DePaul University
University Libraries

DePaul Law Review

Volume 65
Issue 3 *Spring 2016*

Article 6

Where Are Your Papers?: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, The Cloud, and Encryption

Wei Chen Lin

WHERE ARE YOUR PAPERS?: THE FOURTH AMENDMENT, THE STORED COMMUNICATIONS ACT, THE THIRD-PARTY DOCTRINE, THE CLOUD, AND ENCRYPTION

INTRODUCTION

"Where are your papers?!" This is a well-known trope employed to lampoon authoritarian regimes.[1] Although these colloquial "papers" are often seized by executive discretion,[2] other papers enjoy very strong protection under the Fourth Amendment. The Fourth Amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[3] and it generally prohibits warrantless searches.[4] However, electronic systems, which are replacing the papers traditionally used for storage and communication, complicate the analysis of what is and is not protected by the Fourth Amendment. This Comment addresses the practical consequences of continued uncertainty over Fourth Amendment protection of electronically stored information (ESI) and how those consequences can be avoided. Specifically, this Comment asks: What constitutes the papers protected under the Fourth Amendment, and where are those papers?

People routinely send and store sensitive information with various service providers,[5] such as photos in iCloud, documents in Dropbox,

---

1. *See* Harry Binswanger, *Amnesty for Illegal Immigrants Is Not Enough, They Deserve an Apology*, FORBES (Mar. 4, 2013, 8:00 AM), http://www.forbes.com/sites/harrybinswanger/2013/03/04/amnesty-for-illegal-immigrants-is-not-enough-they-deserve-an-apology/#78f4a4bd1a9c.

2. *See generally* Ramzi Kassem, *Passport Revocation as Proxy Denaturalization: Examining the Yemen Cases*, 82 FORDHAM L. REV. 2099 (2014) (examining executive authority to revoke passports).

3. U.S. CONST. amend. IV.

4. Riley v. California, 134 S. Ct. 2473, 2491–95 (2014).

5. *E.g.*, Robert Hackett, *Despite Risks, Businesses Store Sensitive Data in the Cloud Unprotected*, FORTUNE (May 2, 2014, 3:16 PM), http://fortune.com/2014/05/02/despite-risks-businesses-store-sensitive-data-in-the-cloud-unprotected/. An Internet service provider (ISP) provides access to the internet. *ISP Definition from PC Magazine Encyclopedia*, PCMAG, http://www.pcmag.com/encyclopedia/term/45481/isp (last visited May 10, 2016). "Service provider" refers to any provider that provides services on the Internet. *Service provider Definition from PC Magazine Encyclopedia*, PCMAG, http://www.pcmag.com/encyclopedia/term/51187/service-provider (last visited May 10, 2016). An ISP can be considered a subset of service providers. *Id.* The terms are sometimes used interchangeably when the type of entity being referred to is clear from the context. *E.g.*, Fed. Commc'ns Comm'n, Broadband Decisions: What Drives Consumers

e-mails in Gmail, and system backups in Crashplan.[6] Under the third-party doctrine, by revealing information to a third party, people relinquish their Fourth Amendment protection.[7] Electronic devices, such as a cellphone, routinely share information without any meaningful user interaction.[8] In fact, it is practically impossible for the average user operating a device with the latest iteration of Microsoft Windows to stop that device from communicating with the "cloud."[9]

Existing legal protection for ESI is insufficient. The Stored Communications Act (SCA)[10] was enacted to emulate Fourth Amendment protection for some ESI.[11] However, even for the protected ESI, the protection provided by the decades-old SCA no longer conforms to modern privacy expectations. The SCA requires a warrant for the government to search e-mails stored for less than 180 days but only a subpoena or a court order for information stored for more than 180 days.[12] Privacy expectation in remotely stored electronic information does not diminish simply because 180 days has elapsed[13] just as privacy expectation in other storage mediums does not diminish simply because of the passage of time.

[A] landlord or storage locker owner has keys to a tenant's space, a bank has the keys to a safe deposit box, and a postal carrier has the keys to a mailbox."[14] Any information in these storage mediums,

---

To Switch—or Stick with—Their Broadband Internet Provider (working paper) (Dec. 2010), https://apps.fcc.gov/edocs_public/attachmatch/DOC-303264A1.pdf.

6. *See* Rick Broida, *How To Build a Bulletproof Cloud Backup System Without Spending a Dime*, PCWORLD (Apr. 30, 2013, 3:00 AM), http://www.pcworld.com/article/2036488/how-to-build-a-bulletproof-cloud-backup-system-without-spending-a-dime.html; Steve Ragan, *A Blue Team's Reference Guide To Dealing with Ransomware*, CSO (Mar. 22, 2016, 4:00 AM), http://www.csoonline.com/article/3046586/techology-business/a-blue-teams-reference-guide-to-dealing-with-ransomware.html.

7. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

8. *Security Now!: Security Is Difficult* (Gibson Research Corporation podcast Aug. 18, 2015) (transcript at 3–4, 8–9), https://www.grc.com/sn/sn-521.pdf.

9. *Id.* (transcript at 9) ("For example, if we absolutely turn everything that we can find off, that is, to its most privacy-enforcing settings, how does Windows 10 perform? And unfortunately, it cannot resist talking to the Internet.").

10. Pub. L. No. 99-508, §§ 201–02, 100 Stat. 1848, 1860–68 (1986) (codified as amended at 18 U.S.C. §§ 2701–10 (2012)).

11. 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, 1212–14, 1218–23 (2004) (explaining the various warrant, subpoena, and notice requirements for e-mails, content files, records, and logs stored by the ISP).

12. 18 U.S.C. §§ 2703(a)–(c).

13. *See* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2237–38 (2009) (reasoning that electronic information should be treated the same as information stored in private places (e.g., tenant spaces, safe deposit boxes, and mailboxes)).

14. *Id.*

then, are arguably exposed to the third party. Despite that exposure, the third-party doctrine does not give "law enforcement the authority to use those third parties as a means to enter a private space" like a storage locker, a safe deposit box, or a mailbox.[15] This Comment shows that remote electronic storage is comparable to safety deposit boxes. Therefore, similar to Fourth Amendment expectations of privacy in a safety deposit box, and other types of secure storage, expectations of privacy in electronic storage should not simply diminish with the passage of time.[16]

In *Riley v. California*,[17] the U.S. Supreme Court held that warrantless searches of data stored on a cellphone incident to a lawful custodial arrest were unconstitutional, and the Court explicitly noted the challenges of separating local and cloud storage.[18] The data that is physically stored on a cellphone is just a fraction of the personal data duplicated and stored on various cloud-based services that average consumers access using the same cellphone.[19] Legal recognition of the expectation of privacy should extend to consumer data stored in the service provider's physical infrastructure that is used to provide a cloud-based service.

Strong encryption for ESI has been readily available for a long time.[20] The same techniques currently used to enable secure Internet commerce and secure institutional communications can be used for stored communication.[21] Strong encryption commonly refers to encryption that is computationally infeasible to defeat without the correct encryption key.[22] Although currently not widely deployed by the

15. *Id.* at 2238.

16. *See id.* at 2237–38.

17. 134 S. Ct. 2473 (2014).

18. *Id.* at 2491, 2495.

19. *Id.* at 2491. By design, cloud-based services provide a seamless experience that often does not provide clear demarcations between what is stored locally versus remotely. PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-145, THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF STANDARDS AND TECHNOLOGY 2 (Sept. 2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

20. *Security Now!: Shocked by the Shell* (Gibson Research Corporation podcast Oct. 1, 2014) (transcript at 10), https://www.grc.com/sn/sn-475-notes.pdf.

21. *Security Now!: Disconnect* (Gibson Research Corporation podcast Sept. 15, 2015) (transcript at 7–8), https://www.grc.com/sn/sn-525-notes.pdf. (discussing the use of key exchange protocols in secure messaging products, such as Threema and Telegram). Key exchange protocols are used to exchange encryption keys to secure Internet traffic. For example, anytime a user visits a website that displays "https" in the address bar rather than "http," that connection is secured by encryption that exchanged encryption keys using a key exchange protocol. *See id.* (transcript at 11).

22. David Mertz, *Introduction to Cryptology, Part 1: Basic Cryptology Concepts*, IBM: DEVELOPERWORKS, (Jan. 16, 2001), http://www.ibm.com/developerworks/tivoli/tutorials/s-crypto/s-crypto.html.

casual users for stored communication and remote file storage, strong encryption is not new and can be readily deployed en masse if the market demands it.[23]

Wide deployment of strong encryption will have dire practical consequences for law enforcement because strong encryption makes it impossible, irrespective of warrants, for law enforcement to recover encrypted ESI.[24] Strong encryption has not been widely deployed because the technical difficulties of prior implementations create a high bar of entry, and there is a lack of interest in strong encryption by the casual user, which prevents efforts to develop user-friendly implementations.

Before the Snowden revelations,[25] more people accepted that law enforcement had a valid interest in intercepting and recovering information with little restriction for investigative purposes, such as investigating kidnappings or terrorist activities.[26] However, in the wake of the Snowden revelations, interest in strong encryption has increased, and companies are making those technologies widely available in response to consumer demand.[27] If concerns over the uncertainty of legal protections for ESI are not addressed, the combination of increased interest in, and availability of, strong encryption to the casual user will lead to mass adoption of strong encryption, leaving law enforcement in the dark.

This Comment argues that Congress should amend the SCA to provide legal protection of all ESI that conforms to modern privacy expectations and rebuild the trust between law enforcement and the people of the United States to avoid mass adoption of strong encryption and the associated security and economic consequences. This legal protection must provide, at a minimum, an expectation of privacy that does not simply diminish with the passage of time and that

23. *See Worldwide Encryption Products Survey*, SCHNEIER ON SECURITY (Feb. 11, 2016, 11:05 AM), https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html ("The findings of this survey identified 619 entities that sell encryption products. Of those 412, or two-thirds, are outside the U.S.-calling into question the efficacy of any US mandates forcing backdoors for law-enforcement access. . . . These foreign products offer a wide variety of secure applications—voice encryption, text message encryption, file encryption, network-traffic encryption, anonymous currency . . . .").

24. *Security Now!: Shocked by the Shell*, *supra* note 20, (transcript at 8–9).

25. Edward Snowden, an ex-National Security Agency (NSA) contractor, disclosed the NSA's mass surveillance programs. Barton Gellman et al., *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST, June 9, 2013, https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

26. *Security Now!: Shocked by the Shell*, *supra* note 20, (transcript at 9).

27. *Id.* (transcript at 8–9).

removes the arbitrary distinction between communication and storage. Part II presents an overview of Fourth Amendment jurisprudence, SCA case law, cloud computing, strong encryption, and the U.S. Supreme Court's recognition of search and seizure challenges inherent in the cloud.[28] Part III argues that the current protections do not adhere to consumer expectations of privacy because: (1) Internet use, which requires "disclosure" of information to third parties, has become ubiquitous and unavoidable[29] and (2) information stored with a service provider should not be considered "disclosed" to a third party.[30] Thus, uncertainties surrounding Fourth Amendment protection of consumer information will lead to mass adoption of encryption.[31] Part IV argues that if clear and understandable legal protection is not available: (1) people will continue to develop and adopt strong encryption that cannot be circumvented when law enforcement and intelligence agencies have a legitimate need to do so[32] and (2) efforts to ban these technologies would have dire economic consequences.[33] Part V concludes that Congress must amend the SCA to recognize Fourth Amendment protection for ESI, eliminate the arbitrary 180-day rule and the distinction between storage and communication, uphold search warrant requirements despite of the third-party doctrine, and rebuild the trust between law enforcement and the people of the United States to avoid the mass adoption of strong encryption, and the associated security and economic consequences.

II. Background

The third-party doctrine provides that information disclosed to a third party is not protected by the Fourth Amendment.[34] The SCA was enacted approximately thirty years ago as part of the Electronic Communications Privacy Act of 1986[35] to provide some Fourth Amendment-like protection for information disclosed to service providers.[36] In *Riley v. California*, the U.S. Supreme Court recognized complications brought to Fourth Amendment expectation of privacy

28. *See infra* notes 34–162 and accompanying text.
29. *See infra* notes 163–88 and accompanying text.
30. *See infra* notes 189–203 and accompanying text.
31. *See infra* notes 204–46 and accompanying text.
32. *See infra* notes 247–58 and accompanying text.
33. *See infra* notes 259–305 and accompanying text.
34. Kerr, *supra* note 7, at 563.
35. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
36. Kerr, *supra* note 11, at 1212.

analysis by the expansiveness of, and social reliance on, data stored in the cloud.[37]

A. Current Fourth Amendment Protection for Storage and Communications

"The Fourth Amendment offers strong privacy protections for our homes in the physical world."[38] The level of Fourth Amendment protection is highest with regard to a person's home. However, the U.S. Supreme Court has extended Fourth Amendment protection to various other spaces and containers. The third-party doctrine provides that once information is disclosed to a third party, Fourth Amendment protection is waived.[39] The justification for this rule stems from the reasonable expectation of privacy test established in *Katz v. United States*.[40]

In *Katz*, FBI agents attached an electronic recording device on the outside of a public telephone booth in which Charles Katz made telephone calls to make gambling wagers.[41] The Court held that Fourth Amendment "considerations do not vanish when the search in question is transferred from the setting of a home . . . to that of a telephone booth" and reasoned that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[42] The Court emphasized that "the Fourth Amendment protects people, not places"; therefore, "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[43] The now famous test established in Justice Harlan's concurrence consists of a "twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as [objectively] 'reasonable.'"[44]

---

37. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

38. Kerr, *supra* note 11, at 1209 (citing Kyllo v. United States, 533 U.S. 27, 31 (2001)).

39. Kerr, *supra* note 7, at 563 ("The 'third-party doctrine' is the Fourth Amendment rule that governs collection of evidence from third parties in criminal investigations. The rule is simple: By disclosing to a third-party, the subject gives up all of [her] Fourth Amendment rights in the information revealed." (footnote omitted)).

40. 389 U.S. 347, 361(1967) (Harlan, J., concurring); Kerr, *supra* note 7, at 563.

41. *Katz*, 389 U.S. at 348.

42. *Id.* at 359.

43. *Id.* at 351.

44. *See id.* at 361 (Harlan, J., concurring); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information [she] voluntarily turns over to third parties."). The government's bulk collection of metadata—or "data about data," such as sender and recipient information—as service provider business records is a distinct issue and beyond the scope of this Comment. See Laura K.

For instance, as far back as 1966, the Court recognized that Fourth Amendment protection extends to a hotel room.[45] However, a property manager can consent to a warrantless search after the rental period has expired.[46] Fourth Amendment protection also extends beyond homes or places of temporary residence to storage facilities, storage boxes, cordless phones, and, in certain circumstances, e-mails.[47] However, not all containers enjoy Fourth Amendment Protection.

Whether these storage containers should be afforded Fourth Amendment protection generally depends on two factors: (1) whether the containers are of the type that "historically command a high degree of privacy" and (2) "the precautions taken by the owner to manifest [her] subjective expectation of privacy."[48] In addition, "[n]either ownership nor presence are required to assert a reasonable expectation of privacy [in these containers] under the Fourth Amendment."[49] All that is required to gain Fourth Amendment protection for storage shared with a third-party is a "formalized arrangement . . . indicating joint control and supervision of the place."[50]

Because Fourth Amendment protection for storage is important, it is even available to a defendant who denies ownership of a rented storage space at a storage facility. In *United States v. Dilley*,[51] police officers investigating the defendant for illegal drug activity followed the defendant to a storage facility.[52] The defendant tried to escape after the officers "initiated a stop based on . . . outstanding warrants."[53] After the defendant was arrested, handcuffed, and *Mirandized*, the defendant was asked if "he rented a unit at the stor-

---

Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 759–60 (2014), for an example of metadata collection.

45. "A hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office. The Fourth Amendment can certainly be violated by guileful as well as by forcible intrusions into a constitutionally protected area." Hoffa v. United States, 385 U.S. 293 (1966) (citations omitted). The court ultimately rejected Hoffa's Fourth Amendment claims because his incriminating statements were made in the presence of a third party who was not a surreptitious eavesdropper. *Id.* at 302. Therefore, the court reasoned that Hoffa did not rely on the security of his hotel suite but, rather, the misplaced confidence in a third party. *Id.*

46. United States v. Allen, 106 F.3d 695, 699–700 (6th Cir. 1997) (citing United States v. Rahme, 813 F.2d 31, 34 (2d Cir. 1987); United States v. Larson, 760 F.2d 852, 854 (8th Cir. 1985); and United States v. Parizo, 514 F.2d 52, 54 (2d Cir. 1975)).

47. *See infra* notes 52–86 and accompanying text (discussing cases that hold this as the law).

48. United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1992).

49. United States v. Johns, 851 F.2d 1131, 1136 (9th Cir. 1988).

50. United States v. Broadhurst, 805 F.2d 849, 851–52 (9th Cir. 1986).

51. 480 F.3d 747 (5th Cir. 2007).

52. *Id.* at 748.

53. *Id.*

age facility."[54] Even after being confronted about a storage facility receipt that was found in his wallet for the storage facility, the defendant "vehemently denied" ownership.[55] The defendant stated: "I don't have a unit over there. You can search any of them over there. You are not going to find anything."[56] The court reasoned that "Dilley maintained the expectation of privacy in his storage unit even after denying his ownership, then he exercised his property rights by consenting to a search of the location."[57]

Likewise, Fourth Amendment protection for communication is maintained even when the communication can be tapped into with little effort. In *United States v. Smith*,[58] the U.S. Court of Appeals for the Fifth Circuit addressed whether warrantless tapping of cordless phones is permissible.[59] A neighbor suspected the defendant of being involved with break-ins at the neighbor's house.[60] The neighbor eavesdropped on the defendant's cordless telephone calls and discovered that the defendant was a drug dealer.[61] Then, the neighbor contacted a friend at the police department and was instructed to record the calls.[62] The court acknowledged prior cases that held that defendants who used cordless phones had no reasonable expectation of privacy, but ultimately the court held that "these cases should not be read to stand for the proposition that a communication loses Fourth Amendment protection simply because it is not transmitted by wire. There is nothing magical about a telephone line."[63] The court reasoned that just because someone may eavesdrop on a conversation does not grant the government a license to eavesdrop on the conversation.[64]

---

54. *Id.*

55. *Id.*

56. *Id.*

57. *Dilley*, 480 F.3d at 750. The court distinguished *Dilley* from *United States v. Vega*, 221 F.3d 789 (5th Cir. 2000), in which the defendant denied residing at a particular house. *Id.* (citing *Vega*, 221 F.3d at 797). The court in *Dilley* emphasized that refusal to give incriminating answers is not a waiver of the expectation of privacy in a residence. *Id.*

58. 978 F.2d 171 (5th Cir. 1992).

59. *Id.* at 179–80.

60. *Id.* at 173.

61. *Id.*

62. *Id.*

63. *Id.* at 179.

64. *Smith*, 978 F.2d at 180–81 ("No matter how technologically advanced cordless communication becomes, some people will always find a way to eavesdrop on their neighbors. However, '[t]he fact that [Listening] Toms abound does not license the government to follow suit.'" (alterations in original) (footnote omitted) (quoting United States v. Kim, 415 F. Supp. 1252, 1256 (D. Haw. 1976))).

Although the court "express[ed] no opinion as to what features or circumstances would be necessary to give rise to a reasonable expectation of privacy, it should be obvious that as technological advances make cordless communications more private, such communication will be entitled to Fourth Amendment protection."[65] The court also advised against judicial intervention.[66] In his dissenting opinion, Justice Marshall stated: "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[67]

Similar to the inquisitive neighbor, ISPs can eavesdrop on e-mails. Steven Warshak, owner of Berkeley Premium Nutraceuticals,[68] brought a civil case "to stop the government's repeated secret searches and seizures of his stored e-mail using the SCA."[69] A panel of the circuit judges found "little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial [ISPs]."[70] This often-cited opinion was vacated en banc for ripeness, but, as discussed *infra*, in Warshak's criminal appeal, the court essentially agreed with the vacated opinion and recognized Fourth Amendment protection for e-mails.[71]

Drawing from the U.S. Supreme Court's opinion in *Katz*, in *Warshak v. United States*, the court held that the "content of e-mail is something that the user 'seeks to preserve as private' and therefore 'may be constitutionally protected.'"[72] The court stated that "like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications

65. *Id.* at 180.

66. *Id.* at 181 ("Granted, it would be easier to apply a general rule that it either is or is not reasonable to expect privacy for cordless telephone communications. The creation of such a general rule, however, is beyond the proper role of the judiciary.").

67. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

68. Perhaps most famous—outside of electronic discovery circles—for its "Smiling Bob" commercials. *See* Dan Slater, *Fraudulent Male Enhancement Drug Gets Company Founder 25 Yrs.*, WALL ST. J.: L. BLOG (Aug. 27, 2008, 3:43 PM) http://blogs.wsj.com/law/2008/08/27/fraudulent-male-enhancement-drug-gets-company-founder-25-yrs/.

69. *Court Protects E-mail from Secret Government Searches*, ELECTRONIC FRONTIER FOUND. (June 18, 2007), https://www.eff.org/deeplinks/2007/06/court-protects-email-secret-government-searches (citing Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), *reh'g en banc granted*, *opinion vacated*, Oct. 9, 2007).

70. *Warshak*, 490 F.3d at 473.

71. *See infra* notes 95–98 and accompanying text.

72. *Id.* at 473 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past."[73]

In *Warshak*, the government argued that expectations of privacy are waived because service providers screen e-mails for illegal and malicious content.[74] The court analogized this screening process to a "post office screening packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the packages."[75] The court also held that "[t]he fact that such screening occurs as a general matter does not diminish the well-established reasonable expectation of privacy that users of the mail maintain in the packages they send."[76]

Even in government-operated servers, military personnel maintain a reasonable, subjective expectation of privacy in e-mails. In *United States v. Long*,[77] the court took a banner about monitoring, which was displayed at the computer's login prompt, as describing "access to 'monitor' the computer system, not to engage in law enforcement intrusions by examining the contents of particular e-mails in a manner unrelated to maintenance of the e-mail system."[78] The court in *Long* emphasized that the defendant's possession of a password known only to her supported "a subjective expectation that access to her e-mails was protected and severely limited."[79]

In *United States v. Mourning*,[80] the court recognized a reasonable expectation of privacy in a locked strongbox that multiple people had access to through a shared studio.[81] "It is perfectly reasonable to recognize an expectation of privacy in a hidden, locked safe or strong box, despite the fact that more than one person, and as many as ten, had keys or access to the studio."[82] The court reasoned, in part, that "enclosed spaces" represented places with the highest expectations of privacy.[83]

In fact, an expectation of privacy may be maintained even when information is voluntarily shared with a third party. In her concurring opinion in *United States v. Jones*,[84] Justice Sotomayor wrote that "it

73. *Id.*
74. *Id.*
75. *Id.* at 474.
76. *Id.*
77. 64 M.J. 57 (C.A.A.F. 2006).
78. *Id.* at 63.
79. *Id.*
80. 716 F. Supp. 279 (W.D. Tex. 1989).
81. *Id.* at 279, 291–92.
82. *Id.* at 292.
83. *Id.* (quoting United States v. Block, 590 F.2d 535, 541 (5th Cir. 1978)).
84. 132 S. Ct. 945 (2012).

may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[85] Justice Sotomayor recognized the chasm between the traditional third-party doctrine and the way people use technology now, writing:

> [The] approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[86]

Many types of storage and communication are protected by the Fourth Amendment. However, stored communication, such as e-mail, is not protected by the Fourth Amendment. The SCA mimics *some* aspects of Fourth Amendment protection for stored communications.

B. Current SCA Protection for Consumer Data Stored with Service Providers

The SCA was enacted to provide some Fourth Amendment-like protection for information disclosed to service providers;[87] however, advances in technology have made the applicability of the SCA uncertain and imprecise. Congress enacted the SCA to protect certain types of network communications, "freezing into the law the understandings of computer network use as of 1986."[88] When the SCA was enacted as part of the Electronic Communications Privacy Act in 1986, "most people couldn't imagine that online data storage would approach the point where it was so inexpensive people would leave their data online, so it was assumed that email left in networked stor-

85. *Id.* at 957 (Sotomayor, J., concurring).

86. *Id.* (Sotomayor, J., concurring).

87. Kerr, *supra* note 11, at 1212 ("The SCA . . . [offers] network account holders a range of statutory privacy rights against access to stored account information held by network service providers. The statute creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information.").

88. *See id.* at 1214. As a point of reference, the SCA was enacted approximately ten years before Google began as a research project of two Ph.D. students at Stanford University. *Our History in Depth*, GOOGLE CO., https://www.google.com/about/company/history/.

age over 180 days could be considered abandoned—like garbage on the curb."[89]

The SCA defines two types of providers, "providers of electronic communication service (ECS) and providers of remote computing service (RCS)"—a distinction from the age of time-sharing and mainframes.[90] Section 2703(a) of the SCA provides that "[a] governmental entity may require the disclosure by [an ECS] provider of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for *one hundred and eighty days or less*, only pursuant to a [probable cause] warrant."[91] Section 2703(a) also provides that a government entity may require the disclosure of information "that has been in electronic storage in an electronic communications system for *more than one hundred and eighty days* by the means available under subsection (b)." Section 2703(b), which also governs how a government entity can require disclosure by a RCS provider regardless of the amount of time the information has been stored, provides that a government entity may require disclosure "without required notice to the subscriber or customer" with a probable cause warrant, or "with prior notice . . . to the subscriber if the government entity uses an administrative subpoena,"[92] or "obtains a court order" that shall be issued "if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds* to believe that the contents . . . are relevant and material to an ongoing criminal investigation."[93] In short, for any information stored with a RCS provider, or information stored with an ECS provider for more than 180 days, the government entity need not show probable cause but can obtain the information with notice to the customer and either an administrative subpoena or a court order issued under the lower "reasonable grounds" standard.[94]

In *United States v. Warshak*, the Sixth Circuit held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'" and that warrantless searches are unconstitutional.[95] In 2010, the

89. Andrea Peterson, *The Government Can (Still) Read Most of Your E-mails Without a Warrant*, THINKPROGRESS (Mar. 20, 2013, 12:00 PM), http://thinkprogress.org/justice/2013/03/20/1742871/leahy-ecpa-reform-email/.

90. Kerr, *supra* note 11, at 1214.

91. *Id.* §2703(a) (emphasis added).

92. *Id.* §2703(b) (emphasis added).

93. *Id.* §2703(d) (emphasis added).

94. *Id.* §2703 (a)–(d).

95. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), *reh'g en banc granted*, *opinion vacated*, Oct. 9, 2007).

same parties from *Warshak* presented the same issue in a criminal appeal, and "[t]he court *again* held that the government violated Warshak's Fourth Amendment rights by compelling [the service providers] to turn over the contents of his private e-mails."[96] The Sixth Circuit analogized rental spaces, in which "an 'expectation [of privacy] persists, regardless of the incursions of handymen to fix leaky faucets.' Therefore, some routine access to stored e-mail to audit, inspect, or monitor is not enough to break the expectation of privacy."[97] Furthermore, "[t]he Sixth Circuit held that an e-mail account holder has a reasonable expectation of privacy in the contents of stored e-mail, [and declared a provision of the SCA] unconstitutional because it permits the issuance of a search warrant upon a standard short of probable cause."[98] Among the many decisions recognizing the holding in *Warshak*, a D.C. district court held that "to the extent the SCA allows access to e-mails without a warrant, it is unconstitutional" and observed that the limits of the SCA are not clear.[99]

To further complicate the analysis, sometimes it is not even clear whether the information sought is the consumer's data or a provider's business record. In *In re United States for Historical Cell Site Data*,[100] the U.S. Court of Appeals for the Fifth Circuit held that historical cell site data, which reveals the subscriber's location history, is a business record; thus, warrantless searches of that information are not per se unconstitutional.[101] However, in *United States v. Davis*,[102] the U.S. Court of Appeals for the Eleventh Circuit held that "cell site location information is within the subscriber's reasonable expectation of privacy. The obtaining of that data without a warrant is a Fourth Amendment violation."[103]

This uncertainty over whether ESI is protected by the SCA, or even whether the SCA applies in a specific instance, is due, in part, to the fact that "[t]he SCA is not a catch-all statute designed to protect the privacy of stored Internet communications; instead it is narrowly tailored to provide a set of Fourth Amendment-like protections for com-

96. Spencer S. Cady, Note, *Reconciling Privacy with Progress: Fourth Amendment Protection of E-Mail Stored with and Sent Through a Third-Party Internet Service Provider*, 61 DRAKE L. REV. 225, 245 (2012) (emphasis added) (citing *Warshak*, 631 F.3d at 282).

97. *Id.* at 246 (footnote omitted) (quoting *Warshak*, 631 F.3d at 287).

98. *Id.* (citing *Warshak*, 631 F.3d at 288).

99. *Id.*

100. 724 F.3d 600 (5th Cir. 2013).

101. *Id.* at 604.

102. 754 F.3d 1205, *reh'g en banc granted*, *opinion vacated*, 573 F. App'x 925 (11th Cir. 2014) (mem.).

103. *Id.* at 1217.

puter networks."[104] Since the enactment of the SCA in 1986, the Internet has become an indispensable part of everyday life.

On November 10, 2014, President Obama made a statement urging the Federal Communications Commission (FCC) to "reclassify consumer broadband service under Title II of the Telecommunications Act" to protect net neutrality.[105] In the accompanying video, President Obama asked the FCC "to recognize that for most Americans, the Internet has become an essential part of everyday communication and everyday life."[106] On February 26, 2015, the FCC adopted the "Open Internet Rules" designed to ensure net neutrality; the rules went into effect on June 12, 2015.[107]

Cloud computing has developed, in part, to cope with the increased demand on service providers as a result of our increased reliance on the Internet, and strong encryption has garnered public attention.

C. "Cloud" Computing and Strong Encryption

The National Institute of Science and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[108] The term was popularized when Amazon announced its Amazon Elastic Compute Cloud (Amazon EC2),[109] which is part of the Amazon Web Services (AWS) infrastructure that provides computing resources for organizations

104. Kerr, *supra* note 11, at 1214.

105. Statement on Internet Neutrality, 2014 DAILY COMP. PRES. DOC. DCPD201400841 (Nov. 10, 2014). The FCC announced the adoption of the proposed changes on February 26, 2015, and it noted that "the nature of broadband Internet access service has . . . changed since [its] initial classification." Press Release, Fed. Commc'ns Comm'n, FCC Adopts Strong, Sustainable Rules To Protect the Open Internet (Feb. 26, 2015). Net neutrality is the principle that ISPs should not "discriminate" legitimate traffic by blocking, throttling, or utilizing paid prioritization of traffic. *Id.* ISPs therefore, cannot interfere with traffic to the benefit of their affiliates or to the detriment of their competitors. *Id.*

106. Joel Rose, *Obama Backs Net Neutrality, Asks FCC To Regulate Internet*, NPR, http://www.npr.org/2014/11/10/363101482/obama-backs-net-neutrality-asks-fcc-to-regulate-internet (last updated Nov. 10, 2014, 7:08 PM).

107. *Open Internet*, FCC, https://www.fcc.gov/general/open-internet (last visited Jan. 15, 2016).

108. MELL & GRANCE, *supra* note 19, at 2.

109. *See Announcing Amazon Elastic Compute Cloud (Amazon EC2) – beta*, AMAZON WEB SERVS. (Aug. 24, 2006), https://aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2—-beta/.

and companies such as Netflix, Reddit, Yelp, Dow Jones, and the CDC.[110]

Essential characteristics of the cloud, as defined by the NIST, include on-demand self-service, broad network access, resource pooling, rapid elasticity (to automatically scale service capabilities with demand), and measured service (to provide monitoring of resources for both maintenance and billing).[111] These capabilities also allow services, including those that enable mass adoption of strong encryption, to deploy and rapidly respond to consumer demand with very little friction.[112]

Cloud computing's goal is to create an environment in which users are not, and need not be, aware of the number, identity, location, or capabilities of the individual resources that provide them with the computing resources that they can utilize.[113] The cloud actually provides opaqueness because "the cloud is merely an illusion. You don't really get your applications or compute power from a 'cloud' somewhere—there are real physical servers and datacenters that supply this capacity."[114] This leads to the common view among users that the cloud is an abstract entity somewhere "out there." However, the cloud, which is presented as a service, is actually powered by an infrastructure composed of many real physical facilities called "data centers" that perform processing and host data.[115]

Cloud services are marketed, in part, for their security because consumers expect their ESI to be well protected.[116] Data centers are essentially large complexes or warehouses that are home to an array of server hardware.[117] The data centers support and protect these serv-

110. *See* Steven Musil, *Amazon Cloud Outage Downs Netflix, Quora*, CNET (Aug. 8, 2011, 9:35 PM), http://www.cnet.com/news/amazon-cloud-outage-downs-netflix-quora/; *All AWS Customer Stories*, AMAZON WEB SERVS., https://aws.amazon.com/solutions/case-studies/all/ (last visited Apr. 3, 2016).

111. MELL & GRANCE, *supra* note 19, at 2.

112. *See Saying Goodbye to Encrypted SMS/MMS*, OPEN WHISPER SYS. (Mar. 6, 2015), https://whispersystems.org/blog/goodbye-encrypted-sms/; *Telegram FAQ*, TELEGRAM, https://telegram.org/faq (last visited Apr. 3, 2016).

113. *See* Sean Rhea et al., *Maintenance-Free Global Data Storage*, IEEE INTERNET COMPUTING, Sept./Oct. 2001, at 40, 40–41, 48, http://www.srhea.net/papers/ieeeic.pdf.

114. Joe McKendrick, *Needed More than Ever: DevOps To Manage Cloud Unpredictability*, ZDNET (June 23, 2014, 4:15 PM), http://www.zdnet.com/article/needed-more-than-ever-devops-to-manage-cloud-unpredictability/.

115. *See* KAPIL BAKSHI, CISCO SYS., INC., CISCO CLOUD COMPUTING - DATA CENTER STRATEGY, ARCHITECTURE, AND SOLUTIONS 3–4 (1st ed. 2009), http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/CiscoCloudComputing_WP.pdf.

116. *See, e.g.*, *Cloud Services*, IRON MOUNTAIN, http://www.ironmountain.com/Services/Data-Management/Cloud-Backup-Services.aspx (lasted visited Apr. 3, 2016).

117. BAKSHI, *supra* note 115, at 15.

ers with redundant utilities, concrete walls "lined with Kevlar" for extra protection, limited windows, check points with guards who "use mirrors to check underneath vehicles for explosives," and HVAC systems that protect people and equipment from biological and chemical attack, as well as smoke from nearby fires.[118] Access to these facilities is controlled by biometric identification and mantraps as well as layers of security—part of a strategy of "defense in depth."[119] To enter a data center and access a specific server, a visitor must often satisfy the highest standards in multifactor authentication.[120] The three pillars of multifactor authentication are: "something I have, something I am, and something I know."[121] Even for a data center hosting multiple independent users, this authentication often means a badge, a biometric feature, and a PIN.[122]

Although the data in the datacenters is well protected from unauthorized access, service providers can, and do, scan traffic and "read" e-mails.[123] However, the process is accomplished by automated systems that try to, for example, identify spam and mine for data in e-mails that are of interest to advertisers.[124]

Service providers also use hash functions to identify child pornography and other illegal materials.[125] Hash functions are one-way functions that process data to produce a condensed representation called a

---

118. Sarah D. Scalet, *19 Ways To Build Physical Security into a Data Center*, CIO (Mar. 8, 2006, 4:06 PM), http://www.cio.com.au/article/181324/19_ways_build_physical_security_into_data_centre/; *see* SANS INST. READING ROOM, REQUIREMENTS FOR THE DESIGN OF A SECURE DATA CENTER (2002) [hereinafter SANS INST. WHITE PAPERS], https://www.sans.org/reading-room/whitepapers/recovery/requirements-design-secure-data-center-561;

119. *See* NATIONAL SECURITY AGENCY, DEFENSE IN DEPTH, https://www.nsa.gov/ia/_files/support/defenseindepth.pdf (last visited Apr. 3, 2016); Chad Perrin, *Understanding Layered Security and Defense in Depth*, TECHREPUBLIC (Dec. 18, 2008, 6:05 AM), http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/.

120. *See Understanding Security in the Virtualized IT Data Center*, JUNIPER NETWORKS, http://www.juniper.net/techpubs/en_US/release-independent/solutions/topics/concept/security-virtual-it-dc-overview.html (last modified May 18, 2015).

121. *Security Now!: Listener Feedback 217* (Gibson Research Corporation podcast Aug. 25, 2015) (transcript at 16), https://www.grc.com/sn/sn-522.pdf.

122. *Id.* ("[F]or me to get to my servers at Level 3 I have a coded inductive badge, which I have to present to a reader. My right hand is biometrically measured, so there's biometrics. I have to enter a PIN. So I've got something I have, something I am, and something I know. And that gets me into the front door. Then there's conspicuous cameras everywhere, and I have to use a combination lock in order to access my servers.").

123. *See* Jack Schofield, *Is Gmail Secure Enough for My Private E-mails?*, GUARDIAN (Aug. 15, 2013, 10:39 AM), https://www.theguardian.com/technology/askjack/2013/aug/15/gmail-google-email-privacy.

124. *Id.*

125. Sean Gallagher, *Updated: How Verizon Found Child Pornography in Its Cloud*, ARS TECHNICA (Mar. 5, 2013, 10:51 AM), http://arstechnica.com/civis/viewtopic.php?f=2&t=1196577&start=80; Lisa Vaas, *Microsoft Scans E-mail for Child Abuse Images, Leads to*

hash value. In the context of cryptography, the data is called the *message*, while the hash value is called the *message digest*.[126] Hash functions are essentially mathematical functions used to "fingerprint" files without actually examining the file in the traditional sense.[127] Just like fingerprints cannot be used to identify a suspect unless the suspect's fingerprint is already in a database, the examiner is not able to discern anything about the content of the file without an independent record that generates an identical hash.[128] The message digest does not reveal any information about the file other than that it matches the message digest of an identical file if the examiner has an independent record of that identical file.[129]

Hash functions share this characteristic with fingerprints, and they are therefore useful in this manner because of the "extremely low probability that two different . . . messages will yield the same hash value."[130] Any small change in the data will, "with a very high probability, result in a different message digest."[131] For example, "The quick brown fox jumps over the lazy dog" generates the Secure Hash Algorithm 1 (SHA-1) message digest of: "0x 2fd4 e1c6 7a2d 28fc ed84 9ee1 bb76 e739 1b93 eb12," whereas "the quick brown fox jumps over the lazy dog" (with a lowercase t) generates the message digest

---

Arrest, NAKED SECURITY (SOPHOS) (Aug. 10, 2014), https://nakedsecurity.sophos.com/2014/08/10/microsoft-scans-email-for-child-porn-images-leads-to-arrest%E2%80%8F/.

126. *See* U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., FIPS PUB 180-4, SECURE HASH STANDARD (SHS), at iv (Mar. 2012) [hereinafter SHS REPORT], http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

127. Greg Kumparak, *How Dropbox Knows When You're Sharing Copyrighted Stuff (Without Actually Looking at Your Stuff)*, TECHCRUNCH (Mar. 30, 2014), http://techcrunch.com/2014/03/30/how-dropbox-knows-when-youre-sharing-copyrighted-stuff-without-actually-looking-at-your-stuff/.

128. Similar to fingerprints, the message digest itself, generated by a hash function, does not identify the file without an *independent* record of the file. *Id.* ("It might help to think of a hash like a fingerprint. Everyone's fingerprint is unique, but it can't be used to identify a person unless you already have a record of that person's fingerprint to compare it to.").

129. *Id.*

130. Stephen Northcutt, *Hash Functions*, SANS TECH. INST., http://www.sans.edu/research/security-laboratory/article/hash-functions (last visited Feb. 6, 2015).

131. SHS REPORT, *supra* note 126, at 3. Efforts are always underway to stay ahead of increasing computational power to generate collisions or predictably generating files with different content but the same signature. *See, e.g.*, MSRC Team, *Microsoft Releases Security Advisory 2718704*, TECHNET BLOG: MICROSOFT SECURITY RESPONSE CTR (June 3, 2012, 5:41 PM), https://blogs.technet.microsoft.com/msrc/2012/06/03/microsoft-releases-security-advisory-2718704/; *see also When Will We See Collisions for SHA-1?*, SCHNEIER ON SECURITY (Oct. 5, 2012, 1:24 PM), https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html (reporting on estimates of when a practical collision attack will be developed; a collision attack is an attempt to predictably find two different messages that generate the same message digest). And, the information security industry continues to deprecate, or replace, older standards. *See* Bruce Morton, *SHA-1 Deprecation, on to SHA-2*, ENTRUST IDENTITYON: BLOG (Dec. 9, 2013), https://www.entrust.com/sha-1-deprecation-on-to-sha-2/.

of: "0x 1631 2751 ef93 07c3 fd1a fbcb 993c dc80 464b a0f1."[132] "No other file will have the same hash value . . . , except a file that is identical, bit-for-bit. If one altered [the file] by changing so little as one bit, the hash value of [the file] would be different as well."[133] A hash function message digest alone can identify the file, but cannot be used to recreate what is in the file.[134]

Due to the disconnect between the technical and legal protections, and in the wake of the Snowden revelations of government mass surveillance activities, consumers have demanded more information security protections,[135] and the information technology industry responded by enabling encryption by default in more services.[136] Google, Microsoft, and Yahoo all have implemented plans for e-mail encryption in transit.[137] However, this does not protect the message from being read by the service providers themselves. Service providers do sometimes "read" consumers' e-mails, for example, in response to court orders or to investigate internal leaks of intellectual property and trade secrets.[138] However, many service providers deploy strong encryption that makes it impossible, even for the service providers, to decrypt the encrypted information.[139]

"Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its

---

132. *See* WOLFRAM ALPHA, https://www.wolframalpha.com (enter "SHA 'The quick brown fox jumps over the lazy dog,'" and "SHA 'the quick brown fox jumps over the lazy dog'") (last visited Feb. 2, 2016).

133. Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 39 (2006).

134. *Id.* at 42. A properly designed hashing algorithm for computer forensics purposes exhibit two important properties. *Id.* at 39. "First, the hash value will be, for all practical purposes, uniquely associated with the input." *Id.* The probability that two different inputs will result in the same output, or "collide," must be astronomically small. *Id.* Second, the algorithm must be a "one-way function"; that is, "[o]ne can calculate a hash value from input, but cannot derive the input from the hash value." *Id.* at 40.

135. The revelations triggered a "growing public concern for privacy," and the public adopted techniques to "shield their movements online." Lauren C. Williams, *More People Are Encrypting Their Web Traffic in the Wake of NSA Spying Revelations*, THINKPROGRESS (May 17, 2014, 1:02 PM), http://thinkprogress.org/world/2014/05/17/3438919/more-people-turn-to-encryption-after-snowden-leaks/.

136. *See* Amit Chowdhry, *Microsoft Opens Transparency Center and Enhances Encryption for Webmail Services*, FORBES (July 1, 2014, 3:44 PM), http://www.forbes.com/sites/amitchowdhry/2014/07/01/microsoft-opens-transparency-center-and-enhances-encryption-for-webmail-services/#617ca78882ea.

137. *Id.*

138. Zach Miners, *Worried About the Government? Internet Giants Also Dip Their Hands in the Cookie Jar*, PCWORLD (Mar. 21, 2014, 4:10 PM), http://www.pcworld.com/article/2110900/worried-about-the-government-internet-giants-also-dip-their-hands-in-the-cookie-jar.html.

139. *See Secure Messaging Scorecard*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/secure-messaging-scorecard (last visited Dec. 20, 2015).

original form, called plaintext."[140] For example, in Apple's iMessage implementation, "[y]ou send a text message that's encrypted on your device. It passes through Apple servers as jumbled code nobody can crack. And it can only get decrypted by your friend's [device]."[141] Apple and Google have announced plans to encrypt text messages by default.[142] This led FBI Director James Comey to opine that the technology is beyond law enforcement's capabilities to bypass in an emergency.[143] Encryption is designed to make it computationally difficult to derive the original plaintext from the resulting ciphertext without the correct encryption key.[144] For example, the Advanced Encryption Standard (AES), selected by NIST in 2001, puts the plaintext through rounds of the algorithm with each round being dependent on the previous round, resulting in ciphertext that is computationally infeasible to revert to the plaintext.[145]

Encryption is a powerful tool in cryptography that cannot be easily bypassed.[146] For example, assuming there is no unknown built-in weakness or backdoors, "a brute-force attack on a message encrypted with 256-bit AES would take even a supercomputer longer to break than the universe has been in existence."[147] Although the specific implementations can have weaknesses and theoretical attacks exist, the

---

140. U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., FIPS PUB 197, ADVANCED ENCRYPTION STANDARD (AES), at i (Nov. 26, 2011) [hereinafter AES REPORT], http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

141. Jose Pagliery, *FBI Director: iPhones Shields Pedophiles from Cops*, CNN MONEY (Oct. 14, 2014, 10:17 AM), http://money.cnn.com/2014/10/13/technology/security/fbi-apple/.

142. *Id.*

143. *Id.*

144. AES REPORT, *supra* note 140, at i.

145. *Id. See generally What Is Encryption?*, SURVEILLANCE SELF-DEFENSE, https://ssd.eff.org/en/module/what-encryption (last updated Nov. 3, 2014) (providing more information regarding encryption). Although the terms used to describe cryptographic schemes employ the suffix of "text" (e.g., cipher*text* and plain*text*), the techniques are applicable to any data regardless of whether the data represents an e-mail, a photograph, a document, a video, or a phone call because the encryption works on the underlying data and not what is displayed to the user. *See* Daniel J. Sherwinter, Note, *Surveillance's Slippery Slope: Using Encryption To Recapture Privacy Rights*, 5 J. TELECOMM. & HIGH TECH. L. 501, 513–14 (2007). See CAREY PARKER, FIREWALLS DON'T STOP DRAGONS: A STEP-BY-STEP GUIDE TO COMPUTER SECURITY FOR NON-TECHIES 39–49 (2015), for a brief history of cryptography.

146. Steven J. Vaughan-Nichols, *Has the NSA Broken SSL? TLS? AES?*, ZDNET (Sept. 6, 2013, 1:17 PM), http://www.zdnet.com/article/has-the-nsa-broken-ssl-tls-aes/.

147. *Id.* Mohit Arora, *How Secure Is AES Against Brute Force Attacks?*, EE TIMES (May 7, 2012, 05:29 PM), http://www.eetimes.com/document.asp?doc_id=1279619 ("The key length used in the encryption determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. Brute-force attack involves systematically checking all possible key combinations until the correct key is found and is one way to attack when it is not possible to take advantage of other weaknesses in an encryption system.").

underlying cryptography is sound; thus, encrypted data cannot be decrypted without the encryption key.[148] This is commonly called "strong encryption."

Although encryption does not always make it impossible for law enforcement or intelligence agencies to access someone's data, encryption does make it much more difficult and time consuming to do so.[149] In fact, it is practically impossible to do this if the one who holds the encryption key (assuming it is a strong key) does not cooperate.[150] If information is encrypted, law enforcement can no longer access the information "secretly by going to Apple or Google."[151] Instead, law enforcement "must knock on your front door with a warrant in hand" in the same way that other searches of information that is protected are conducted pursuant to the Fourth Amendment.[152] For example, "if you don't give the FBI access to your phone, it can ask a federal judge to force you. If you refuse, the government can throw you in jail and hold you in contempt of court."[153] However, if the encryption key is not divulged, it is practically impossible to access that information.[154]

Courts are currently divided on whether defendants can be compelled by a court order to divulge the encryption key without violating the defendant's Fifth Amendment rights.[155] These uncertainties further complicate the analysis under both the Fourth Amendment and the SCA. The U.S. Supreme Court recognized these complications in *Riley*.[156]

---

148. Jennifer Seberry, *World's Toughest Encryption Scheme Found 'Vulnerable*,' PHYS.ORG (Aug. 23, 2011), http://phys.org/news/2011-08-world-toughest-encryption-scheme-vulnerable.html ("Academics say an algorithm is 'broken' if it has a 'certification weakness.' Simply, an encryption implementation is said to have a certification weakness if the content of the encrypted message can be read in less time than it would take to try every possible key.") This does not mean that the algorithm is no longer safe to use. Rather, "plenty of further study is needed before we are even close to thinking AES implementations are insecure." *Id.*

149. Pagliery, *supra* note 141.

150. *See id.*

151. *See id.*

152. *See id.*

153. *Id.*

154. *See id.*

155. *See, e.g.*, *In re* Boucher, No. 2:06–MJ–91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009) (reasoning that because the government knew of the existence and location of the files, providing the government access to the unencrypted form of those files added nothing to the government's information). *But see In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1352 (11th Cir. 2012) (holding that compelling the defendant to decrypt the drives would be testimonial and violate the defendant's Fifth Amendment right against self incrimination).

156. 134 S. Ct. 2473 (2014).

D. Riley v. California, *the U.S. Supreme Court Recognizes the Blurred Line Between Local and Remote Storage*

In *Riley* the U.S. Supreme Court refused to allow warrantless searches of cell phones incident to arrest.[157] These searches could have been a simple extension of the Fourth Amendment exception long enjoyed by law enforcement incident to arrest, but the Court drew the line at cell phones.[158] However, *Riley* "does not address the broader question of whether information stored in the cloud is entitled to Fourth Amendment protection in other contexts."[159]

The Court recognized complications brought by the complex interactions of mobile devices and the expansiveness of, and social reliance on, data stored in the cloud, noting:

> Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing." Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.[160]

Riley did not "address[ ] how the third-party doctrine applies to digital data," that is, whether the consumer waives Fourth Amendment protection by giving the information to a service provider.[161] Therefore, *Riley* did "little to clarify how the third-party doctrine applies to information stored in the cloud in other contexts, leaving open the question of whether police can acquire cloud-based information from third parties who host the cloud servers."[162] However, *Riley* showed the Court's recognition of the difficulties that both the consumer and the courts face in assessing information that enjoys a reasonable expectation of privacy in ESI. These difficulties are the result of the disconnect between the current Fourth Amendment jurisprudence, SCA protection, the state of information technology, and consumer expectations.

---

157. *Id.* at 2494–95; Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, 2013–2014 CATO SUP. CT. REV. 307, 308.

158. Pincus, *supra* note 157, at 308.

159. Ryan Watzel, Riley*'s Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73, 73 (2014).

160. *Riley*, 134 S. Ct. at 2491 (citation omitted).

161. Watzel, *supra* note 159, at 75.

162. *Id.* at 76.

III. Analysis

Riley suggested that the U.S. Supreme Court is willing to extend Fourth Amendment protection to the cloud, which is increasingly used in the same way that local storage is used on hardware directly controlled by consumers.[163] The SCA is outdated and must be updated to reflect modern expectations of privacy because electronic communication has been widely adopted and has become unavoidable in modern society.[164] In addition, information stored with a service provider should not be considered "disclosed" to a third-party.[165] Today, consumers subjectively retain an expectation of privacy in their data stored with a service provider. If legal protection is not clarified to alleviate consumer anxieties about mass surveillance and warrantless searches, uncertainties surrounding Fourth Amendment protection of consumer information will lead to mass adoption of encryption. The decades-old SCA no longer conforms to consumer expectations of privacy and the omnipresence of ESI; ESI should enjoy the same treatment as the other forms of communication and the storage that it is rapidly replacing. This Comment presents three reasons why the SCA is outdated.

First, it is now virtually impossible to conduct business without using e-mail or other electronic communication mediums and storing information with service providers.[166] Consequently, consumers are forced to expose their information to service providers.[167] Second, the differentiation between local and remote storage is blurring.[168] Many of the major service providers design their products and services to be dependent on the "cloud" and to provide a seamless experience for the consumer that purposely blurs local and remote resources.[169] Finally, the average consumer does not often delete e-mails within 180 days. In fact, many consumers never delete e-mails because the space allocated by popular e-mail services far exceeds the space required by

163. Although the hardware is controlled by service providers, consumers store their information on that hardware through cloud-based services. *Id.* at 79.

164. *See* Press Release, Leahy, Lee Introduce Legislation To Update Electronic Communications Privacy Act (Mar. 19, 2013) [hereinafter Press Release, Leahy and Lee Introduce Legislation], https://www.leahy.senate.gov/press/leahy-lee-introduce-legislation-to-update-electronic-communications-privacy-act.

165. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551 (2005).

166. *See infra* notes 171–88 (discussing normalities of stored communication).

167. *See infra* notes 171–88.

168. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2491 (2014); *see supra* notes 157–62.

169. *Riley*, 134 S. Ct. at 2491.

the average consumer.[170] Therefore, Congress must amend the SCA to recognize Fourth Amendment protection for ESI, eliminate the arbitrary 180-day rule and distinction between storage and communication, uphold search warrant requirements despite the third-party doctrine, and rebuild the trust between law enforcement and the people of the United States.

A. Stored Communications Is Unavoidable in Everyday Life

Internet adoption has gone from 14% in 1995 to nearly 80% in 2009, and, in 2013, 98% of U.S. households had access to broadband Internet.[171] Companies that have utilized Amazon's cloud service, AWS, include Comcast, Novartis, Pfizer, Bristol-Myers Squibb, Dow Jones, and even government entities like the CDC, the FDA, and NASA.[172] Because the Internet is so important to everyday life, many states offer low-cost, high-speed Internet access assistance to low-income households, which include those on "Medicaid, Food Stamps, SSI, home energy assistance or public housing assistance."[173] In fact, Internet access for communication and information is so essential to modern life that in 2012, "a federal court . . . struck down a Louisiana statute that banned sex offenders from using social network websites because the statutory definition of 'social networking' was overbroad, potentially extending to cover 'many commonly read news and information websites.'"[174]

Telephone services traditionally enjoyed very high protections despite the users arguably exposing conversations to the third-party service providers.[175] But, consumers are increasingly abandoning

170. Matt Warman, *One in Ten 'Never Delete E-mail,'* TELEGRAPH (Mar. 15, 2012, 7:00 AM), http://www.telegraph.co.uk/technology/news/9144134/One-in-ten-never-delete-e-mail.html.

171. Edward Wyatt, *Most of U.S. Is Wired, but Millions Aren't Plugged In*, N.Y. TIMES, Aug. 18, 2013, http://www.nytimes.com/2013/08/19/technology/a-push-to-connect-millions-who-live-offline-to-the-Internet.

172. *All AWS Customer Stories*, *supra* note 110.

173. Jim T. Miller, *How To Get Cheap or Free Internet Access at Home*, HUFFINGTON POST (Dec. 2, 2013, 6:08 PM), http://www.huffingtonpost.com/jim-t-miller/how-to-get-cheap-or-free-_b_4368774.html.

174. Benjamin F. Jackson, *Censorship and Freedom of Expression in the Age of Facebook*, 44 N.M. L. REV. 121, 160 n.193 (2014) (quoting Doe v. Jindal, 853 F. Supp. 2d 596, 604 (M.D. La. 2012)).

175. *See, e.g.*, Katz v. United States, 389 U.S. 347, 359 (1967) ("These considerations do not vanish when the search in question is transferred . . . to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."). *But see* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information [she] voluntarily turns over to third parties."). The information at issue in *Smith* was metadata—specifically call records, not the contents of the conversation—as service provider business records. *Id.* at 743

traditional telephone services in favor of services provided by ISPs, and "[a]t current rates the last landline in America will be disconnected sometime in 2025."[176]

Consumers are increasingly dependent on network storage.[177] A projected one-third of consumer digital content will be in the cloud by 2016.[178] According to the *Cisco Global Cloud Index: Forecast and Methodology, 2014–2019*, "global cloud IP traffic will reach 8.6 ZB [per year] (719 EB per month) by the end of 2019, up from 2.1 ZB per year (1176 EB per month) in 2014."[179] "Global cloud IP traffic will account for more than four-fifths (83%) of total data center traffic by 2019."[180] In addition, "[b]y 2019, 55 percent (2 billion) of the consumer Internet population will use personal cloud storage, up from 42 percent (1.1 billion users) in 2014." Further, "consumer cloud storage traffic per user will be 1.6 Gigabytes per month by 2019, compared to 992 megabytes per month in 2014."[181] In other words, by 2019, the majority of consumers will use some form of cloud storage, and the vast majority of Internet traffic will be used to support the infrastructure making that possible.

Some legislators have recognized this issue, and "[Democratic] Senator Patrick Leahy (D-VT) and [Republican] Senator Mike Lee (R-UT) introduced a bipartisan bill . . . to reform the Electronic Communications Privacy Act (ECPA) that would grant new privacy protections for email and other cloud stored data."[182] Organizations have also formed coalitions around this issue to ensure Fourth Amendment

("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").

176. JULIE SIEBENS, U.S CENSUS BUREAU, P70-136, EXTENDED MEASURES OF WELL-BEING: LIVING CONDITIONS IN THE UNITED STATES: 2011, at 11 (Sept. 2013), http://www.census.gov/prod/2013pubs/p70-136.pdf ("Although landlines were nearly universal in 1998 at 96 percent, by 2011 the percentage of householders with a landline dropped to 71 percent. During this same time, the number of householders with access to only a landline (no cellular phone) dropped much more. Six out of 10 householders had a landline only in 1998, but by 2011 this proportion fell to 1 out of 10."); *The Decline of the Landline: Unwired*, ECONOMIST (Aug. 13, 2009), http://www.economist.com/node/14213965.

177. *See* Peterson, *supra* note 89. Information stored on remote servers is, therefore, far from "abandoned garbage on the curb" as envisioned by the original drafters of the SCA. *See id.*

178. Press Release, Gartner Says That Consumers Will Store More than a Third of Their Digital Content in the Cloud by 2016 (June 25, 2012), http://www.gartner.com/newsroom/id/2060215.

179. CISCO, CISCO GLOBAL CLOUD INDEX: FORECAST AND METHODOLOGY, 2014–2019, at 12 (2015), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.

180. *Id.*

181. *Id.*

182. Peterson, *supra* note 89.

protections for Internet communications; the coalitions include the American Civil Liberties Union, Heritage Action for America, Americans for Tax Reform, the Center for Democracy and Technology, and "[p]rivacy advocates, trade associations, think tanks, legal scholars, start-ups, and major Internet and communications companies."[183]

Senator Leahy, one of the authors of the original 1986 legislation, sponsored the proposed amendment to the SCA[184] and stressed: "No one could have imagined just how the Internet and mobile technologies would transform how we communicate and exchange information today."[185] Senator Leahy also stated:

> "Privacy laws written in an analog era are no longer suited for privacy threats we face in a digital world. Three decades later, we must update this law to reflect new privacy concerns and new technological realities, so that our Federal privacy laws keep pace with American innovation and the changing mission of our law enforcement agencies."[186]

In the midst of these uncertainties over legal protections, Americans are increasingly interested in technological solutions that enable them to take matters into their own hands; thus, the information security field has enthusiastically supplied both the knowledge and the technology. In the wake of the Snowden revelations, the Electronic Frontiers Foundation (EFF) relaunched its "Surveillance Self-Defense" guide with the goal of "provid[ing] information on how to use technology more safely," including tutorials on how to encrypt devices

---

183. *About the Issue*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Feb. 6, 2014); *see also About Us*, DIGITAL 4TH (2016), http://www.digital4th.org/about-us.php.

184. A nearly identical bill, The Electronic Communications Privacy Act Amendments Act of 2015, was introduced in 2015. S. 356, 114th Cong. (as reported by S. Comm. on the Judiciary, Sept. 16, 2015); Press Release, Leahy Joined by Bipartisan, Bicameral Group To Introduce Bill Protecting Online Privacy (Feb. 4, 2015), http://www.leahy.senate.gov/press/leahy-joined-by-bipartisan-bicameral-group-to-introduce-bill-protecting-online-privacy. In April, 2016, the House Judiciary Committee approved the similar Email Privacy Act; the bill is sponsored by 315 of the 435 representatives but is expected to land in a gridlocked Senate. Dustin Volz, *Long-Stalled Email Privacy Bill Advances in Congress*, REUTERS (Apr. 13, 2016, 5:25 PM), http://www.reuters.com/article/us-usa-cyber-emails-idUSKCN0XA1VK.

185. Press Release, Leahy and Lee Introduce Legislation, *supra* note 164 (quoting Sen. Patrick Leahy).

186. *Id.* (quoting Sen. Mike Lee). Senator Leahy explained: "At the time that Congress enacted ECPA . . ., Congress assumed that most Americans would periodically access their email accounts and download any emails that they wished to read, and that third-party service providers would subsequently delete any email stored on their servers." S. REP. NO. 113-34, at 2 (2013). However, technological advances have changed the way that consumers access their e-mails and other stored communications. *Id.* Senator Leahy further stated: "The digital privacy protections that the Congress put in place by enacting ECPA have not kept pace with these changes." *Id.*

and communications.[187] In fact, information security is so important to modern consumers that a 2014 Gallup poll found that Americans worry more often about being hacked than being murdered.[188] As these systems rapidly replace traditional forms of storage and communication, the legal protections for ESI need to reflect how consumers actually view the relationship between themselves, their data, and third parties like service providers.

B. Information Stored with, or Transported by, a Third Party Is Not "Disclosed" to the Third Party

The third-party doctrine provides that Fourth Amendment protection is relinquished for information disclosed to a third party.[189] Service providers scan traffic, for example, to identify spam and mine information for advertisers[190] or use hash values (often simply called hashes) to identify illegal materials by matching the hash values to known illegal materials.[191] However, Fourth Amendment jurisprudence does not consider hash matching a search by a human examiner; therefore hash matching should not constitute disclosure to a third party.[192] Hash matching is used to quickly and accurately ensure that seized illegal materials match previously generated records of identical illegal materials without the need for a human examiner.[193] Automatic traffic scanning does not involve a human actually reading the contents of the message; therefore, it should not implicate the third-party doctrine or negate Fourth Amendment privacy expectations in electronic communications at all.

Hash matching is similar to the use of narcotics sniffing dogs, and the U.S. Supreme Court has held that the use of narcotics sniffing

187. Jillian York, *EFF Relaunches Surveillance Self-Defense*, ELECTRONIC FRONTIER FOUND. (Oct. 23, 2014), https://www.eff.org/deeplinks/2014/10/eff-relaunches-surveillance-self-defense ("In the time since the Snowden revelations, we've learned a lot about the threats faced by individuals and organizations all over the world—threats to privacy, security, and free expression. And there is still plenty that we don't know. In creating the new [Surveillance Self-Defense guide], we seek to help users of technology understand for themselves the threats they face and use technology to fight back against them. These resources are intended to inspire better-informed conversations and decision-making about digital security in privacy, resulting in a stronger uptake of best practices, and the spread of vital awareness among our many constituents.").

188. Rebecca Riffkin, *Hacking Tops List of Crimes Americans Worry About Most*, GALLUP (Oct. 27, 2014), http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx.

189. Kerr, *supra* note 7, at 563.

190. Schofield, *supra* note 123.

191. Gallagher, *supra* note 125; Vaas, *supra* note 125.

192. *See* Salgado, *supra* note 133, at 42–43.

193. *See id.* at 43.

dogs is not a search because only contraband would generate a hit.[194] "The analogous argument for hashing runs as follows: there is no legitimate expectation of privacy in the possession of contraband; government conduct that reveals only the presence of contraband compromises no legitimate interests; a hash value search will only reveal the presence or absence of child pornography files."[195] In addition, as discussed *supra*, hash matching is inherently different from directly reading the materials because the examiner can only identify a match if he has an independent record of the original.[196]

Some commentators have argued that a hash is not analogous to a narcotics sniffing dog because the information is exposed to the government during processing.[197] However, this argument is based on the premise that the processing of the files is a search.[198] "[A] search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer."[199]

In *In re Warrant To Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*,[200] a U.S. district court held that a war-

194. Alexandra L. Mitter, *Deputizing Internet Service Providers: How the Government Avoids Fourth Amendment Protections*, 67 N.Y.U. ANN. SURV. AM. L. 235, 259–60 (2011) (discussing Illinois v. Caballes, 543 U.S. 405 (2005); United States v. Place, 462 U.S. 696 (1983)). "[The Court] held that narcotics-sniffing dogs could be used without implicating the Fourth Amendment, because the dogs can only detect the presence or absence of contraband." *Id.*

195. *Id.* at 259.

196. *See supra* notes 125–38 and accompanying text.

197. *See, e.g.*, Kerr, *supra* note 165, at 547–48 ("[R]ules for looking through a computer should be governed by the Fourth Amendment's prohibitions on searches, and specifically by what I term an 'exposure-based approach' to searches. Under this approach, a search of data stored on a hard drive occurs when that data, or information about that data, is exposed to human observation. Any observable retrieval of information stored on a computer hard drive, no matter how minor, should be considered a distinct Fourth Amendment search."); Mitter, *supra* note 194, at 260 ("While, like a drug-sniffing dog, child pornography hash values are designed to detect only contraband, the manner in which searches of Internet activity are carried out is fundamentally different. In running a hash, private electronic files must be opened, accessed, and copied, unlike a dog sniff that can permeate a closed suitcase or car trunk. . . . While hashing is designed to reveal only contraband files, the investigator running the hash program, unlike a trained canine, must copy and access each file in order to derive its unique hash value, even those in which a reasonable expectation of privacy remains, a process that could potentially reveal information about non-contraband files." (footnotes omitted)).

198. Mitter, *supra* note 194, at 260.

199. Kerr, *supra* note 165, at 551.

200. 15 F. Supp. 3d 466 (S.D.N.Y. 2014) *rev'd*, No. 14-2985, 2016 WL3770056 (2d Cir. July 14, 2016) [hereinafter *Warrant To Search Microsoft E-mail Accounts*]. The Second Circuit noted that "[t]here decades ago, international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st-century demands for access and speed and their related, evolving expectations of privacy." *Id.* at 6. Concurring in a seperate opinion, Judge Gerard E. Lynch emphasized the need for Congress to amend the "badly outdated" SCA. *Id.* (Lynch, J., concurring).

rant to search data stored in Microsoft's data centers in Ireland through Microsoft's Global Criminal Compliance Department located in the United States did "not implicate principles of extraterritoriality" because "no such exposure takes place until the information is reviewed in the United States, and, consequently, no extraterritorial search has occurred."[201] Therefore, the data stored with a third party is not exposed to that third party if the information is automatically processed by a computer.[202] However, none of these techniques will work to identify illegal materials protected by strong encryption.[203]

If Congress enacts clear legal protections for ESI that adhere to the consumers' expectations of privacy despite the third-party doctrine, consumers will be less likely to adopt strong encryption and less concerned about trusting domestic companies with their data. Further, law enforcement will maintain access to the information they need in emergencies.

C. The SCA Does Not Conform to Modern Expectations of Privacy

The decades-old SCA no longer conforms to modern expectations of privacy because consumers do not use service provider controlled hardware in the same manner as they did when the SCA was enacted. Service providers control the hardware and services that store consumer data and regularly analyze that data with automated processes.[204] Nevertheless, consumers who are aware of what service providers do with their data believe that they have an expectation of privacy in that data.[205] In an opinion piece for the *Wall Street Journal*, Brad Smith, General Counsel and Executive Vice President for legal

201. *Id.* at 472.

202. *See* Kumparak, *supra* note 127.

203. Encryption obfuscates plaintext into ciphertext. Without breaking open the encryption, an eavesdropper is unable to obtain the plaintext from the ciphertext. *See generally Inspection of SSL Traffic Overview*, JUNIPER NETWORKS (Jan. 12, 2010), https://www.juniper.net/techpubs/en_US/idp5.0/topics/concept/intrusion-detection-prevention-ssl-decryption-overview.html (describing the cryptographic protocol). A hash value calculated from the ciphertext would be different from a hash value calculated from the plaintext. The same plaintext will generate different ciphertexts if the keys are different. *See Generating a Key from a Password*, MICROSOFT DEVELOPER: .NET SECURITY BLOG (Apr. 14, 2004), https://blogs.msdn.microsoft.com/shawnfa/2004/04/14/generating-a-key-from-a-password/. Even two users who use the same password will almost always have different keys because a properly designed cryptosystem does not simply use the password as the key, but derives a key from the password by incorporating a salt, iteration count, and other sources of entropy. *See id.* By design, encryption makes it computationally infeasible to obtain any information from the ciphertext without the key.

204. *See, e.g.*, Kumparak, *supra* note 127.

205. Brad Smith, *We're Fighting the Feds over Your E-mail*, WALL ST. J., July 29, 2014, http://online.wsj.com/articles/brad-smith-were-fighting-the-feds-over-your-email-1406674616.

and corporate affairs at Microsoft, stated that Microsoft is fighting the ruling in *Warrant To Search Microsoft E-mail Accounts.* [206] Smith further stated that Microsoft believes their consumers "own emails stored in the cloud, and that they have the same privacy protection as paper letters sent by mail. This means . . . that the U.S. government can obtain emails only subject to the full legal protections of the Constitution's Fourth Amendment."[207] Microsoft commissioned a survey that found "86% [of American voters] believe police should have to follow the same legal requirements for obtaining personal information stored in the cloud as they do for personal information stored on paper."[208]

At least "28 media and technology companies, 23 trade associations, and 35 computer scientists signed on to amicus briefs supporting [Microsoft's] court case."[209] Smith also discussed court cases recognizing the need for a warrant to search shipping packages, safe deposit boxes, hotel room drawers, and to listen in on telephone calls.[210] "Courts have long recognized the distinction between a company's business records and an individual's personal communications."[211]

The distinction is between the information the business must use to provide services to the consumer and "what a consumer put inside" those services.[212] For example, information that shows where a customer shipped packages is generally considered a business record because the customer expects that the shipping company needs that information to deliver the package.[213] However, the contents of that package are protected, and, generally, the government must "establish probable cause and get a warrant" to look inside the package.[214]

---

206. *Id.*

207. *Id.*

208. Brad Smith, *Digital Common Sense: New Survey Shows Americans Want a Better Privacy Balance*, DIGITAL CONSTITUTION: BLOG (July 16, 2014), http://digitalconstitution.com/2014/07/digital-common-sense-new-survey-shows-americans-want-better-privacy-balance/.

209. Matt Day, *Amazon, HP, eBay Join Microsoft Bandwagon in Warrant Case*, SEATTLE TIMES (Dec. 15, 2014, 9:50 AM), http://blogs.seattletimes.com/microsoftpri0/2014/12/15/amazon-hp-ebay-join-microsoft-bandwagon-in-warrant-case/.

210. Smith, *supra* note 205.

211. *Id.*

212. *Id.*

213. *Id.*

214. *Id.*

> Similarly, the government can use a subpoena to obtain bank records that show when a customer accessed a safe-deposit box, but it needs a warrant to search the private papers kept inside. It may subpoena the business records containing a hotel's guest registry, but it cannot take the diary in a guest's hotel-room drawer except through a legal search and seizure.

Id.

"[U]nder current rules for telephone calls, the government can more readily obtain the metadata contained in company records about who called what phone numbers and when than it can listen to an individual's conversations."[215] Similarly, service providers need to ascertain certain information to process stored communications, but the contents need not to be "read" by the service provider for the customer to utilize those services. Although the information security community generally accepts the notion that sender and receiver metadata is extremely difficult to completely obfuscate in the current electronic communication infrastructure, the contents of the stored communication can be easily encrypted.[216]

"Another potential argument against requiring a warrant before the government may request ISP monitoring of their subscribers' Internet activity focuses on the privacy policy that every user must agree to before accessing their Internet services."[217] Nevertheless, the consumer's subjective intentions remain essential; a consumer does not send an e-mail intending for the ISP to intercept it, but, rather, the consumer intends to have the ISP transmit the e-mail to the recipient.[218] This markedly differs from, for example, "[a] child who reveals to a teacher that her parents abuse her"; in such an instance, the child "loses any reasonable expectation of privacy by sharing the information with another."[219] The intended recipient in that scenario is the teacher. Consequently, "[t]his differs from the communication between two private actors intercepted by an ISP, because the information was never intentionally shared with the ISP."[220] Instead, the subjective intention of the sender is for the ISP to transmit the information to the recipient, which is much like sending a letter—one does not send a letter intending that the U.S. Postal Service will read the letter.

At a House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations hearing in 2013, Elana Tyrangiel, Acting Assistant Attorney General in the Office of Legal Policy at the U.S.

---

215. *Id.*

216. *See Security Now!: Tor: Not So Anonymous* (Gibson Research Corporation podcast Feb. 3, 2015) (transcript at 10–12), https://www.grc.com/sn/sn-493.pdf.

217. Mitter, *supra* note 194, at 263. "Where the consenting party has no reasonable alternatives or choices relating to a particular term among different contractual providers, courts' reliance on a consumer's ability to find a better offer seems misplaced." *Id.* at 264. *But see id.* ("Compared to the variety of *e-mail providers*, there is relatively little choice between *Internet providers*. Therefore, a customer is limited in his or her ability to shop around to find the privacy policy that best suits his or her needs." (emphasis added)).

218. *Id.* at 273–74.

219. *Id.* at 274.

220. *Id.*

Department of Justice, echoed the widely held view that the SCA has "failed to keep up with the development of technology and the ways in which we use electronic and stored communications."[221] Specifically, the Office of Legal Policy agreed "that there is no principal basis to treat e-mail less than 180 days old differently than e-mail more than 180 days old" or treat unopened e-mails differently from opened e-mails.[222] The testimony emphasized that "[a]ll of us use e-mail and other technologies to share personal and private information, and we want it to be protected appropriately."[223]

The SCA was enacted to provide some Fourth Amendment-like protection for information disclosed to service providers.[224] However, the SCA no longer conforms with the average consumer's expectations of privacy.[225] This is evident from the type of information consumers store with third parties[226] and the public's reaction to the Snowden Revelations. Edward Snowden, an ex-National Security Agency (NSA) contractor, disclosed the NSA's mass surveillance programs that collected a high proportion of telephone and Internet data on U.S. citizens and residents, which far outnumbered data on legally targeted foreign surveillance targets.[227] In light of the Snowden reve-

221. *ECPA (Part I): Lawful Access to Stored Content: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary*. 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, U.S. Department of Justice).

222. *Id.* (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, U.S. Department of Justice).

223. *Id.* (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, U.S. Department of Justice).

224. Kerr, *supra* note 11, at 1212 ("The SCA addresses this imbalance by offering network account holders a range of statutory privacy rights against access to stored account information held by network service providers. The statute creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information.").

225. *See* Kim Zetter, *What We Know About the NSA and AT&T's Spying Pact*, WIRED (Aug. 17, 2015, 5:57 PM), http://www.wired.com/2015/08/know-nsa-atts-spying-pact/ ("In the last two years, revelations exposing the breadth of the NSA's surveillance, as well as the cooperation of technology companies in helping the NSA spy, have forced the agency to curtail some of its activity. Some companies have also begun to push back against the agency's requests for data in the wake of the public's anger about their duplicity in helping the agency spy.").

226. This was vividly demonstrated when hackers publicly posted private "nude photos of as many as 100 celebrities, [that were] taken from their Apple iCloud backups." *See* Sean Gallagher, *What the Celebrity Photo Hack Can Teach Us About Cloud Security*, WIRED U.K. (Sept. 2, 2014), http://www.wired.co.uk/news/archive/2014-09/02/j-law-cloud-security; Press Release, Pennsylvania Man Charged with Hacking Apple and Google E-Mail Accounts Belonging to More Than 100 People, Mostly Celebrities (Mar. 15, 2016), https://www.justice.gov/usao-cdca/pr/pennsylvania-man-charged-hacking-apple-and-google-e-mail-accounts-belonging-more-100.

227. *See* Barton Gellman et al., *supra* note 25; Andy Greenberg, *Intelligence Officials Admit That Edward Snowden's NSA Leaks Call for Reforms*, FORBES (Sept. 13, 2013, 3:37 PM), http://www.forbes.com/sites/andygreenberg/2013/09/13/intelligence-officials-admit-that-edward-

lations, Fourth Amendment jurisprudence has returned to the spotlight. Yet, courts continue to apply the SCA to areas that the SCA was not designed to be applied to, and the legislature did not likely anticipate when the SCA was enacted as part of the ECPA in 1986.[228] The narrow scope of the SCA is not obvious to judges and has not stopped them from "twist[ing] the statute to do things that it was never intended to do. For example, several district courts have applied the SCA to regulate the placement of electronic cookies on home computers."[229] The SCA should not apply to electronic cookies on home computers because "home computers are already protected by the Fourth Amendment, so statutory protections are not needed."[230]

Stored communication is unavoidable in everyday life, and the decades old SCA does not conform to modern expectations of privacy. If Congress fails to provide adequate legal protections that conform to modern expectations of privacy, consumers will likely adopt technical protections that cannot be circumvented even in an emergency. In the face of uncertain legal protections, consumers are likely to take matters into their own hands. Steve Gibson, a security researcher, observed that consumer interest in privacy technologies, like encryption, was a reaction to the Snowden revelations.[231] Techniques to make all wiretapping and recovery of stored information mathematically infeasible has been readily available for a very long time, and experts in the information security sector have both the will and the expertise to

---

snowdens-leaks-call-for-reforms. "By law, the NSA may 'target' only foreign nationals located overseas unless it obtains a warrant based on probable cause from a special surveillance court." Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted far Outnumber the Foreigners Who Are*, WASH. POST, July 5, 2014, https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html. However, Snowden revealed that NSA surveillance programs, such as PRISM and Upstream, mass-collected information on U.S. citizens and residents, and "[m]ost of the people caught up in those programs are not the targets and would not lawfully qualify as such." *Id.* In addition, "[t]he NSA treats all content intercepted incidentally from third parties as permissible to retain, store, search and distribute to its government customers." *Id.*

228. Peterson, *supra* note 89.

229. Kerr, *supra* note 11, at 1212 (footnote omitted). HTTP Cookies, commonly called "cookies," are a way for websites to store and retrieve information on your device. *What Are Cookies*?, BBC: WEBWISE (Oct. 10, 2012), http://www.bbc.co.uk/webwise/guides/about-cookies. Cookies are used to store preferences and session data, but they also enable marketers to track users. *Id.*

230. Kerr, *supra* note 11, at 1215.

231. *Security Now!: Shocked by the Shell*, *supra* note 20 (transcript at 8).

help consumers utilize those techniques.[232] Before the Snowden revelations, more people accepted that the government had a valid interest in intercepting and recovering limited information for investigative purposes, such as kidnappings or terrorist activities, but interest in privacy technologies and strong encryption has increased in the wake of the flood of high profile data breaches.[233]

Adoption of strong encryption for e-mails was slow because current implementations require the users to surmount many technical hurdles, and, as a result, the adoption has been limited to those who are already familiar with information security.[234] However, partly in response to the Snowden revelations, new services are being launched to enable encrypted e-mail for users who do not have the knowledge that is required to deploy complex solutions traditionally associated with encrypted communications.[235] There is also increased interest in investigating the underlying soundness of those solutions as the NSA continues to try to undermine those solutions.[236]

Regardless of whether the government, industry, or the people themselves should be responsible for ensuring privacy in electronic communication,[237] the use of encryption in general for web traffic has

232. *Id.* ("[W]e have the technology to absolutely lock this stuff down. And it'll take a while for it to get deployed. But once it has, it's game over for the intelligence agencies. This is not an insolvable problem if we choose to solve the problem.").

233. *Id.* (transcript at 8–9).

234. Damien Gayle, *The Edward Snowden Guide to Encryption: Fugitive's 12-Minute Homemade Video Ahead of Leaks Explaining How To Avoid NSA from Tracking E-mails*, DAILY MAIL.COM, http://www.dailymail.co.uk/news/article-2628082/The-Edward-Snowden-guide-encryption-Fugitives-12-minute-homemade-video-ahead-leaks-explaining-avoid-NSA-tracking-emails.html (last updated May 14, 2014, 8:00 AM) ("PGP and similar programs are just too complicated for the masses . . . . [T]hus adoption over the past 20 years has been limited to the highly technical – the uber geeks. Now, if a service like gmail.com had an option in there to perform digital signing and encryption in a way that most people could use it, that would have a huge impact." (quoting TK Keanini, Chief Technology Officer, Lancope)).

235. These range from those that are purportedly "NSA proof," such as ProtonMail, in which the provider never has access to unencrypted messages, to those that hamper mass collection but could be vulnerable if the provider is presented with a court order. *See* Kashmir Hill, *The NSA Gives Birth to Start-Ups*, FORBES (Sept. 10, 2014, 2:17 PM), http://www.forbes.com/sites/kashmirhill/2014/09/10/the-nsa-gives-birth-to-start-ups/#2715e4857a0b66d19d783e08; Hollie Slade, *'NSA-Proof' E-mail ProtonMail Launching Mobile App*, FORBES (Aug. 1, 2014, 6:00 AM), http://www.forbes.com/sites/hollieslade/2014/08/01/nsa-proof-email-protonmail-launching-mobile-app/#539a33f959e3.

236. *See, e.g.*, *Secure Messaging Scorecard*, *supra* note 139 (listing characteristics, including whether messages can be decrypted by the provider, thereby making them vulnerable to government searches and whether the code is open to and has recently been independently audited to find backdoors or intentional undermining of the cryptography).

237. "People need to understand that when people offer free services, you and your information are the payment." Gayle, *supra* note 234 (quoting TK Keanini, Chief Technology Officer, Lancope). *But see* Gayle, *supra* note 234 ("[T]here needs to be more pressure on government to

already increased by over 60% in the United States since the Snowden revelations;[238] thus, services that enable encryption of users' traffic are becoming more popular.[239] Despite law enforcement and intelligence agencies' concerns about companies "marketing something expressly to allow people to place themselves above the law,"[240] efforts are underway to make encrypted communications available to all for free.[241]

The only hurdle, then, is consumers' desire and willingness to adopt and deploy strong encryption for stored communication. People of the United States have already shown the capacity to increase adoption of protection against a perceived threat to, or uncertainty over, a constitutional right, particularly in the context of firearms ownership.[242] Firearms sales soared in response to uncertainty over constitutional protection of the private ownership of firearms.[243] That fervor decreases once uncertainty is resolved.[244] For firearms, produc-

---

stop them from snooping on the private lives of ordinary people . . . ." (quoting Mike Rispoli, spokesman for Privacy International)).

238. Williams, *supra* note 135 (discussing SANDVINE, 1H 2014, GLOBAL INTERNET PHENOMENON REPORT 6 (2014), https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf).

239. *See* Byron Acohido, *How Free VPNs Could Return Privacy to a Social Norm*, USA TODAY (Nov. 9, 2013, 2:15 PM), http://www.usatoday.com/story/cybertruth/2013/11/05/how-free-vpns-can-make-privacy-a-social-norm/3431597/.

240. Pamela Brown & Evan Perez, *FBI Tells Apple, Google Their Privacy Efforts Could Hamstring Investigations*, CNN: POLITICS (Oct. 12, 2014, 8:12 PM), http://www.cnn.com/2014/09/25/politics/fbi-apple-google-privacy/ (quoting James Comey, Director, Federal Bureau of Investigation).

241. *See* Martyn Casserly, *How To Send Encrypted Emails the Easy Way: Get Total Email Privacy Regardless of Your Email Provider - Works with Gmail, Hotmail and more*, PC ADVISOR (Mar. 18, 2016), http://www.pcadvisor.co.uk/how-to/internet/how-send-encrypted-emails-easy-gmail-hotmail-3636950/; *Worldwide Encryption Products Survey*, *supra* note 23.

242. *See* Michael Cooper, *Sales of Guns Soar in U.S. as Nation Weighs Tougher Limits*, N.Y. TIMES, Jan. 11, 2013, http://www.nytimes.com/2013/01/12/us/as-us-weighs-new-rules-sales-of-guns-and-ammunition-surge.html ("When you are threatened with the possibility that you are going to lose something, you get a bunch of it." (quoting Rev. Laurence Hesser)); Arpita Mukherjee & Siddharth Cavale, *PREVIEW- U.S. Gun Makers Aim for Record Quarter as Curbs Loom*, CHI. TRIB., Feb. 25, 2013, http://articles.chicagotribune.com/2013-02-25/news/sns-rt-gun manufacturers-results-previewl4n0bl6es-20130224_1_gun-sales-gun-makers-newtown-shootings; *see also* Sari Horwitz & Peter Finn, *Untitled*, WASH. POST: NAT'L SECURITY, Jan. 17, 2013, http://www.washingtonpost.com/world/national-security/2013/01/17/011bb7e0-60de-11e2-9940-6fc488f3fecd_story.html. *But see* Frank Miniter, Opinion, *What the Left Won't Tell You About the Boom in U.S. Gun Sales*, FORBES (Aug. 23, 2012, 11:52 AM), http://www.forbes.com/sites/frankminiter/2012/08/23/what-the-left-wont-tell-you-about-the-boom-in-u-s-gun-sales/2/ (explaining that the surge in gun sales began in 2005, years before the proposed legislation).

243. Gregor Aisch & Josh Keller, *Gun Sales Soar After Obama Calls for New Restrictions*, N.Y. TIMES, http://www.nytimes.com/interactive/2015/12/10/us/gun-sales-terrorism-obama-restrictions.html (last updated Mar. 18, 2016).

244. *See, e.g.*, Aaron Smith, *Gun Sales Are Plunging*, CNN: MONEY (Feb. 14, 2014, 12:01 PM), http://money.cnn.com/2014/02/14/news/companies/guns-ammo-sales/ (noting that the frenetic pace of purchasing guns and ammunition subsided when fear of increased legislation dissipated).

tion speed is a mitigating factor; there may be an increased demand, but supplies are limited to production, and it takes time to increase production.[245] However, the elasticity provided by the cloud allows service providers to quickly respond to increased demand for services, and this limit does not prevent adoption of strong encryption provided by cloud services.[246] Therefore, the most appropriate and feasible way to avoid a world in which warrants are essentially useless against all ESI is to conform legal protections to modern expectations of privacy and, therefore, disincentivize the mass adoption of strong encryption.

Consumers do not have a meaningful choice over whether to use stored communications, but they do have a choice over whether to adopt services that protect such communications with strong encryption.

IV. IMPACT

If legal protection is not clarified to alleviate consumer anxieties about mass surveillance and warrantless searches, uncertainties regarding Fourth Amendment protection of consumer information will likely lead to mass adoption of strong encryption. Mass adoption of strong encryption will lead to dire security, social, and economic implications.

A. Potential Security Implications Surrounding the Mass Adoption of Strong Encryption

If strong encryption is widely adopted, law enforcement would have no access to protected information even with a court order. In an emergency, law enforcement and intelligence agencies may be able to serve a court order to a provider or break down a physical door, but no one can break the mathematical principles that underlie strong encryption.[247] Law enforcement officials are already subjected to an increase in devices that they cannot access because of encryption, and this change has been swift.[248] It is clear that strong encryption already causes a problem for law enforcement because "[p]rosecutors have now [resorted to] the All Writs Act, an 18th-century federal law that simply allows courts to issue a writ, or order, which compels a person

245. *See* Cooper, *supra* note 242.

246. *See generally* MELL & GRANCE, *supra* note 19, at 2 (noting the rapid elasticity of cloud computing); *infra* notes 108–48 (describing how cloud computing is linked to strong encryption)

247. *See Security Now!: Poodle Bites* (Gibson Research Corporation podcast Oct. 21, 2014) (transcript at 3), https://www.grc.com/sn/sn-478.pdf.

248. *Id.*

or company to do something."[249] In fact, some police departments whose own data has been maliciously encrypted and held at ransom had no choice but to pay that ransom.[250]

Strong encryption deployed in stored communication presents much of the same challenges. If these techniques are widely adopted, the problem can no longer be solved with court orders because the decryption would be computationally infeasible.[251] Requiring disclosure of encryption keys protecting content may be viewed as testimonial and trigger Fifth Amendment protection.[252] "Something you are," such as a fingerprint, or "something you have," such as a hard drive, do not implicate the Fifth Amendment. However, encryption keys are "something you know," and the Eleventh Circuit held that "decryption and production of the contents of the hard drives would sufficiently implicate the Fifth Amendment privilege."[253]

To fulfill consumer demands, companies may also decide to place data centers outside of the United States to insulate them from

249. Cyrus Farivar, *Feds Want Apple's Help To Defeat Encrypted Phones, New Legal Case Shows*, ARS TECHNICA (Dec. 1, 2014, 8:00 PM), http://arstechnica.com/tech-policy/2014/12/feds-want-apples-help-to-defeat-encrypted-phones-new-legal-case-shows/; *e.g.*, *In re* Search of an Apple Iphone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016). In a recent case, the FBI sought an order to compel Apple to help it conduct a brute-force passcode attack on an iPhone used by one of the shooters in the 2015 San Bernadino attack. Orin Kerr, Opinion, *Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case (Part 1)*, WASH. POST: VOLOKH CONSPIRACY (Feb. 18, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/18/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-1/. However, this case does not directly implicate the Fourth Amendment because the government has a search warrant but sought "Apple's help in carrying out the warrant that the government already has." *Id.* The FBI has since indicated it no longer needs Apple's assistance in that specific case; however, many other similar cases remain. Eliza Sweren-Becker, *This Map Shows How the Apple-FBI Fight Was About Much More than One Phone*, ACLU (Mar. 30, 2016, 9:00 AM), https://www.aclu.org/blog/speak-freely/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone.

250. *See, e.g.*, Gregory Pratt, *Midlothian Cops Pay Ransom To Retrieve Data from Hacker*, CHI. TRIB., Feb. 20, 2015, http://www.chicagotribune.com/news/local/breaking/ct-midlothian-hacker-ransom-met-20150220-story.html. *See also, e.g.*, *Hospital Declares 'Internal State of Emergency' After Ransomware Infection*, KREBS ON SECURITY (Mar. 22, 2016), https://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/.

251. *See Security Now!: Poodle Bites*, *supra* note 247 (transcript at 12–13). "[M]ath is fundamentally unbreakable. We have unbreakable math." And the fact that we've been maybe somewhat lackadaisical in deploying it or enforcing it doesn't mean that it's not available to us. And it really hasn't taken long at all." *Id.* (transcript at 3). "[T]here may be vulnerabilities in the specific implementations of unbreakable math. *Security Now!: The (In)Security of 2014* (Gibson Research Corporation podcast Dec. 30, 2014) (transcript at 31), https://www.grc.com/sn/sn-488.pdf ("And we have great math. It is implementation vulnerabilities, and there are some architectures which are weak. The architecture of the public key system is weak.").

252. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

253. *See id.*

searches.[254] This will not only have an economic impact on the United States,[255] but it is also antithetical to the Internet as a distributed "medium without borders"[256] Many companies that are concerned about overreach by intelligence agencies from other countries, are turning to Swiss data centers for protection.[257] Imposing such drastic geographic restrictions on the location of the data centers will do little to curb the adoption of strong encryption; these actions will only "break the Internet,"[258] restrict the free flow of information that enables technological and social advancements, and diminish the functionality of a system designed to provide redundancies irrespective of geography.

B. Potential Social and Economic Implications Surrounding the Mass Adoption or Prohibition of Strong Encryption

Concerns over mass Internet surveillance have prompted interest in encryption,[259] and some commentators have argued that the solution is to ban strong encryption or to require all implementations to have built in undisclosed backdoors.[260] Others suggest allowing law en-

---

254. Julian Hattem, *Google Chief on NSA: 'We're Going To End Up Breaking the Internet*,' HILL (Oct. 8, 2014, 3:24 PM), http://thehill.com/policy/technology/220176-google-head-without-reform-nsa-will-break-the-internet.

255. *See* DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 3 (Aug. 2013), http://www2.itif.org/2013-cloud-computing-costs.pdf ("On the low end, U.S. cloud computing providers might lose $21.5 billion over the next three years. . . . On the high end, U.S. cloud computing providers might lose $35.0 billion by 2016."); Tom Groenfeldt, *Gov Spying Boosts Swiss Data Center Revenues*, FORBES (July 4, 2013, 12:06 PM), http://www.forbes.com/sites/tomgroenfeldt/2013/07/04/gov-spying-boosts-swiss-data-center-revenues/.

256. Hattem, *supra* note 254.

257. Groenfeldt, *supra* note 255 ("Mateo Meier, director at Artmotion, Switzerland's biggest offshore hosting company, said revenues grew 45 to 50 percent last year as companies from industries as varied as oil and gas to technology to finance look for a place to store confidential data."). *But see August 2013 Web Server Survey*, NETCRAFT (Aug. 9, 2013), http://news.netcraft.com/archives/2013/08/09/august-2013-web-server-survey.html ("Despite speculation that the recent PRISM revelations would result in a mass exodus from American data centers and web hosting companies, Netcraft has not yet seen any evidence of this.").

258. Hattem, *supra* note 254.

> By creating national barriers to data, data localization measures break up the World Wide Web, which was designed to share information across the globe. The Internet is a global network based on a protocol for interconnecting computers without regard for national borders. Information is routed across this network through decisions made autonomously and automatically at local routers, which choose paths based largely on efficiency, unaware of political borders.

Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015) (footnote omitted).

259. *Secure Messaging Scorecard*, *supra* note 139.

260. *See, e.g.*, Jon Brodkin, *FBI Official: It's America's Choice Whether We Want To Be Spied On*, ARS TECHNICA (Nov. 4, 2015 10:42 PM), http://arstechnica.com/tech-policy/2015/11/fbi-official-its-americas-choice-whether-we-want-to-be-spied-on/ (providing the viewpoint of James

forcement to have documented "exceptional access" to encrypted materials, such as key escrow, which is third-party storage of encryption keys in escrow.[261] These prohibitions on encryption would mean joining the ranks of China, Iran, and Russia.[262]

More importantly, these suggestions are inherently unworkable because they would introduce unacceptable weaknesses to the very core of what makes encryption secure.[263] In fact, the information security industry recognizes the necessity of "forward secrecy" in stored communication.[264] Forward secrecy ensures that past communication cannot be decrypted by a compromised key because each key is only used for one session, which is another barrier to exceptional access.[265] The technology is already widely supported by browsers and servers, and companies are already aggressively adopting the use for normal transactions with consumers.[266] If domestic companies are required to maintain encryption keys to decrypt past communication, it would mean "[turning] back the clock on this substantial improvement in security . . . to dramatically improve functional security" while compa-

---

Baker, General Counsel, FBI); Chris Strohm & Del Quentin Wilber, *Paris Attacks Renew Call for Access to Encrypted Messages*, BLOOMBERG (Nov. 11, 2016), http://www.bloomberg.com/news/articles/2015-11-16/paris-attacks-renew-u-s-call-to-access-encrypted-communications (providing the viewpoints of Senator Dianne Feinstein, Representative Michael McCaul, and Senator John McCain). *See generally* ABELSON ET AL., THE RISKS OF KEY RECOVERY, KEY ESCROW, AND TRUSTED THIRD-PARTY ENCRYPTION (rev. 1998), https://www.schneier.com/cryptography/archives/1997/04/the_risks_of_key_rec.html (describing the requirements and proposals of key recovery); Cory Bennett, *Activists up Pressure on White House To Reject Encryption Bill*, HILL (Apr. 11, 2016, 5:15 PM), http://thehill.com/policy/cybersecurity/275885-activists-up-pressure-on-white-house-to-reject-encryption-bill (discussing the "Compliance with Court Orders Act of 2016" draft measure from Senators Richard Burr and Dianne Feinstein).

261. *See, e.g.*, Mike Rogers, *Encryption a Growing Threat to Security*, CNN, http://www.cnn.com/2015/08/01/opinions/rogers-encryption-security-risk/ (last updated Aug. 1, 2015, 7:57 AM). *But see Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 15–16 (July 8, 2015) (statement of Peter Swire, Professor of Law & Ethics, Scheller College of Business, Georgia Institute of Technology), http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf (arguing that exceptional access would increase costs and decrease security).

262. Nicholas Watt, *PM's Plans To Monitor Encrypted Messages 'Would Turn UK into China,'* GUARDIAN (Jan. 15, 2015 9:09 PM), http://www.theguardian.com/politics/2015/jan/16/david-cameron-plan-monitor-encrypted-messages-challenge.

263. HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 15–17 (June 7, 2015), https://assets.documentcloud.org/documents/2158970/data-security-report.pdf.

264. *Security Now!: SQRL Revisited* (Gibson Research Corporation podcast July 14, 2015) (transcript at 10), https://www.grc.com/sn/sn-516.pdf.

265. *Id.* (transcript at 11).

266. *Id.*

nies outside of the United States would be free to offer this function, which would put domestic companies at a disadvantage.[267]

Congress previously tried to curb the adoption of strong encryption by banning it outright; however, this was largely unsuccessful.[268] The "Arms Export Control Act (AECA) of 1976 and the International Trade in Arms Regulations (ITAR), which was revised in 1992, severely restrict [U.S.] companies from exporting any and all military and intelligence related technologies[,]" including strong encryption.[269] The "mathematical algorithms on which cryptography is based" were famously "classified as military technologies" and placed on the same list regulating the export of munitions, sharing space on a list with "tanks, fighter jets, and aircraft carriers."[270]

Not only were domestic companies put at a disadvantage in the market for encryption software, but cryptographers and activists found "success in propagating strong cryptography.[271] Thus, encryption software was made available on the Internet, making it "available worldwide to anybody with a computer and a modem, so it had in effect been exported without the prior approval of the [U.S.] State Department" despite restrictions on exporting of encryption software.[272]

In practice, trying to ban encryption is comparable to trying to ban the spread of an idea;[273] the algorithms behind strong encryption can easily be described in a few short paragraphs (which comfortably fit within the footnote to this sentence) and implemented by relatively

267. *See id.*

268. *Security Now!: The Enigma Machine* (Gibson Research Corporation podcast Jan. 13, 2015) (transcript at 14), https://www.grc.com/sn/sn-490.pdf. Previous attempts by the U.S. government to regulate encryption technologies did little to stop the spread of strong encryption. *Id.* The renewed interest in the United Kingdom for this type of scheme to unilaterally prevent people from using strong encryption will likely fail as well because adequate enforcement is simply unrealistic. *Id.* ("Are they going to throw everybody [who uses strong encryption] in jail . . . ?").

269. Michael Schwartzbeck, *The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies (U)*, ENCRYPTION TECH. 21, 23–24 (Top Secret document, approved for release Sept. 10, 2014) (footnotes omitted), http://www.foia.cia.gov/sites/default/files/DOC_0006231614.pdf.

270. *Id.* at 24. *See generally* Arms Export Control Act, 22 U.S.C. §2751 (2012); International Traffic in Arms Regulations, 22 C.F.R. §§120.1–.32 (2011).

271. *Id.* (footnote omitted).

272. *Id.*

273. Activists have lampooned these restrictions by wearing shirts "with the source code for the RSA encryption system printed on the front. At the time the shirt was created, the United States government's export laws forbade taking the shirt from the country." Peter Wayner, *Cryptography and Paranoia in Anguilla*, N.Y. TIMES, Mar. 4, 1997, http://partners.nytimes.com/library/cyber/week/030497anguilla.html.

simple programming.[274] Therefore, banning strong encryption or requiring backdoors will do nothing to stop the propagation of strong encryption to those who wish to access it.[275] Further, it will only lead to a repeat of the economic impact on domestic companies.[276] The nature of the Internet makes it easy for consumers to go beyond borders, and the cloud makes it easy for the companies to accommodate essentially unlimited consumer demand. The very systems that enable cloud computing would also allow easy access to services provided by companies in countries that do not have restrictions on the use of strong encryption. In addition, modern commerce is simply impossible without strong encryption.[277] Public interest is better served by

---

274. For example, the Diffie-Hellman key agreement protocol, which "is a method for two computer users to generate a shared private key with which they can then exchange information across an insecure channel" and is the basis of many key exchange protocols, can be described in this relatively short section of text:

> Let the users be named Alice and Bob. First, they agree on two prime numbers g and p, where p is large (typically at least 512 bits) and g is a primitive root modulo p. (In practice, it is a good idea to choose p such that $p - 1)/2$ is also prime.) The numbers g and p need not be kept secret from other users. Now Alice chooses a large random number a as her private key and Bob similarly chooses a large number b. Alice then computes $A = g^a \pmod p$, which she sends to Bob, and Bob computes $B = g^b \pmod p$, which he sends to Alice.
>
> Now both Alice and Bob compute their shared key $K = g^{ab} \pmod p$, which Alice computes as
>
> $K = B^a \pmod p$
>
> and Bob computes as
>
> $K = A^b \pmod p = (g^a)^b \pmod p$
>
> [Because $(x^m) = x^{mn}$ and, therefore, $(g^b)^a = (g^a)^b = g^{ab}$,] Alice and Bob can now use their shared key K to exchange information without worrying about other users obtaining this information. In order for a potential eavesdropper (Eve) to do so, she would first need to obtain $K = g^{ab} \pmod p$ knowing only g, p, $A = g^a \pmod p$ and $B = g^b \pmod p$.
>
> This can be done by computing a from $A = g^a \pmod p$ and b from $B = g^b \pmod p$. This is the discrete logarithm problem, which is computationally infeasible for large p. Computing the discrete logarithm of a number modulo takes roughly the same amount of time as factoring the product of two primes the same size as p, which is what the security of the RSA cryptosystem relies on. Thus, the Diffie-Hellman protocol is roughly as secure as RSA.

David Terr, *Diffie-Hellman Protocol*, WOLFRAM MATHWORLD, http://mathworld.wolfram.com/Diffie-HellmanProtocol.html (last visited Feb. 6, 2015). This mathematical principle is easily memorized, making the restrictions on this type of technology comparable to the restrictions on ideas.

275. *Security Now!: Listener Feedback 217*, *supra* note 121 ("[T]he cat's out of the bag. Bad guys will use bulletproof, unbreakable crypto, which at the moment everybody's using. But if it turns out that that's illegal, then they'll keep using it, and everybody else will just have law enforcement-breakable crypto.").

276. *See* HAROLD ABELSON ET AL., *supra* note 263, at 1, 17.

277. *See id.* at 8–10.

the ubiquitous availability of strong encryption used in regular transactions that make modern commerce possible.[278] Modern commerce simply will not work without sufficient information security.

Failure to recognize and protect the expectation of privacy in ESI will also lead to unexpected results for those who have a duty to keep information secure. Legal protection is indispensable when technical solutions are impractical. For example, the American Bar Association recognized a general reasonable expectation of privacy in e-mails. Model Rule of Professional Conduct 1.6 states: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [other provisions in the Rules]."[279] In addition, "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[280] Comments to the Model Rules note that the lawyer is not required to use special security measures if the "method of communication affords a reasonable expectation of privacy."[281] The Standing Committee on Ethics and Professional Responsibility concluded that a lawyer may communicate with the client by unencrypted e-mail "because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[282]

Plaintext electronic communication does not provide privacy from a technological standpoint, and information security best practices would urge requiring all lawyers to encrypt communications with clients.[283] The legal community is left with two options: (1) require all communication with clients to be protected by strong encryption or (2) change the ethical rules to allow plaintext communication and rely

278. Mike McConnell et al., *Why the Fear over Ubiquitous Data Encryption Is Overblown*, WASH. POST, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html ("We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.").

279. MODEL RULES OF PROF'L CONDUCT r. 1.6(a) (AM. BAR ASS'N 2013).

280. *Id.* at r. 1.6(c).

281. *Id.* at r. 1.6. cmt. 19.

282. Am. Bar Ass'n Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459, DUTY TO PROTECT THE CONFIDENTIALITY OF E-MAIL COMMUNICATION WITH ONE'S CLIENT (Aug. 2011).

283. Nevertheless, it would be illogical for any lawyer to argue, on the one hand, that expectation of privacy in e-mails is diminished in the Fourth Amendment context yet, on the other hand, maintain that there is a reasonable expectation of privacy in e-mails, and, therefore, it is ethical to send unencrypted e-mails to clients.

on legal protections. The former makes information inaccessible, even with a warrant, without cooperation from someone who holds the encryption keys and the latter leaves clients more vulnerable to information leaks.

Adhering to consumers' demands for privacy, the information technology industry responded by marketing privacy as a feature.[284] WhatsApp, the instant messaging platform acquired by Facebook in 2014, worked with Open Whisper Systems to implement the TextSecure protocol.[285] As of February 2016, WhatsApp has more than one billion monthly active users.[286] The ubiquity of WhatsApp makes it convenient to communicate with anyone securely without any burdensome preparation.[287] In 2016, WhatsApp enabled end-to-end encryption by default for all users through the improved Signal protocol, and "[t]he result is practically uncrackable encryption" for the "most popular messaging app in the world, where people exchange billions of messages a day."[288] With the Signal protocol, "WhatsApp messages will now travel all the way to the recipients' device before being decrypted, rather than merely being encrypted between the user's device and WhatsApp's server."[289]

Jan Koum, WhatsApp founder who grew "up in Soviet Ukraine in the 1980s," credits his distrust of government surveillance with the decision to enable encryption.[290] Many other messaging platforms provide similar encryption functionality for other security conscious consumers.[291] Without clear legal protections, more companies will

284. *See, e.g.*, *Security Now!: The (In)Security of 2014*, *supra* note 251 (transcript at 31).

285. Stephanie Mlot, *WhatsApp Surpasses 700M Users*, PCMAG (Jan. 7, 2015, 10:16 AM) http://www.pcmag.com/article2/0,2817,2474750,00.asp (discussing Apple's and Google's response).

286. Samuel Gibbs, *WhatsApp and Gmail Join the 1 Billion User Club*, GUARDIAN (Feb. 2, 2016, 6:15 AM), https://www.theguardian.com/technology/2016/feb/02/whatsapp-gmail-google-facebook-user-app.

287. Jethro Mullen, *What Is ISIS' Appeal for Young People?*, CNN, http://www.cnn.com/2015/02/25/middleeast/isis-kids-propaganda/ (last updated Feb. 25, 2015, 2:33 PM).

288. Cyrus Farivar, *WhatsApp Is Now Most Widely Used End-to-End Crypto Tool on the Planet*, ARS TECHNICA (Apr. 5, 2016, 9:02 PM), http://arstechnica.com/tech-policy/2016/04/whatsapp-is-now-most-widely-used-end-to-end-crypto-tool-on-the-planet/; Andy Greenberg, *Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users*, WIRED (Nov. 18, 2014, 10:54 AM), http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

289. Farivar, *supra* note 288; Greenberg, *supra* note 288. The signal protocol also implements perfect forward secrecy, so even if encryption keys are compromised, they cannot be used to decrypt previously transmitted messages. Farivar, *supra* note 288.

290. *Id.* ("I grew up in a society where everything you did was eavesdropped on, recorded, snitched on . . . . Nobody should have the right to eavesdrop, or you become a totalitarian state—the kind of state I escaped as a kid to come to this country where you have democracy and freedom of speech. Our goal is to protect it." (quoting Jan Koum, WhatsApp founder)).

291. *See Secure Messaging Scorecard*, *supra* note 139.

make strong encryption available, and more consumers will adopt strong encryption, leading to a world in which not even a warrant can make information available to law enforcement.[292]

Microsoft General Counsel Brad Smith warns of heavy repercussions for domestic tech companies if intelligence agencies continue to conduct mass surveillance[293] Concerns over privacy may push consumers to utilize the cloud "because big tech companies have the resources to properly secure data."[294] And, if legal protections are not clear in the United States, consumers can simply choose to utilize services provided by foreign companies operating infrastructures outside of the United States and far out of law enforcement's reach, even with probable cause and search warrants. In fact, many companies already locate servers outside of the United States to comply with the more stringent privacy regulations in the European Union as well as to market the location of the servers as a special feature to consumers.[295]

However, if legal protections conform with modern privacy expectations, consumers are more likely to continue using services offered by domestic companies, and many companies may continue to situate servers in the United States.[296] If the servers remain within the United States, and if consumers do not adopt strong encryption en masse, the data will remain within the reach of law enforcement through warrants.[297]

Many hold the belief that "I have nothing to hide; therefore, I have nothing to worry about."[298] During a conference regarding privacy and cybercrime at Georgetown Law, Judge Richard Posner, U.S. Court of Appeals for the Seventh Circuit, agreed with that senti-

292. However, when a perceived threat to a constitutional right is removed, people have less incentive to take matters into their own hands. *See, e.g.*, Aaron Smith, *Gun Sales Are Plunging*, CNN MONEY (Feb. 14, 2014, 12:01 PM), http://money.cnn.com/2014/02/14/news/companies/guns-ammo-sales/.

293. Jack Clark, *Microsoft: NSA Security Fallout 'Getting Worse' . . . 'Not Blowing Over,'* REGISTER (June 19, 2014, 6:30 PM), http://www.theregister.co.uk/2014/06/19/microsoft_nsa_fallout/ ("If the US government does not work to clear up the rules around how it intercepts data both at home and abroad, how deeply its spy agencies penetrate tech from its domestic companies, and how it accesses overseas data held by American companies, then there's a real danger that US companies could suffer . . . .").

294. *Id.*

295. *See, e.g.*, THREEMA: THE BEST-SELLING SECURE MESSENGER (Sept. 10, 2014), https://threema.ch/press-files/1_press_info/Press-Info_Threema_EN.pdf.

296. *August 2013 Web Server Survey*, *supra* note 257.

297. *Contra Warrant To Search Microsoft E-mail Accounts*, 15 F. Supp. 3d 466, 474, 477 (S.D.N.Y. 2014) (arguing that Congress intended an ISP to produce information regardless of where that information is stored).

298. Moxie Marlinspike, *Why 'I Have Nothing to Hide' Is the Wrong Way To Think About Surveillance*, WIRED (June 13, 2013, 6:30 AM), http://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/.

ment.[299] Judge Posner stated that "lawmakers should give the NSA 'carte blanche'" and that "[i]f the NSA wants to vacuum all the trillions of bits of information that are crawling through the electronic worldwide networks, I think that's fine."[300] Judge Posner also "criticized mobile OS companies [(such as Google and Apple)] for enabling end-to-end encryption in their newest software."[301]

However, Judge Margaret McKeown of the U.S. Court of Appeals for the Ninth Circuit spoke at the same event and disagreed with Judge Posner.[302] Judge McKeown warned that "[w]ith much of U.S. privacy law based on a reasonable expectation of privacy, it's difficult . . . to define what that means when people are voluntarily sharing all kinds of personal information online."[303] David Cole, Georgetown University Law Center Professor, noted that the "U.S. and other governments have a long history of targeting people 'who they are concerned about because they have political views and political positions that the government doesn't approve of.'"[304] U.S. Department of Justice Deputy Solicitor General Michael Dreeben took an even stronger position, noting that a "certain degree of privacy is perhaps a precondition for freedom, political freedom, artistic freedom, [and] personal autonomy."[305]

Regardless of the lofty principles of freedom and privacy, mass adoption of encryption would have immediate and practical implications for both personal and national security and economics. Without sufficient legal protections, consumers may be sufficiently motivated to utilize readily available and easy to deploy services hosted in countries with legal protections that *do* conform to their expectations of privacy, which would make information inaccessible to law enforcement even with a warrant.

V. Conclusion

ESI should enjoy the same treatment as the other forms of communication and storage that it is rapidly replacing. Even if mass adoption

299. Grant Gross, *Judge: Give NSA Unlimited Access to Digital Data*, PCWorld (Dec. 5, 2014, 7:49 AM), http://www.pcworld.idg.com.au/article/561258/judge-give-nsa-unlimited-access-digital-data/.

300. *Id.* (quoting Judge Posner).

301. Gross, *supra* note 299 ("I'm shocked at the thought that a company would be permitted to manufacture an electronic product that the government would not be able to search . . . ." (quoting Judge Richard Posner)).

302. *Id.* (quoting Judge Margaret McKeown).

303. *Id.*

304. *Id.* (quoting David Cole, Professor, Georgetown University Law Center).

305. *Id.* (quoting Michael Dreeben, Deputy Solicitor General, U.S. Department of Justice).

of encryption is inevitable or, perhaps, preferable, the laws governing search and seizure of ESI must reflect modern expectations of privacy, and the decades-old SCA no longer conforms to these expectations of privacy. Without clear legal protections, consumers are likely to adopt strong encryption that cannot be circumvented by law enforcement and intelligence agencies. Consequently, Congress must amend the SCA to: (1) explicitly protect remote storage in addition to communication; (2) eliminate the arbitrary 180-day rule; (3) uphold search warrant requirements despite the third-party doctrine; (4) and rebuild the trust between the government and the people of the United States.

With clear legal protections for ESI that conform to modern expectations of privacy, consumers would be less likely to adopt strong encryption en masse, and would be more likely to continue using services provided by domestic companies. The practical consequences of clear legal protection for information consumers store with service providers are far from helping criminals elude law enforcement. It may be the only way for law enforcement to dissuade mass adoption of strong encryption, maintain access to the information law enforcement needs in emergencies, and avoid a world in which a warrant would mean nothing more than the possibility of holding the encryption key owner in contempt while law enforcement makes futile attempts to guess the encryption key, and the passage of time renders the information useless.

*Wei Chen Lin**

* J.D. Candidate, DePaul University College of Law, 2016; B.S., DePaul University, 2012. I would like to thank the Editorial Board and Staff of Volumes 64 and 65, especially Riebana Sachs for her work editing this Comment. I would also like to thank my mentors, family, and friends who supported me in this endeavor. All errors are my own.