S. at 143–44 n.12.

50. *Rakas*, 439 U.S. at 143–44 n.12.

B. The Effect of Concealment Efforts on the Reasonable Expectation of Privacy

When a person seeks to exclude others and takes reasonable steps to do so, have they created a reasonable expectation of privacy? It is clear that they exhibit at least a subjective expectation of privacy.[51] For example, in *Florida v. Riley*, a defendant growing marijuana on his private property attempted to ensure that no one knew of the illegal activity by building a fence and covering the marijuana so that it could not be seen from the street.[52] Law enforcement flew a helicopter over the defendant's property and viewed the defendant's property from the public airspace above.[53] The defendant argued that he had a reasonable expectation of privacy in the enclosed area and that the government should have procured a warrant before flying over.[54] The Court reasoned that although the defendant could have rationally expected that his fence and structures would create privacy, the government agents had the right to enter public airspace, from where they could see the marijuana in plain view.[55] Thus, although the defendant had a subjective expectation of privacy in his private property, it was not one that society was prepared to honor.[56]

Conversely, the Supreme Court has held that "the Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view."[57] For example, in *United States v. Chadwick*,[58] the Court determined there was a reasonable expectation of privacy in a locked footlocker even though the footlocker was in public view.[59] The Court reasoned that the privacy interest in the footlocker was not in the container itself, which was exposed to public view, but in its contents.[60] Chadwick had the right to exclude others from the contents of the footlocker and employed the footlocker to do so. Similarly, in *Bond v. United States*,[61] the

51. Florida v. Riley, 488 U.S. 445, 449–51 (1989).
52. *Id.* at 445.
53. *Id.* at 448.
54. *Id.* at 451–52.
55. *Id.* at 450–52.
56. *Id.* at 449.
57. United States v. Ross, 456 U.S. 798, 822–23 (1982).
58. 433 U.S. 1 (1977).
59. *Id.* at 11.
60. *Id.* at 13–14 n.8.
61. 529 U.S. 334 (2000).

Court reasoned that a bus passenger exhibited a reasonable expectation of privacy in his luggage, even though it was not locked, "by using an opaque bag and placing that bag directly above his seat."[62] The Court found the opacity of the bag sufficient to satisfy the reasonable-expectation-of-privacy test, even absent a lock, because the bag concealed the contents, thereby excluding prying eyes.[63] In each instance, the Court found the concealment efforts were ones that society was willing to recognize as affording a reasonable expectation of privacy.[64] It should also be noted that the Court explicitly refuses to recognize a constitutional distinction between worthy and unworthy containers, as long as they conceal their contents from plain view.[65]

C. Applying These Principles to Encryption

When applied in the context of encryption and the digital world, these guiding principles should lead to the conclusion that encryption does indeed trigger Fourth Amendment protection. The sole purpose of encryption is to prevent unauthorized access to digital files by rendering them unreadable to those without the decryption key. That is, the purpose is to exclude and conceal. Encryption serves both to facilitate and protect electronic communication and the storage of, often personal, information. The types of data stored and transmitted electronically are as varied as tangible objects carried in the physical world. Smart phone, computer, and Internet users enjoy access to digital calendars,[66] photographs,[67] address books,[68] correspondence in the form of e-mail messages,[69] and diaries in the form of personal

62. *Id.* at 338–39.

63. *Id.*

64. *Chadwick*, 433 U.S. at 11; *Bond*, 529 U.S. at 338–39.

65. *See* United States v. Ross, 456 U.S. 798, 822 (1982) (noting that for purposes of the Fourth Amendment, "the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion," and thus a traveler's toothbrush and clothing carried in a paper bag or scarf should not be treated any differently than a "sophisticated executive" with a locked briefcase) (citing Miller v. United States, 357 U.S. 301, 307 (1958)).

66. *E.g.*, *Google Calendar*, GOOGLE, https://support.google.com/calendar/answer/2465776?co=GENIE.Platform%3DDesktop&hl=en (last visited Jan. 2, 2017).

67. *E.g.*, *Google Photos*, GOOGLE, https://www.google.com/photos/about/ (last visited Jan. 2, 2016).

68. *E.g.*, *Mac Basics: Address Book*, APPLE (Mar. 23, 2016), https://support.apple.com/en-us/HT201728.

69. *See, e.g.*, *Gmail*, GOOGLE, https://www.google.com/intl/en-GB/mail/help/about.html (last visited Jan. 2, 2017).

blogs[70]—the same materials deemed "highly personal" by the Supreme Court.[71] The fact that the encrypted items are digital should not diminish the privacy interest in them; after all, the Supreme Court recognized in *Katz v. United States* that intangibles are covered by the Fourth Amendment,[72] and in *Riley v. California* the Court recognized a privacy interest in digitally stored information.[73] Encryption is simply the means to exclusion, the affirmative step taken to ensure privacy, like the bag in *Bond*[74] or the footlocker in *Chadwick*.[75]

IV. AN ANALYSIS OF EXISTING VIEWPOINTS REGARDING ENCRYPTION AND THE REASONABLE EXPECTATION OF PRIVACY TEST

There are two camps of thought regarding whether encryption itself can trigger a reasonable expectation of privacy.[76] One camp believes that encryption functions like a virtual container.[77] The other compares encryption to a foreign language, arguing that the encrypted contents are in plain view—they must simply be translated.[78] This section explores both views and responds to their various arguments. This section also examines indications from current case law that our judicial system may be on its way to recognizing that encryption creates a reasonable expectation of privacy.

---

70. *E.g.*, *About WordPress*, WORDPRESS, http://wordpress.org/about (last visited Jan. 2, 2017).

71. New Jersey v. T.L.O., 469 U.S. 325, 339 (1985).

72. Katz v. United States, 389 U.S. 347, 353 (1967).

73. Riley v. California, 134 S. Ct. 2473, 2489, 2494–95 (2014) (deeming cell phones "minicomputers" that hold "the privacies of life" and stating that "the fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."). Nor does it matter that digital communications are usually written, not oral, since the Court has determined that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable." United States v. Jacobsen, 466 U.S. 109, 114 (1984).

74. Bond v. United States, 529 U.S. 334, 338–39 (2000).

75. United States v. Chadwick, 433 U.S. 1, 11 (1977).

76. *See* Crain, *supra* note 21, at 870 (stating that "[e]ncryption technologies serve as the locks and keys of cyberspace."); Kerr, *supra* note 47, at 515–19.

77. David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2231 (2009).

78. Kerr, *supra* note 47, at 515–19.

A. Arguments That Encryption Creates a Reasonable Expectation of Privacy

Most commentators believe encryption is the virtual equivalent of a lock and key or an opaque container[79] because the encryption algorithm converts plaintext (the contents of the file) into a set of symbols and scrambled text that mean nothing without the encryption key, even if one knows the encryption algorithm.[80] The plaintext is literally unviewable (or invisible) because it is concealed behind a digital ciphertext wall or barrier.[81] This is virtual opacity. Because digital encryption works to ensure that the individual encrypting the file can control access with the encryption key, it works just like a locked container and a complete sense of privacy exists.[82]

B. Arguments That Encryption Does Not Create a Reasonable Expectation of Privacy

Still, some respected scholars dismiss this assessment by pointing out that an encrypted message (or file) can still be viewed, albeit in encoded form.[83] That is, the encrypted message itself remains in plain view. Thus, they contend that a law enforcement officer's observation of such an encrypted message is not a search and does not implicate the Fourth Amendment.[84] Furthermore, they maintain that the encrypted message, once observed, may be decrypted without implicating the Fourth Amendment, just as law

79. Crain, *supra* note 21, at 870 (stating that "[e]ncryption technologies serve as the locks and keys of cyberspace."); Edgett, *supra* note 15, at 350–51; Couillard, *supra* note 77, at 2232; Timothy B. Lennon, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984?*, 58 ALB. L. REV. 467, 487 (1994); 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f), at 721 (4th ed. 2004) (quoting Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995) ("protections such [as] individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is penetrable.").

80. Andrew B. Berman, *International Divergence: The "Keys" To Signing On the Digital Line-the Cross-Border Recognition of Electronic Contracts and Digital Signatures*, 28 SYRACUSE J. INT'L L. & COM. 125, 128 (2001) (providing a general overview of the encryption process and its effectiveness to protect documents); *See generally* Singh, *supra* note 22.

81. *See* Edgett, *supra* note 15, at 365 ("Encryption makes a document invisible to outsiders . . . . Instead of using physical walls, it creates a digital wall . . . .").

82. *Id.* at 350.

83. Kerr, *supra* note 47, at 515–19; Scott Brady, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1604 (1997).

84. Brady, *supra* note 83, at 1604.; Kerr, *supra* note 47, at 515–19.

enforcement agents may "decode" communications they overhear in foreign languages or idiosyncratic terms (code words) used by street gangs.[85] Finally, they argue that, historically, decrypting encrypted communications has been held not to violate a reasonable expectation of privacy and that conclusion does not change in the Internet or digital context.[86]

C. Encryption Creates a Reasonable Expectation of Privacy

The above arguments suggesting encryption does not create a reasonable expectation of privacy fail in several respects, and this Note will address each in turn. First, an encrypted message's contents are not in plain view; if they were, the very point of encryption would be defeated. An individual's privacy interest is in the plaintext, or original message, which is not in plain view. Without the encryption key, only the ciphertext (encrypted text) is in plain view. Much like the locked container in *Chadwick*, which was found to trigger Fourth Amendment protection, the privacy interest is not in the ciphertext but in the original *contents* or plaintext.[87] Thus, attempting to decrypt the ciphertext by brute force attack would be like the bus employee in *Bond* who violated Bond's Fourth Amendment privacy interest by attempting to determine the contents of Bond's opaque bag by feeling and squeezing it.[88]

The case of *Walter v. United States* nicely illustrates these principles.[89] In *Walter*, 12 packages were delivered to the wrong company and were opened by its employees.[90] Inside the packages were several boxes of 8-millimeter film.[91] On the side of each box "were suggestive drawings, and . . . explicit descriptions of the contents."[92] One employee attempted to hold some of the films up to the light, but was unable to observe the content of the films.[93] The

85. Brady, *supra* note 83, at 1604; Kerr, *supra* note 47, at 515–19.

86. Kerr, *supra* note 47, at 532.

87. In *Chadwick*, there was not a reduced expectation of privacy in the footlocker just because it was in public view. United States v. Chadwick, 433 U.S. 1, 11, 13–14 n.8 (1977) ("Respondents' principal privacy interest in the footlocker was, of course, not in the container itself, which was exposed to public view, but in its contents.").

88. Bond v. United States, 529 U.S. 334, 338–39 (2000).

89. Walter v. United States, 447 U.S. 649 (1980).

90. *Id.* at 651–52.

91. *Id.* at 652.

92. *Id.*

93. *Id.* at 651.

company contacted the FBI, who viewed the films with a projector without first obtaining a search warrant.[94]

Although a majority of the Court concluded that the federal agents' viewing of the film with a projector violated the Fourth Amendment, there was no majority opinion. Justice Stevens authored the opinion announcing the judgment of the court.[95] Justice Stevens asserted that because the employee was unable to actually view the content of the films, the petitioners retained their reasonable expectation of privacy in their contents.[96] That the descriptive labels on the boxes had been exposed merely "gave [the federal agents] probable cause to believe that the films were obscene . . . and offended the criminal code."[97] But because the contents of the films were still not known with certainty, the petitioners' reasonable expectation of privacy in their contents remained intact and the agents needed a warrant to view them with a projector.[98] The four dissenters in *Walter* believed that no real expectation of privacy remained in the contents of the films by the time the FBI received them because the descriptions on the boxes had "clearly revealed the *nature* of their contents" to the employees.[99] Thus, in the dissenting Justices' view, the subsequent viewing of the films by the FBI did not change the nature of the search and was not an additional search.[100]

It is clear that under either Justice Stevens or the dissent's view, people who encrypt their communications would maintain a reasonable expectation of privacy in those communications, thus triggering Fourth Amendment protections. Just as the contents of the films in *Walter* could not be viewed without a film projector, the contents (plaintext) of an encrypted message cannot be viewed without the encryption key. While the 8-millimeter film itself was

94. *Id.* at 654.

95. *Id.* at 657. Justice White, joined by Justice Brennan in a concurring opinion, believed the Fourth Amendment was violated because the agents had not obtained a warrant. *Id.* at 660–62 (White, J., concurring). Justice Marshall also concurred in the judgment but did not write an opinion. *Id.* at 660 (Marshall, J., concurring).

96. *Id.* at 659 ("The private search merely frustrated that expectation in part. It did not simply strip the remaining unfrustrated portion of that expectation of all Fourth Amendment protection.").

97. *Id.* at 654.

98. *Id.* at 654, 659.

99. *Id.* at 663 (Blackmun, J., dissenting) (emphasis added).

100. *Id.* at 663–64.

exposed to the employee's view, the content of the film was not. Similarly, even if the cyphertext is exposed to or in "plain view" of a third party, the original content (the plaintext) is not. Moreover, unlike the boxes that housed the films in *Walter*, encrypted cyphertext does not carry any descriptive information that would "clearly reveal" anything about the plaintext contents of the file or message or their "*nature*". The contents of the encrypted message remain unknown to the police or a third party until they are decrypted. Thus, people should retain a reasonable expectation of privacy in the contents of their encrypted communications.

Second, decrypting an encrypted message is nothing like "decoding" idiosyncratic terms used by street gangs or communications in a foreign language that are overheard by officers. Idiosyncratic terms or "code words" used by gangs are readily associated with observable actions and events. The true meaning of the term is already technically known or presumed, it just needs to be proved. For example, a gang known to deal in drugs uses the word "shirts" to refer to cocaine. If members of the gang discuss a shipment of "shirts" they expect at 5:00 pm and are observed receiving a shipment of cocaine, then the presumption that "shirts" stands for drugs is simply proven. In contrast, the contents of an encrypted message are unknown and the key is not usually guessable. Moreover, a code word is known to and used by multiple gang members, if not the entire gang, and foreign languages, though foreign, are generally spoken by millions of people. Encryption does not work like a foreign language. One unique key is shared between at most two users.[101] If decryption were as simple as translating a language, for which one can rely on general intelligence and education, encryption would lack the assurances of privacy that people rely upon in engaging in online transactions and communications. Furthermore, "law enforcement could conceivably 'figure out' the combination to a padlock more quickly and easily than it could decrypt modern encryption, but that does not eviscerate privacy interests in a physically locked container."[102]

101. Edgett, *supra* note 15, at 356–57 ("If individuals speaking a language unique to the two of them—an equivalent to encryption—then there should be a reasonable expectation of privacy.").

102. Couillard, *supra* note 77, at 2235.

The third contention, that decrypting encrypted communications has historically been held not to violate a reasonable expectation of privacy, is somewhat misleading. None of the cases cited by one proponent of this argument, Professor Kerr, expressly holds that decryption does not violate the Fourth Amendment.[103] In none of these cases did the litigants raise the Fourth Amendment issue,[104] and it is not the place or duty of the courts to advocate for the parties. In any event, all three points fail to address the second prong of the reasonable-expectation-of-privacy test: whether an expectation of privacy is objectively reasonable.[105]

In determining whether an expectation of privacy is objectively reasonable, the Court considers whether society is willing to accept the expectation as reasonable.[106] The use of technology and the Internet is now commonplace. It is integrated into every aspect of our lives: from school and work, to banking and shopping, to socializing and conducting business, to paying taxes and bills. Personal communications, electronic diaries, trade secrets, and other personal data rapidly fill hard drives, network servers, and the Internet. Millions of people and businesses now use cloud computing to store data on remote servers owned by service providers instead of on their own hard drives because it is more cost effective and has a larger capacity. The proliferation of the Internet, e-commerce, and cloud computing would not have occurred if there were not safeguards protecting this data and upon which people could rely. In the digital world, those safeguards are limited to unlisted links, passwords, and encryption. Though digital protection measures are limited in

103. *See, e.g.*, Allis v. United States, 155 U.S. 117, 120 (1894) (upholding use at trial of plaintext version of encrypted telegram sent by defendant because no objections were raised or preserved in the lower courts); Buckley v. United States, 33 F.2d 713, 716 (6th Cir. 1929) (discussing defendant's own voluntary testimony describing his practice of encrypting his telegraph messages to conceal their true meaning); Wong v. Esola, 6 F.2d 828, 829 (9th Cir. 1925) (noting that coconspirators communicated via encrypted telegraph communications and that those communications coincided with the dates of their alleged illegal activities, thus the use of a cipher telegram was suspicious); *see also* United States v. Burr, 25 F. Cas. 38 (C.C. Va. 1807) (Marshall, C.J.) (noting that a letter was still in encrypted form and seeking to determine "whether the letter could be deciphered," the court ruled that Burr's secretary could not refuse to testify regarding his present knowledge of the cipher on Fifth Amendment grounds "because his present knowledge would not . . . justify the inference that his knowledge was acquired" before the message was written).

104. *See*, *supra* note 103, and accompanying text.

105. Kerr, *supra* note 47, at 503–07.

106. *Id.*; Rakas v. Illinois, 439 U.S. 128, 151 (1978).

number, this does not mean they are not powerful. Many encryption products now available to consumers provide more security and protection to digital data than is available to most things in the physical world. Thus, society expects its data to maintain the same protection in cyberspace as it would if stored on a home computer or in a home safe. Indeed, society relies on this expectation of protection daily, with every online transaction or digital communication sent.

D. Indications from the Courts That Encryption Creates a Reasonable Expectation of Privacy

Finally, some of the Supreme Court's recent decisions indicate that our judicial system may be on its way to recognizing that encryption creates an expectation of privacy. In his concurring opinion in *United States v. Jones*,[107] Justice Alito, writing for four Justices, remarked that "technology can change" an individual's expectations of privacy and thus alter the calculus that courts must perform.[108] Additionally, in her own concurring opinion, Justice Sotomayor emphasized that technology can disrupt the calculus so much that "it may be necessary to reconsider" basic Fourth Amendment premises.[109] Similarly, in *Riley v. California* the Court noted that analogizing the digital world and processes to the physical world is difficult and unhelpful; an "analogue test would 'keep defendants and judges guessing for years to come.'"[110] In *Riley*, the Court held that the contents of cell phones cannot be searched without a warrant, even incident to arrest, because they differ qualitatively and quantitatively from physical containers in the amount and types of information they hold.[111] Similarly, encryption differs quantitatively and qualitatively from physical locks and barriers in the amount of protection it affords. In his *Riley* concurrence, Justice Alito noted that "the Court's broad holding favors information in digital form over information in hard-copy form," but that he "do[es] not see a workable alternative."[112] Even some lower federal courts seem ready to recognize that digital

107. 132 S. Ct. 945 (2012).
108. *Id.* at 962 (Alito, J., concurring).
109. *Id.* at 957 (Sotomayor, J., concurring).
110. Riley v. California, 134 S. Ct. 2473, 2493 (2014).
111. *Id.* at 2489–92, 2495.
112. *Id.* at 2497 (Alito, J., concurring).

protection measures can trigger additional Fourth Amendment protection, even when the government already has lawful access to the container at issue.

For example, in *Trulock v. Freeh*,[113] law enforcement relied on the third-party consent exception to the warrant requirement to gain lawful access to the defendant's computer.[114] Under the consent exception, voluntary consent to a police search given by a third party with authority over the subject property makes a warrantless search reasonable and therefore constitutional.[115] A third party has authority to consent to a search if that third party has either joint access or control for most purposes.[116] In *Trulock*, the defendant's live-in girlfriend, who had access to the defendant's computer but not his password-protected files, consented to a search of the defendant's property and computer.[117] Among the things searched were the defendant's password protected documents located in the computer's hard drive.[118] The court held that the search of the computer was valid.[119] However, the Fourth Circuit found that the search of the password-protected files was invalid because the files carried an additional expectation of privacy.[120]

Still, the lower courts are not in agreement. In *United States v. Andrus*,[121] law enforcement used forensic software to gain direct access to the defendant's hard drive, without first determining whether a username and password were needed.[122] The Tenth Circuit concluded that the search of the computer was lawful, despite the fact that the forensic software allowed the police to bypass the password protection on the defendant's computer, because the defendant's father, who had apparent authority over his son's computer,[123] had consented to the police search.[124] Although the court in *Andrus* acknowledged that the function of password

113. 275 F.3d 391 (4th Cir. 2001).
114. *Id.* at 398.
115. United States v. Andrus, 483 F.3d 711, 716 (10th Cir. 2007).
116. *Id.*; *see also* United States v. Matlock, 415 U.S. 164, 171 (1974).
117. *Trulock*, 275 F.3d at 398–402.
118. *Id.*
119. *Id.* at 403.
120. *Id.*
121. 483 F.3d 711 (10th Cir. 2007).
122. *Id.* at 713–14.
123. *Id.* at 716 ("[A] third party has apparent authority to consent to a search when an officer reasonably . . . believes the third party possesses [actual] authority to consent.").
124. *Id.* at 719–22.

protection in the computer context is analogous to a lock on a physical container, it also distinguished password protection from physical locks because passwords are not readily apparent.[125] Despite the analogous function, the court refused to presuppose that password protection is so common that a reasonable police officer should know that a computer is likely to be so protected.[126]

Contrasting these two holdings illustrates the Supreme Court's point in *Riley*: analogizing the digital world and digital processes to the physical world is difficult and unhelpful.[127]

V. THE EFFECT OF THE THIRD-PARTY DOCTRINE ON ENCRYPTED COMMUNICATIONS

Trulock and *Andrus* both address situations in which third parties had access to or control of the object of the search. In such situations, an expectation of privacy may no longer be reasonable.

A. The Third-Party Doctrine

Under the "third-party" doctrine, which developed from a line of "third-party cases" decided by the Supreme Court, information that is voluntarily revealed to third parties does not warrant Fourth Amendment protection.[128] It should be noted, however, that the mere ability of a third-party intermediary to access the contents of a communication is not sufficient to extinguish a reasonable expectation of privacy.[129] "Nor is the right of access."[130] In *Katz*, for example, telephone companies had both the ability and right to monitor calls, yet the Supreme Court found that the defendant had a reasonable expectation of privacy during a telephone call he made from a public phone booth.[131] Likewise, letters and other sealed

125. *Id.* at 718–19.

126. *Id.* at 721.

127. Riley v. California, 134 S. Ct. 2473, 2493 (2014).

128. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004) ("The Supreme Court has repeatedly held, however, that the Fourth Amendment does not protect information revealed to third parties."); *see also* United States v. Miller, 425 U.S. 435, 443 (1976); United States v. White, 401 U.S. 745, 749, 754 (1971).

129. United States v. Warshak, 631 F.3d 266, 286–87 (6th Cir. 2010).

130. *Id.* at 287.

131. Katz v. United States, 389 U.S. 347, 359 (1967); *see also* Smith v. Maryland, 442 U.S. 735, 746–47 (1979) (Stewart, J., dissenting) (noting that telephone conversations such as the one at issue in Katz "must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment").

packages carry with them the sender's expectation of privacy,[132] despite the fact that they are handed over to numerous mail carriers and are exposed to the risk that any mail handler "could tear open the thin paper envelopes that separate the private words from the world outside."[133]

Conversely, individuals assume the risk that the third party to whom they convey information may subsequently reveal that information to the government when that information is "voluntarily" turned over or "knowingly exposed" to a third party.[134] This "voluntary act of disclosure invokes the third-party doctrine, which gives the government additional leeway in obtaining . . . private[] information."[135] When third-party intermediaries are involved, the third-party doctrine holds that certain transactional aspects of the communication may be lawfully obtained from the intermediary.[136] The Supreme Court has held that transactional data are part of the intermediary's business records. [137] Rather than merely holding the documents as a neutral third party, the intermediary is in fact an interested party to the transaction.[138] Thus, the Court reasons that an individual turns the data over to an intermediary with the knowledge that they will not remain completely private.[139] Current law holds that accounting firms are parties to tax records, banks are considered parties to the bank records of their customers, mail couriers are parties to the addresses on the outside of envelopes, and a telephone-service provider is considered a party to the numbers dialed.[140]

---

132. United States v. Jacobsen, 466 U.S. 109, 114 (1984).

133. *Warshak*, 631 F.3d at 285.

134. *See, e.g.*, *Katz*, 389 U.S. at 351 (finding that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection"); Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir. 1978) ("To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections . . . ").

135. Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand Over Passwords*, 30 BERKELEY TECH. L.J. 1, 15 (2015).

136. Couillard, *supra* note 77, at 2227.

137. *See* United States v. Miller, 425 U.S. 435, 440–41 (1976) (citing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 48–49, 52 (1974)).

138. *Id.*

139. *See, e.g.*, Couch v. United States, 409 U.S. 322, 335–36 (1973).

140. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979) (dialed telephone numbers); *Miller*, 425 U.S. 435 (1976) (bank records); *Couch*, 409 U.S. 322 (1973) (business and tax records); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905–06 (9th Cir. 2008) ("[I]ndividuals do not enjoy a reasonable expectation of privacy in what they write on the outside of an envelope.").

For example, in *Smith v. Maryland*, the Supreme Court held that law enforcement's use of a pen register[141] to record the numbers dialed from the defendant's home telephone did not constitute a search.[142] The Court concluded that the defendant did not have the requisite expectation of privacy to support a Fourth Amendment claim.[143] The Court reasoned that callers can have no expectation of privacy in numbers they dial because people "realize that they must 'convey' phone numbers to the telephone company since it is through the telephone company switching equipment that their calls are completed."[144] The Court emphasized that telephone users place calls with the understanding that telephone companies keep records of numbers dialed "for a variety of legitimate business purposes."[145] According to the Court, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,"[146] and as such, an expectation of privacy in dialed phone numbers is not one society is prepared to recognize as reasonable.[147] Thus, whether an expectation of privacy is "one that society is prepared to recognize as reasonable"[148] is dependent, at least in part, on whether information is *voluntarily* conveyed and *knowingly* used.[149]

B. Third Parties and Expectations of Privacy in Cyberspace

What does this mean in today's digital world, where the content of a communication is itself turned over to the service provider in order to be sent?[150] Or in the cloud-computing world, where e-mails, photos, calendars, and other documents are turned over to cloud service providers for remote storage?[151] For the purposes of this Note, a simplified understanding of the Internet and e-mail will

141. A pen register is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument . . . from which a wire or electronic communication is transmitted, provided . . . that such information shall not include the contents of any communication . . ." 18 U.S.C. § 3127(3) (2012).

142. *Smith*, 442 U.S. at 745–46.

143. *Id.* at 745.

144. *Id.* at 742.

145. *Id.* at 743.

146. *Id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)).

147. *Id.* at 743.

148. *Smith*, 442 U.S. at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

149. Wilson, *supra* note 135, at 16.

150. Kerr, *supra* note 128, at 1209–10.

151. Eric Griffith, *What Is Cloud Computing?*, PC MAG. (May 3, 2016), http://www.pcmag.com/article2/0,2817,2372163,00.asp.

suffice. The Internet is a global network of computer networks.[152] An Internet user typically has a network account consisting of a block of computer storage that is owned by a service provider, such as Time Warner Cable.[153] When we use the Internet, we communicate with and through those remote computers to contact other computers.[154] When we write an e-mail message on an e-mail client (e.g., Gmail), both the message text (in binary code) and the recipient's e-mail address are turned over to the service provider, which must necessarily have access to the contents of the message in order to send it.[155] The service provider then routes the message through various networks of computers until it reaches the intended recipient.[156] Thus, every network system through which the message travels could access its content.[157] Because routing is dependent upon current traffic, nobody could know which systems these will be. The sender knows, however, that his or her Internet Service Provider ("ISP") has (and requires) access, as does the recipient's ISP.[158] For this reason, commentators have argued that in the cyberspace and Internet context, Fourth Amendment doctrines afford little protection.[159]

C. The ECPA and SCA Purportedly Address the Third-Party Problem in Cyberspace

To address the "dramatic changes in new computer and telecommunication technologies"[160] and the consequences of those technologies for privacy and Fourth Amendment protection, Congress enacted the Electronic Communications Privacy Act[161]

152. Rus Shuler, *How Does the Internet Work?* (last updated 2002), https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm.

153. Kerr, *supra* note 128, at 1209.

154. *Id.*

155. *How Email Works*, RUNBOX, https://runbox.com/email-school/how-email-works/ (last visited Feb. 6, 2017).

156. *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 522–24 (2005).

157. *Id.* at 523.

158. *Id.* at 523–24.

159. *See generally* Kerr, *supra* note 128 (explaining why it may be difficult under current Fourth Amendment doctrine to offer strong privacy protections online); Jim W. Ko, *The Fourth Amendment and the Wiretap Act Fail to Protect Against Random ISP Monitoring of E-Mails for the Purpose of Assisting Law Enforcement*, 22 J. MARSHALL J. COMPUTER & INFO. L. 493 (2004).

160. S. Rep. No. 99-541 (1986).

161. 18 U.S.C. §§ 2510–2522 (2012).

("ECPA") in 1986. The ECPA was meant to amend the Omnibus Crime Control and Safe Street Act of 1968, often called the Wiretap Act.[162] The Wiretap Act, as originally drafted, proscribed the unauthorized interception of oral and wire communications such as telephone calls.[163] The ECPA extended restrictions on government wiretaps from telephone calls to include real-time interception of transmissions of electronic data by computer, such as e-mails.[164] Title II of the ECPA, known as the Stored Communications Act ("SCA"), addresses the voluntary and compelled disclosure of stored communications and transactional records held by third-party service providers.[165] Section 2702(a) of the SCA generally bans voluntary disclosure by service providers of content as well as non-content records to any government entities, except when certain narrow, limited exceptions apply.[166]

D. The Content versus Non-Content Distinction

As illustrated above, the SCA distinguishes content information from non-content information.[167] This is likely for reasons that most people find intuitive: the contents of messages generally implicate greater privacy concerns than information about those communications.[168] The functional role of the distinction to a communications network may also explain the different treatment the two categories receive under the SCA.[169] Content information is the communication that an individual wishes to share only with the intended recipient.[170] In contrast, non-content information (sometimes referred to as "envelope" information) is information about the communication that the service provider or network uses to

162. Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 212.

163. Ko, *supra* note 159, at 512.

164. 18 U.S.C. §§ 2510–2521 (2012).

165. 18 U.S.C. §§ 2701–2712 (2012).

166. *See* 18 U.S.C. § 2702(a), (b)(5)–(8). A provider can disclose contents when: disclosure is needed to protect the provider from unauthorized use of the network; a provider discovers images of child pornography that the provider must disclose to the police by federal law; the provider inadvertently discovers evidence that relates to a crime, and; when disclosure is necessary given a dangerous emergency.

167. *See id.* § 2703(a)–(b) (compelled disclosure of content information); *id.* § 2703(c) (compelled disclosure of non-content information); *id.* § 2702(b) (voluntary disclosure of contents); *id.* § 2702(c) (voluntary disclosure of non-content records).

168. Kerr, *supra* note 128, at 1228.

169. *Id.*

170. *Id.*

deliver and process the content information.[171] Under the SCA, "contents" include "any information concerning the substance, purport, or meaning of [a] communication."[172] This clearly covers the body of electronic communications such as e-mails, that is, the actual text of the message.[173] It also arguably covers the subject line of the e-mail, since the subject line generally carries a substantive message.[174] It does not cover e-mail to/from addresses, for example, because the service provider needs this information to route communications.[175]

The content versus non-content distinction was also drawn by the Supreme Court in *Smith v. Maryland*. There, the Court noted that law enforcement's use of a pen register differed significantly from the listening device used in *Katz* because pen registers "do not acquire the *contents* of communications."[176] The court also noted that a pen register does not reveal who was on either end of the line or whether the call was even completed.[177]

E. The Effect of the ECPA and the Content versus Non-Content Distinction on Encryption

Especially in light of the distinction between content and non-content information, encryption should trigger Fourth Amendment protection. If the law *already* acknowledges that contents that are knowingly exposed to service providers deserve privacy protections under the ECPA, then contents that are concealed using digital security measures like encryption should be entitled to additional protection under the Fourth Amendment. In *Smith v. Maryland*, the Court noted that the defendant could not preserve the privacy of the number he dialed because, regardless of his attempts to keep the conversation private, he had to convey the number to the telephone company if he wished to complete his call.[178] The fact "that he dialed the number on his home phone made no conceivable difference, nor

171. *Id.*
172. *See* 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(8).
173. Kerr, *supra* note 128, at 1228.
174. *Id.*
175. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013); United States v. Forrester, 495 F.3d 1041, 1048–49 (9th Cir. 2007).
176. Smith v. Maryland, 442 U.S. 735, 741 (1979) (emphasis added).
177. *Id.*
178. *Id.* at 743.

could any subscriber rationally think that it would."[179] Conversely, encrypting a file or message before sending it renders it unreadable to the service provider and others without the decryption key. Nevertheless, the message or file can still be processed by the third-party service provider and routed to its intended recipient in its encrypted, ciphertext form. In this way, encrypting the contents of a message is very much like putting a letter in an envelope. The message can be conveyed to a third-party intermediary without revealing its contents.

Yet it was not the content versus non-content distinction that ultimately made the difference in the outcome of *Smith v. Maryland*; the deciding factor was whether the defendant's expectation of privacy in the dialed numbers was one that society was prepared to recognize as reasonable.[180] Thus, while the government can utilize the ECPA to compel disclosure of content information and contents of communications, most courts have nevertheless recognized that there is both a subjective and objective expectation of privacy in the contents of e-mails, and therefore afforded e-mails Fourth Amendment protection.[181] E-mails contain the contents of an individual's business and personal life, and it is highly unlikely that individuals "expect[] them to be made public."[182] Like the telephone user, an e-mail user is "entitled to assume that the words he utters into [a device] will not be broadcast to the world."[183]

Given the fundamental similarities between e-mail and other traditional forms of communication, like the telephone and the letter, it would "defy common sense to afford e-mails less protection."[184] Such recognition by courts demonstrates the current understanding of

179. *Id.*

180. *Id.*

181. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 284–86 (6th Cir. 2010); *In re* Application for Search Warrants for Info. Associated with Target Email Address, No. 12-MJ-8119-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (holding that "an individual has a reasonable expectation of privacy in emails" and that the Fourth Amendment protections apply to email); Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1, 8 (D.D.C. 2014) (noting the "obvious expectation of privacy e-mail account holders have in their communications"); United States v. DiTomasso, 2014 WL 5462467, at *9 (S.D.N.Y. Oct. 28, 2014) (No. 14-CR-160SAS) (holding that defendant had a reasonable expectation of privacy in e-mails but waived this Fourth Amendment protection by agreeing to AOL's terms of service).

182. *Warshak*, 631 F.3d at 284.

183. Wilson, *supra* note 135, at 13 (quoting Katz v. United States, 389 U.S. 347, 352 (1967)).

184. *Id.* (quoting *Warshak*, 631 F.3d at 285–86).

society's expectations in relation to electronic communication technologies. After all, having been enacted more than twenty years before Apple released the first iPhone in 2007, the ECPA and SCA are vastly outdated by the current state of electronic communication technology.

VI. COURTS SHOULD RECOGNIZE VIRTUAL-CONCEALMENT EFFORTS TO STANDARDIZE PRIVACY APPRAISALS IN DIGITAL CONTEXTS

The use of encryption to protect communications in transit or to secure data stored on a hard drive or remote server has become common practice.[185] Indeed, tech companies and service providers tout their encryption technologies in order to attract customers.[186] Given the pervasiveness of encryption, its effectiveness as an electronic security measure, and society's reliance upon it, courts should recognize that the use of encryption to protect the privacy of digital files and communications creates a reasonable expectation of privacy under the Fourth Amendment—one that society has already demonstrated it is willing to recognize.

Furthermore, given the difficulty and futility of comparing digital technologies to physical-world analogues, courts should follow the advice of the Supreme Court in *Riley*. That is, courts should not analogize digital technologies to the physical world,[187] but should instead look to the qualitative and quantitative differences or effects of a particular technology and its current use in our society.[188] Thus, courts should acknowledge that, although encryption is one of a limited number of security options in the digital context, its function is to protect the privacy of digital contents. Courts should also acknowledge that encryption differs qualitatively and quantitatively from physical-world security measures. Because it would take an unauthorized user millennia to determine a decryption

185. *See Our Approach to Privacy*, APPLE, http://www.apple.com/privacy/approach-to-privacy (last visited Feb. 6, 2017); *End-to-End Encryption*, WHATSAPP, https://www.whatsapp.com/faq/en/general/28030015 (last visited Feb. 6, 2017); *Making End to End Encryption Easier to Use*, GOOGLE (Jun. 3, 2014), https://security.googleblog.com/2014/06/making-end-to-end-encryption-easier-to.html.

186. *See Our Approach to Privacy*, APPLE, http://www.apple.com/privacy/approach-to-privacy/ (last visited Feb. 6, 2017); *End-to-End Encryption*, WHATSAPP, https://www.whatsapp.com/faq/en/general/28030015 (last visited Feb. 6, 2017).

187. Riley v. California, 134 S. Ct. 2473, 2493 (2014).

188. *Id.* at 2489–92.

key, current encryption standards are virtually unbreakable.[189] One "could conceivably 'figure out' the combination to a padlock more quickly and easily than [one] could decrypt modern encryption, but that does not eviscerate privacy interests in . . . physically locked container[s]."[190]

By recognizing that the use of digital encryption affords a reasonable expectation of privacy, the courts will prevent legislation that would allow law enforcement to use a technological backdoor to avoid Fourth Amendment limitations.

VII. CONCLUSION

Nevertheless, whether encryption itself triggers Fourth Amendment protection has not yet been addressed by the Supreme Court. The current state of the law allows law enforcement to create a copy of lawfully obtained digital files in their encrypted form, after which the government is free to attempt decryption without an additional warrant.[191] Moreover, the argument for encryption triggering Fourth Amendment protection only has merit if the encryption key is privately held or generated by the user (i.e., is not known to or held by the service provider). For example, Gmail, which provides encryption to protect communications in transit from hackers, also retains the encryption keys in order to scan a user's e-mails to deliver relevant advertisements to the user.[192] Under CALEA,[193] an amendment to the ECPA, service providers must provide the contents in decrypted form if they have access to the customer's encryption key. For this reason, companies like Apple, WhatsApp, and Proton Mail use encryption models that purposely put the keys beyond the company's reach and solely in the user's

189. NAT'L RES. COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 63 (Kenneth W. Dam & Herb S. Lin eds., National Academy Press 1996) (describing how increasing the key size slightly will increase the time it takes a single computer to decipher a document from a few days to 2,000 years).

190. Couillard, *supra* note 77, at 2235; *see also* Roland Pease, *'Unbreakable' Encryption Unveiled*, BBC NEWS (Oct. 9, 2008, 1:50 PM), http://news.bbc.co.uk/2/hi/science /nature/7661311.stm. (explaining that recently unveiled quantum encryption offers security using the "inherently unbreakable" laws of quantum theory).

191. FED. R. CRIM. P. 41(e)(2)(B) (2016); Kerr, *supra* note 47, at 518.

192. Hollie Slade, *The Only Email System the NSA Can't Access*, FORBES (May 19, 2014, 11:54 AM) http://www.forbes.com/sites/hollieslade/2014/05/19/the-only-email-system-the-nsa-cant-access/#6ecd192055ed.

193. 47 U.S.C. § 1002 (2012).

control.[194] Even if served with a warrant, these companies could not disclose the plaintext, only the ciphertext.

Because more and more companies are consciously moving toward this standard of encryption, CALEA is no longer helpful. Such service providers can only be compelled to provide ciphertext. Thus, even if the government first obtains a warrant to seize files or the "container" on which the files are located and is free to decrypt those files, current levels of encryption still pose a serious impediment to law enforcement. The FBI itself has stated that our law enforcement lacks the resources and technical ability to crack such encryption.[195] One company, however, has begun selling quantum computers[196] to cybersecurity agencies and law enforcement in an effort to combat the "unhackable" encryption strategies in use today.[197] Quantum computers can run computations in a coffee break that would take a supercomputer of today millions of years.[198] In response, the technology community is developing quantum encryption,[199] leading to an all-out crypto arms race.[200] For these reasons, legislation regulating encryption has been proposed.[201]

194. *See Our Approach to Privacy*, APPLE, http://www.apple.com/privacy/approach-to-privacy (last visited Feb. 6, 2017); *End-to-End Encryption*, WHATSAPP, https://www.whatsapp.com/faq/en/general/28030015 (last visited Feb. 6, 2017); Slade, *supra* note 192.

195. U.S. DEP'T OF HOMELAND SEC., GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE (2016), https://homeland.house.gov/wp-content/uploads/2016/09/Staff-Report-Going-Dark-Going-Forward-Version-2.0.pdf.

196. A normal computer uses bits (data that can exist in two states: zero or one). Quantum computers use quantum bits, or "qubits," which can be zero, one, or any state in between. This means that the computational abilities and speed of a supercomputer are exponentially increased. Nicola Davis, *Quantum Computing Explained: Harnessing Particle Physics to Work Faster*, THE GUARDIAN (Mar. 6, 2014, 1:59 PM), https://www.theguardian.com/science/2014/mar/06/quantum-computing-explained-particle-mechanics.

197. Lily Hay Newman, *Quantum Computers Versus Hackers, Round One. Fight!*, WIRED (Jan. 27, 2017, 7:00 AM), https://www.wired.com/2017/01/quantum-computers-versus-hackers-round-one-fight.

198. Tom Simonite, *Google's Quantum Dream Machine*, MIT TECH. REV. (Dec. 18, 2015), https://www.technologyreview.com/s/544421/googles-quantum-dream-machine.

199. Quantum encryption exploits the properties of physics and literally encodes atomic light particles, called photons, with information. Because quantum encryption exploits the laws of physics, quantum computing, which exploits statistical and mathematical concepts, will not help decrypt communications encrypted using quantum encryption technologies. Devin Powell, *What Is Quantum Cryptography? And Can it Make Codes Truly Unbreakable?*, POPULAR SCI. (Mar. 3, 2016), www.popsci.com/what-is-quantum-cryptography.

200. Adam Mann, *Laws of Physics Say Quantum Cryptography Is Unhackable. It's Not.*, WIRED (Jun. 7, 2013, 6:30 AM), https://www.wired.com/2013/06/quantum-cryptography-hack/.

201. *See generally* Compliance with Court Orders Act of 2016 (Discussion Draft 2016), https://www.burr.senate.gov/imo/media/doc/BAG16460.pdf; *The Encryption Tightrope:*

Nevertheless, for the reasons discussed in this Note, any attempt at regulation should be analyzed under the Fourth Amendment and will likely receive criticism on Fourth Amendment grounds.

Balancing Americans' Security and Privacy: Hearing before the H. Comm. on the Judiciary, 114th Cong. (2016) (statement of James B. Comey, Director, Federal Bureau of Investigation).