Georgia State University Law Review

Volume 33
Issue 2 *Winter 2016-2017*

Article 5

3-9-2017

Civil Liberty or National Security: The Battle Over iPhone Encryption

Karen Lowell
Georgia State University College of Law, karenlowell1@gmail.com

CIVIL LIBERTY OR NATIONAL SECURITY: THE BATTLE OVER IPHONE ENCRYPTION

Karen G. Lowell*

INTRODUCTION

On June 5, 2013,[1] Edward Snowden[2] released what would be the first of many documents exposing the vast breadth of electronic surveillance the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) had been conducting on millions of United States citizens.[3] Although the federal agencies had legal authority under the Foreign Intelligence Surveillance Act (FISA) to collect metadata from companies such as Verizon, many Americans considered this data collection to be a massive invasion of privacy.[4]

Equipped with the knowledge of sweeping domestic surveillance programs, citizens and technology firms fighting for strong privacy and security protection, have started to take matters into their own hands.[5] Most notably, Apple responded in 2014 by announcing that its operating system, iOS 8, now prevents anyone—including both

---

*J.D. Candidate 2017, Georgia State University College of Law. I would like to first thank my husband, Evan, for his constant support and encouragement, and my family for their love and patience during this journey. I would also like to thank Professor Caren Morrison for her insightful feedback and edits during the revision process.

1. Mirren Gidda, *Edward Snowden and the NSA Files - Timeline*, GUARDIAN (Aug. 21, 2013, 5:54 PM), https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

2. "Edward Snowden is a former National Security Agency subcontractor who made headlines in 2013 when he leaked top-secret information about NSA surveillance activities." *Edward Snowden Biography*, BIOGRAPHY.COM, http://www.biography.com/people/edward-snowden-21262897#synopsis (last visited Dec. 9, 2016).

3. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see* Joshua Eaton, *Timeline of Edward Snowden's Revelations*, AL JAZEERA AM., http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html (last visited Dec. 9, 2016) (organizing the release of all articles related to Edward Snowden and his disclosure of NSA surveillance methods).

4. Dan Roberts & Spencer Ackerman, *Anger Swells After NSA Phone Records Court Order Revelation*, GUARDIAN (June 6, 2013, 9:05 PM), http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records.

5. Alex Hern, *Apple Defies FBI and Offers Encryption by Default on New Operating System*, GUARDIAN (Oct. 17, 2014, 1:57 PM), http://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx.

Apple and law enforcement—from bypassing the device owner's consent in order to access any data on the smartphone or tablet.[6] Google, Facebook, Yahoo, and Microsoft followed suit soon after.[7]

Standing in contrast to privacy supporters are national security advocates.[8] For months now, the FBI and NSA have expressed great concern for public safety as their ability to collect both real-time data and stored data from terrorists and criminals has been "crippled" by encryption.[9] The FBI's fears came to fruition through the deadly attacks in both Paris and San Bernardino, California where the attackers allegedly used encryption to avoid detection.[10] Encryption is not only a national security issue, however, as it also affects local law enforcement's ability to solve criminal cases.[11] For example, the

6. Elise Hu, *Apple: iOS 8 Prevents Cooperation with Police Unlocking Requests*, NPR (Sept. 18, 2014, 12:16 PM), http://www.npr.org/sections/alltechconsidered/2014/09/18/349561490/apple-ios-8-prevents-cooperation-with-police-unlocking-requests.

7. Pamela Brown & Evan Perez, *FBI Tells Apple, Google, Their Privacy Efforts Could Hamstring Investigations*, CNN: POL., http://www.cnn.com/2014/09/25/politics/fbi-apple-google-privacy/index.html (last updated Oct. 12, 2014); Andrea Peterson, *Yahoo's Plan to Get Mail Users to Encrypt Their E-mail: Make It Simple*, WASH. POST (Mar. 15, 2005), https://www.washingtonpost.com/news/the-switch/wp/2015/03/15/yahoos-plan-to-get-mail-users-to-encrypt-their-e-mail-make-it-simple/.

8. Damian Paletta, *Silicon Valley Faces Showdown as Lawmakers Fume over Encryption*, WALL ST. J. (Dec. 10, 2015, 11:05 PM), http://blogs.wsj.com/washwire/2015/12/10/silicon-valley-faces-showdown-as-lawmakers-fume-over-encryption/; Evan Perez & Shimon Prokupecz, *Paris Attackers Likely Used Encrypted Apps, Officials Say*, CNN: POL. (Dec. 17, 2015, 10:00 AM), http://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/index.html#.

9. *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*: *Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 6–16 (2001) [hereinafter *Going Dark*] (statement of Valerie Caproni, General Counsel, Fed. Bureau of Investigation); James B. Comey, Dir., Fed. Bureau of Investigation, Address at the International Association of Chiefs of Police 121st Annual Conference: The FBI and the IACP: Facing Challenges Together (Oct. 27, 2014), https://www.fbi.gov/news/speeches/the-fbi-and-the-iacp-facing-challenges-together. *But see* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 466–70 (2012). Although law enforcement may be losing one avenue of electronic surveillance to encryption, there has never been a time when more technology innovations are available to increase law enforcement's capabilities. *Id.* at 470.

10. Paletta, *supra* note 8; Eric Lichtblau & Joseph Goldstein, *Justice Dept. Appeals Ruling in Apple iPhone Case in Brooklyn*, N.Y. TIMES (Mar. 7, 2016), http://www.nytimes.com/2016/03/08/technology/justice-dept-appeals-ruling-in-apple-iphone-case-in-brooklyn.html. *But see* Mike Masnick, *The Paris Attacks and the Encryption/Surveillance Bogeyman: The Story So Far*, TECHDIRT (Nov. 19, 2015, 11:48 AM), https://www.techdirt.com/articles/20151119/06374432860/paris-attacks-encryptionsurveillance-bogeyman-story-so-far.shtml (noting that some terrorists likely used unencrypted SMS to communicate).

11. *See* Nicole Arce, *Manhattan DA Blames Apple Encryption for Failing to Solve 111 Criminal Cases*, TECH TIMES (Nov. 19, 2015 3:52 AM), http://www.techtimes.com/articles/108322/20151119/manhattan-da-blames-apple-encryption-for-failing-to-solve-111-criminal-cases.htm.

Manhattan District Attorney's Office has reported that "roughly 111" cases—involving homicide, attempted murder, child sexual abuse, sex trafficking, and assault and robbery—went unsolved last year due to cell phone encryption.[12]

In the past, the FBI was able to serve a court order to telecommunication providers, and the providers were then required to intercept and provide communications to law enforcement.[13] Currently, however, either law enforcement no longer serves such court orders on technology firms, such as Apple, or the firms simply reject and return the court orders because they do not have the means to access the requested data due to encryption.[14] The FBI refers to this increasing disparity between legal authority and technological capabilities as "going dark."[15] This dark realm of electronic communications is a forum "where pedophiles can't be seen, kidnappers can't be seen, [and] drug dealers can't be seen."[16] To be clear, the FBI claims it is not opposed to privacy protection; rather, the FBI supports such measures so long as a "legal framework" or another solution exists that will enable law enforcement to access encrypted communications when probable cause of criminal activity arises.[17]

With law enforcement and privacy advocates settling on opposite ends of the debate, cooperation and compromise seems unlikely.[18] Therefore, Congress will likely have to weigh in on the issue to find an amicable solution that balances the needs of law enforcement against the privacy protections demanded by citizens.[19]

---

12. *Id.*

13. *Going Dark*, *supra* note 9, at 6–7.

14. Matt Apuzzo, David E. Sanger & Michael S. Schmidt, *Apple and Other Tech Companies Tangle with U.S. over Data Access*, N.Y. TIMES (Sept. 7, 2015), http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html.

15. *Going Dark*, *supra* note 9, at 10.

16. Aaron Sankin, *FBI Director Urges Congress to Crack Down on Encryption*, DAILY DOT (Mar. 26, 2015, 3:33PM), http://www.dailydot.com/politics/james-comey-encryption-law-fbi/.

17. Sam Sacks, *NSA Joins FBI in Fight Against Total Encryption*, DIST. SENTINEL (Feb. 23, 2015), https://www.districtsentinel.com/nsa-joins-fbi-in-fight-against-total-encryption/.

18. *See* Apuzzo, Sanger & Schmidt, *supra* note 14.

19. *Id.* ("Microsoft argues that Congress will ultimately have to weigh in on the issue, since it is as much a political matter as a legal one: 'Only Congress has the institutional competence and constitutional authority to balance law enforcement needs against our nation's sovereignty, the privacy

This Note analyzes why certain communications on smartphones should not be automatically encrypted if the provider does not have the means to decrypt the communication. Although Congress explicitly blocked past legislation from preventing unregulated encryption, current technology trends unreasonably favor civil liberties, undermining law enforcement's ability to maintain a safe society. Part I of this Note provides a basic understanding of encryption while also outlining relevant wiretap statutes.[20] Part II provides both the legal background and an analysis using the framework outlined in *Katz* as it applies to communications transmitted through encrypted smartphones.[21] Part II also outlines the protections afforded to individuals by the Fourth Amendment as well as relevant legislation for electronic surveillance and encryption.[22] Part III of this Note recommends a legal framework for technology firms that employ encryption software on smartphones.[23]

I. BACKGROUND

A. Encryption

As a result of the Edward Snowden leaks, headlines spouted titles such as "Apple and Google Have Won Praise From Privacy Proponents for Efforts to Encrypt Their Latest Smartphones."[24] Although encryption offers privacy benefits, it also cripples law enforcement and, in turn, jeopardizes public safety.[25]

---

of its citizens and the competitiveness of its industry.'"). *But see* Cory Bennett, *Top House Democrat: Silicon Valley Asking for Encryption Proposal*, THE HILL: POLICY (Sept. 10, 2015, 10:43 AM), http://thehill.com/policy/cybersecurity/253205-top-house-intel-dem-silicon-valley-wants-to-see-encryption-proposal (Rep. Adam Schiff (D-Cal.) stating Congress will be of little help suggesting a solution on the fight over encryption due to the complexity and political nature of the problem); Mike Masnick, *White House Realizes Mandating Backdoors to Encryption Isn't Going to Happen*, TECHDIRT (Sept. 17, 2015, 8:17 AM), https://www.techdirt.com/articles/20150916/15035232275/white-house-realizes-mandating-backdoors-to-encryption-isnt-going-to-happen.shtml (disclosing there is not enough support from Congress to mandate a legislative backdoor to encryption).

20. *See infra* Part I.
21. *See infra* Part II.
22. *See infra* Part III.
23. *See infra* Part III.
24. Brown & Perez, *supra* note 7.
25. James Comey, *Encryption, Public Safety, and "Going Dark*," LAWFARE (Jul. 6, 2015, 10:38

1. History

Despite the recent tension between Silicon Valley and the FBI and NSA, encryption is not new technology. Cryptology first took the main stage in the twentieth century during World War II when Germany developed the Enigma machine to secretly communicate with U-boats in the Atlantic Ocean.[26] Once the Internet launched, encryption became a hotly debated policy issue in the 1990s.[27] As a result, the federal government proposed a solution called the "Clipper Chip," which would protect private communications through encryption while enabling the government to decrypt the communications through a permitted "key."[28] Due to extreme controversy, however, the program was abandoned by 1996.[29] Soon after, the "crypto wars" died down.[30] Recently, the threat of security breaches and warrantless searches has rekindled the debate.

2. How Encryption Works

Put simply, encryption is the process of rendering information indecipherable except to the people holding an authorized electronic key.[31] A "key" consists of ones or zeros, which computers then use in

AM), https://www.lawfareblog.com/encryption-public-safety-and-going-dark.

26. Swire & Ahmad, *supra* note 9, at 425–26. Unlike the Enigma machine, which was broken by the "Ultra" project, modern encryption programs are resistant to "brute force" attacks where a computer program essentially tries every possible key combination until a working key is discovered. Chris Hoffman, *Brute-Force Attacks Explained: How All Encryption Is Vulnerable*, HOW-TO GEEK (Jul. 6, 2013), http://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/; *see, e.g.*, Dena R. Klopfenstein, Comment, *Deciphering the Encryption Debate: A Constitutional Analysis of Current Regulations and a Prediction for the Future*, 48 EMORY L.J. 765, 772 (1999) (noting that in 1996, former NSA director William Crowell told the House Committee on National Security that a 56-digit encryption key took internet participants 96 days using 78,000 computers simultaneously to decipher; a 65-bit encryption would likely take about 6,000 to 7,000 years; and a "128-bit encrypted message would take 8.6 trillion times the 'age of the universe' to crack").

27. Swire & Ahmad, *supra* note 9, at 433.

28. *Clipper Chip*, CRYPTO MUSEUM, http://www.cryptomuseum.com/crypto/usa/clipper.htm (last updated July 26, 2016).

29. *Id.*

30. Swire & Ahmad, *supra* note 9, at 433 (noting that in 1999, the Clinton administration ended the "crypto war" by changing its position and accepting widespread encryption use).

31. David B. Walker, *Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, ¶ 14.

a complex algorithm to scramble the text.[32] Once the algorithm scrambles the information, the message can only be decrypted by either a recipient who holds the authorized key or through a "brute force" attack.[33] Thus, the longer the key, the longer a computer will have to work to try and break the code using brute force.[34]

a. Private or Symmetric Key

Private Key encryption requires both the sender and the recipient of a message to use the same single key to encrypt and decrypt the information.[35] Therefore, a message is only secure if the key is kept private.[36] Once the key has been compromised, anyone can later use the key to access or send encrypted information.[37] The significant barrier with maintaining a secure key is resolving how to safely share

32. *Id.* (explaining that electronic keys consist of zeros and ones, usually at least forty in length or longer, that encryption software uses to convert the intended text into an unreadable format until decrypted by the intended recipient); Klopfenstein, *supra* note 26, at 771 (noting more specifically that computers convert data by using ones and zeros in an algorithm to scramble information).

33. Klopfenstein, *supra* note 26, at 767, 772. Currently, most cryptographic systems use a 128-bit or 256-bit symmetric key; that means there are 2^{128} or 340,282,366,920,938,463,463,374,607,431,768,211,456 possible key combinations in a 128-bit symmetric key. *Cracking Encryption Algorithms*, MYCRYPTO.NET, http://mycrypto.net/encryption/encryption_crack.html (last visited Dec. 14, 2016). Meaning, if all 7 billion people on the planet owned ten supercomputers from the year 2012, with each computer testing 1 billion key combinations per second, it would take about 77,000,000,000,000,000,000,000,000 years to succeed in a brute-force attack on a 128-bit symmetric key. Mohit Arora, Sr., *How Secure Is AES Against Brute Force Attacks?*, EETIMES: DESIGNLINES (May 7, 2012, 5:29 PM), http://www.eetimes.com/document.asp?doc_id=1279619. On a four-digit iPhone password, however, it can take as little as thirty minutes to correctly guess the combination. Alina Selyukh, *Apple, the FBI and iPhone Encryption: A Look at What's at Stake*, NPR (Feb. 17, 2016, 4:18 PM), http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake. Furthermore, it would take about five years to break a six-digit alphanumeric password containing lower-case letters and numbers. Zach Whittaker, *For iPhone, iPad Privacy, Here's How to Turn on Encryption in Just One Minute: Enabling Encryption on Your Apple Smartphone or Tablet Is Easier Than You Think*, ZDNET (May 27, 2015), http://www.zdnet.com/article/how-to-turn-on-iphone-ipad-encryption-in-one-minute/.

34. Klopfenstein, *supra* note 26, at 771–72.

35. Elizabeth Lauzon, Note, *The Philip Zimmermann Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech*, 48 SYRACUSE L. REV. 1307, 1315 (1998).

36. William A. Hodkowski, Comment, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13 SANTA CLARA COMPUTER & HIGH TECH. L.J. 217, 227 (1997).

37. *Id.* at 229.

your key with the intended recipient.[38] Philip Zimmermann, a famous cryptography programmer, said it best, "If you have a secure channel for exchanging keys, then why do you need cryptography in the first place?"[39]

b. Public or Asymmetrical Key

Public key encryption was developed after realizing the practical shortcomings of private keys.[40] Rather than using the same key to both encrypt and decrypt a message, a public key uses three separate authorized keys: a known public key; a private key to encrypt; and another distinct private key to decrypt.[41] Each individual involved has both a public key and a private key.[42] To send a message to an individual, the sender would use his private key in combination with the recipient's publically available key to encrypt the message.[43] The recipient would then use his private key to decrypt the text.[44] By using a public key system, individuals bypass the problematic step of having to find a way to securely disclose the private key before being able to communicate privately.[45]

---

38. *Id.* at 227.

39. *Export Controls on Mass Market Software: Hearing Before the Subcomm. on Econ. Policy, Trade and Env't of the H. Comm. of Foreign Affairs*, 101st Cong. 110 (1993) (statement of Phillip Zimmerman, Cryptograph Consultant).

40. Lauzon, *supra* note 35, at 1317–18 (finding that public key encryption was developed because private keys proved difficult to distribute securely, especially to large groups).

41. *Id.* at 1318.

42. Swire & Ahmad, *supra* note 9, at 427.

43. *Id.*

44. *Id.* Swire and Ahmad provide the following example:

> The recipient Bob has a public key that everyone can access. Bob also has a secret, private key that allows him to decrypt these messages. Though Bob publishes his public key he does not tell anyone his private key, not even Alice. When Alice wants to send Bob a message, she wraps the message in his publically available key, and then sends it in encrypted form to her ISP where it travels through the network to Bob's ISP and eventually reaches Bob. Upon receipt, Bob uses his private key to unwrap the message and read its plaintext contents. Figure 5 illustrates the structure of a public key encryption system. If Bob wants to reply back to Alice, he wraps his message in her public key and then she unwraps it using her private key.

Id.

45. *Id.* at 428.

B. Domestic Law Enforcement and Related Congressional Action

Surveillance is a useful tactic for those who employ it to provide insight and security for the population.[46] Although surveillance is often used for the good of the nation to effectively prosecute criminals and to ensure public safety, electronic surveillance also has a history of governmental abuse.[47] Thus, Congress has enacted several statutes that bolster Fourth Amendment protections from unwarranted invasions of privacy.[48]

1. Early Electronic Surveillance History

Communications surveillance, specifically telephone wiretapping, developed shortly after Alexander Graham Bell invented the telephone in 1876.[49] The FBI and private detectives alike tapped into wires for decades, despite many state legislatures outright banning the practice due to its intrusive nature.[50] The constitutionality of wiretapping was not addressed, however, until 1928 in *Olmstead v. United States* where a Seattle bootlegger was convicted based on evidence obtained through a wiretap.[51] Olmstead moved to suppress the evidence, claiming the wiretap invaded his Fourth Amendment protections, but the Court held the wiretap did not amount to a "search" because no physical trespass onto Olmstead's property occurred.[52] The American public was outraged by the Court's disregard of Fourth Amendment protections in *Olmstead*.[53]

---

46. Daniel J. Solove, *Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1266 (2004).

47. *See id.* at 1266–67.

48. *See id*. at 1266.

49. Tom Harris, *How Wiretapping Works*, HOWSTUFFWORKS: CULTURE, http://people.howstuffworks.com/wiretapping3.htm (last visited Dec. 14, 2016) (recounting the history of telephone wiretapping). "In the 1860s, before the modern telephone was even invented, many state courts in the United States enacted statutes that prohibited anybody from listening in on telegraph communication. By the 1890s, the modern telephone was in widespread use—and so was wiretapping." *Id.*

50. Howard J. Kaplan, Joseph A. Matteo & Richard Sillett, *The History and Law of Wiretapping*, 2012 A.B.A. SEC. OF LITIG. 2.

51. William Lee Adams, *Brief History: Wiretapping*, TIME (Oct. 11, 2010), http://content.time.com/time/magazine/article/0,9171,2022653,00.html.

52. *Id.*

53. David Price, *A Social History of Wiretaps*, COUNTERPUNCH (Aug. 9, 2013), http://www.counterpunch.org/2013/08/09/a-social-history-of-wiretaps-2/.

In response to the public's outcry against the Supreme Court permitting unrestricted wiretapping, Congress passed the Federal Communications Act of 1934, which made wiretapping illegal and deemed all wiretap evidence inadmissible in court.[54] However, J. Edgar Hoover, former FBI director, was not deterred by the law's passage.[55] Although the FBI maintained a public façade of prohibiting the use of wiretaps, it continued to use wiretaps in secret, even lying to Congress.[56] Hoover went onto expand illegal wiretap use even more by appealing to public fears claiming that wiretaps were necessary to investigate spies, Nazis, and communists.[57] Despite the illegality of the FBI's activity, it never incurred sanctions, even after courts eventually learned of the FBI's illicit wiretapping.[58] In 1967, wiretapping returned to the Supreme Court's attention in *Katz v. United States*.[59] *Katz* replaced *Olmstead* by ruling that a person has a reasonable expectation of privacy in their person, and not just in the context of property rights.[60]

---

54. Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 151 (1982)) (enacting legislation "[t]o provide for the regulation of interstate and foreign communication by wire or radio, and for other purposes"); Kaplan, Matteo, & Sillett, *supra* note 50, at 3.

55. *See* Price, *supra* note 53.

56. *Id.*

57. *Id.* The history of government wiretapping is shrouded in secrecy. As Price recounted:

> President Roosevelt issued a secret executive order authorizing widespread Justice Department wire-taps of "subversives" and suspected spies. Hoover used these vague new powers to investigate not just Nazis but anyone he thought subversive. . . . The social history of wiretaps is a history of mission creep, where FBI agents initially hunting for wartime Nazi spies soon monitored progressive activists fighting racial segregation.

Id. The FBI would also use illegal wiretaps during the McCarthy era to target suspected communists, civil rights activists, and other progressive groups. *Id.*

58. *Id.*

59. Alex Markels, *Timeline: Wiretaps' Use and Abuse*, NPR (Dec. 20, 2005, 12;00 AM), http://www.npr.org/templates/story/story.php?storyId=5061834; *see also* Katz v. United States, 389 U.S. 347, 358 (1967) (holding an electronic wiretap of a phone booth unconstitutional, reasoning "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures," and "No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment.").

60. Kaplan, Matteo & Sillett, *supra* note 50, at 3–4.

2. Title III of the Omnibus Crime Control and Safe Streets Acts of 1968

The year following *Katz*, Congress responded to growing gang violence in America by passing the Omnibus Crime Control and Safe Streets Act of 1968, also commonly known as "The Wiretap Act."[61] Title III of this Act permits the interception of wire, oral, or electronic communications through wiretapping.[62] The Act authorizes wiretapping for twenty-six enumerated crimes only if the proper steps are followed including obtaining a valid court order founded upon probable cause.[63] The USA Patriot Act later enhanced Title III to permit investigations into terrorism and national security threats.[64]

3. Foreign Intelligence Surveillance Act of 1978

After Watergate and Nixon's resignation in 1974, Senator Frank Church established a committee to investigate a report revealing large-scale, warrantless searches conducted by the FBI and CIA.[65] The committee discovered that the executive branch had overreached its authority by pervasively invading the civil liberties of citizens.[66] Thus, the pendulum continued to swing in favor of public policy advocating for civil liberties.

The federal government does not need a warrant to collect communications if foreign adversaries or terrorists communicate

---

61. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2510) (stating its purpose was "[t]o assist State and local governments in reducing the incidence of crime, to increase the effectiveness, fairness, and coordination of law enforcement and criminal justice systems at all levels of government, and for other purposes"); Markels, *supra* note 59; *Privacy: Wiretap Act*, ELEC. FRONTIER FOUND., https://ilt.eff.org/index.php/Privacy:_Wiretap_Act (last modified Jan. 28, 2007) (Title III of the Omnibus Crime Control and Safe Streets Act of 1968 is also known as "The Wiretap Act").

62. JAMES A. ADAMS & DANIEL D. BLINKA, ELECTRONIC SURVEILLANCE: COMMENTARIES & STATUTES 16 (2003-2004 ed. 2003).

63. Laura K. Donohue, *Criminal Law: Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1078–79 (2006).

64. ADAMS & BLINKA, *supra* note 62, at 19.

65. *See* Tom Head, *The Foreign Intelligence Surveillance Act (FISA)*, ABOUT.COM: CIVIL LIBERTIES, http://civilliberty.about.com/od/waronterror/tp/History-of-FISA.htm (last visited Dec. 15, 2016).

66. *Id.*

outside of the United States.[67] Once a communication from a terrorist or foreign adversary penetrates the United States, however, intelligence officials are required to show probable cause before collecting targeted communications.[68] The Foreign Intelligence Surveillance Act ("FISA") was therefore established as the "exclusive means" to patrol physical searches and foreign intelligence surveillance occurring in the United States.[69] In order to conduct a physical search or electronic surveillance, the FBI must establish probable cause that the target is a "foreign power" or "an agent of a foreign power" and that the purpose of the surveillance is to collect foreign intelligence.[70] The warrants are then secretly reviewed and either approved or rejected by the Foreign Intelligence Surveillance Court, which was created by FISA.[71] In 2005, The New York Times revealed that President Bush authorized warrantless surveillance of communications connected to Al-Qaeda, which became known as the "Terrorist Surveillance Program."[72] Although

---

67. ERIC ROSENBACH & AKI J. PERITZ, *Electronic Surveillance and FISA*, *in* CONFRONTATION OR COLLABORATION?: CONGRESS AND THE INTELLIGENCE COMMUNITY 69 (2009), http://belfercenter.ksg.harvard.edu/publication/19156/electronic_surveillance_and_fisa.html.

68. *Id.*

69. *Id.* at 70.

70. The USA Patriot Act changed the primary "purpose" requirement of a FISA warrant to a "significant purpose." Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102(b), 92 Stat. 1783 (amended by Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) and codified as amended at 50 U.S.C. § 1804(a)(6)(B); *see also infra* p. 25–26 and note 93. Rosenbach and Peritz explained:

> Under FISA, U.S. citizens, legal residents and U.S. corporations (known as "U.S. persons") are protected against illegal search and seizure by the Fourth Amendment; hence, FISA includes a number of provisions to protect civil liberties. Furthermore, FISA also explicitly states that, "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment of the Constitution of the United States." While surveillance of U.S. persons is permitted under FISA, the IC must "minimize" the collection of information not directly applicable to the intended target.

ROSENBACH & PERITZ, *supra* note 67, at 69.

71. Head, *supra* note 65; Bill Moyers, *The Church Committee and FISA*, PBS (Oct. 26, 2007), http://genius.com/Public-broadcasting-service-the-church-committee-and-fisa-annotated (the FISA court consists of seven judges who are appointed by the Chief Justice and serve on the court for seven years); Jason Sattler, *FISA Court Has Only Rejected 10 of 20,909 Spying Requests: One Congressman Has a Solution*, NAT'L MEMO (Sept. 20, 2015, 10:24 AM), http://www.nationalmemo.com/fisa-court-has-only-rejected-10-of-20909-spying-requests-one-congressman-has-a-solution/ ("Between 2001 and 2012, the court heard 20,909 surveillance and property search warrants and rejected just 10.").

72. ROSENBACH & PERITZ, *supra* note 67, at 69; Ben Johnson, *Impeaching "Big Brother"?*,

there is still a debate as to whether the President had the legal authority to authorize surveillance, then Attorney General Alberto Gonzales clarified that President Bush was discontinuing the program in 2007.[73]

4. Electronic Communications Privacy Act of 1986

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA"), because emerging technologies threatened the right to privacy.[74] The ECPA codified the government's legal authority to access domestically stored electronic communications, and has since expanded to include wire communications due to the USA Patriot Act amendment.[75] Typically, when an individual sends an electronic communication, the message is temporarily stored within a local network server or an Internet service provider server before being opened by the intended recipient.[76] Thus, ECPA is the appropriate vehicle to retrieve wire and electronic communications that are stored, rather than Title III, because the concept of "interception" is not applicable while the message is temporarily in storage and not in current transmission.[77] Once the government realizes a stored

FRONTPAGEMAGAZINE.COM (Dec. 21, 2005), http://archive.frontpagemag.com/readArticle.aspx?ARTID=6171 ("The *New York Times* revealed in a front page story December 16th that the Bush administration allowed the NSA to wiretap calls involving someone resident in the United States (N.B.: not necessarily an American *citizen*) without seeking a court warrant, as long as at least one party to the call was overseas and the American was a known al-Qaeda contact.") (original emphasis).

73. ROSENBACH & PERITZ, *supra* note 67, at 70.

74. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-22 (1986); Solove, *supra* note 46, at 1277 ("House Report 647 noted that 'legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.' Additionally, Senate Report 541 mentioned that threats to privacy in these new communications media 'may unnecessarily discourage potential customers from using innovative communications systems.'").

75. 18 U.S.C. § 1825(2)(a)(ii) (2000).

76. ADAMS & BLINKA, *supra* note 62, at 43–44.

77. *Id.* at 45; Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994) ("The E-mail in issue was in 'electronic storage.' Congress' use of the word 'transfer' in the definition of 'electronic communication,' and its omission in that definition of the phrase 'any electronic storage of such communication' (part of the definition of 'wire communication') reflects that Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'"). *Compare* 18 U.S.C. § 2510(1) (2012) ("'[W]ire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . ."), *with* 18 U.S.C. § 2510(12) ("'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part

communication exists and it would like to access the information, the government must obtain a Fourth Amendment warrant.[78]

5. Communications Assistance for Law Enforcement Act

When telephone carriers switched from analog to digital networks in the 1980s, law enforcement complained of chaos and difficulty accessing various types of network structures due to technological advances.[79] After the FBI proved this difficultly created a significant problem,[80] Congress responded by passing the Communications Assistance for Law Enforcement Act ("CALEA") in 1994, which required all U.S. telecommunication carriers to redesign their network structures so that law enforcement officers could access both content and call-identifying information in a timely manner.[81] In addition, CALEA provides further legal protection against the unauthorized interception of communications for new technologies not covered under Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[82]

Almost ten years later, Congress addressed an apparent shortcoming of CALEA, which previously required only limited types of communication providers to comply with the statute.[83] In 2005, Congress expanded the term "telecommunications carriers" under the Act to include broadband-service providers and interconnected VoIP providers, such as Skype, after law enforcement

---

by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . but does not include . . . any wire or oral communication . . . .").

78. ADAMS & BLINKA, *supra* note 62, at 45.

79. John Edwards, *The Instant Expert Guide to CALEA*, VOIP-NEWS (Jul. 11, 2012), http://web.archive.org/web/20120711144311/http://www.voip-news.com/feature/guide-calea-030608/.

80. 140 CONG. REC. 27,709 (1994) (statement of Rep. Don Edwards, Chairman of the H. Subcomm. on Civil Liberties and Civil Rights). The FBI submitted 183 cases from around the country where they were having problems carrying out wiretaps due to new technologies. *Id.*

81. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, § 103, 108 Stat. 4279 (codified at 47 U.S.C. § 1002(a)(1)–(4) (2012); Constance L. Martin, Note and Comment, *Exalted Technology: Should CALEA Be Expanded to Authorize Internet Wiretapping?*, 32 RUTGERS COMPUTER & TECH. L.J. 140, 144 (2005); Edwards, *supra* note 79.

82. *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties and the Administration of Justice of the H. Comm. on the Judiciary*, 99th Cong. 3, 4 (1986) (testimony of Sen. Patrick J. Leahy, Vice Chairman of the Sen. Select Comm. on Intelligence).

83. Edwards, *supra* note 79.

made additional requests due to the growth of computer-based communications.[84] Significantly, the FBI again compromised by agreeing to exempt instant messaging and email, which were not a vulnerability of great concern in 2004, from CALEA's expanded scope of coverage to get the law passed.[85]

6. The USA Patriot Act

After 9/11, the Bush administration realized the public leaned in favor of equipping law enforcement with the necessary authority to fight terrorism rather than constricting law enforcement to protect civil liberties.[86] Immediately following 9/11, the National Commission on Terrorism reiterated this sentiment by stating that "[p]riority one is to prevent terrorist attacks."[87] As a result, the USA Patriot Act was passed in 2001, which seeks to use the full breadth of law enforcement authority to gather intelligence on terrorist plans and methods.[88] It is therefore known as "one of the key legislative tools in our fight against terrorism" because it updated surveillance laws to accommodate technological advancements.[89] As the Patriot Act relates to electronic surveillance, it revamped Title III by adding predicate offenses including terrorism-related offenses, chemical weapon crimes, and computer-based crimes.[90]

---

84. *Id.*

85. *Id.*; *Communications Assistance for Law Enforcement Act: Frequently Asked Questions*, ELECTRONIC FRONTIER FOUND., https://w2.eff.org/Privacy/Surveillance/CALEA/?f=faq.html (last visited Dec. 15, 2016); Martin, *supra* note 81, at 169–70.

86. *See* Robert N. Davis, *Striking the Balance: National Security vs. Civil Liberties*, 29 BROOKLYN J. INT'L L. 175, 216 (2003).

87. STAFF OF THE S. COMM. ON FOREIGN RELATIONS, 107TH CONG., STRATEGIES FOR HOMELAND DEFENSE 5 (Comm. Print 2001). The National Commission on Terrorism is a congressionally mandated bi-partisan body that assesses U.S. laws, policies, and practices for preventing and punishing terrorism affecting U.S. citizens. RAPHAEL F. PERL, CONG. RESEARCH SERV., RS 20598, NATIONAL COMMISSION ON TERRORISM REPORT: BACKGROUND AND ISSUES FOR CONGRESS 2 (2001); *see also* Act of Oct. 22, 1998, Pub. L. No. 105-277, § 591, 112 Stat. 2681.

88. USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (codified as amended in scattered sections of the U.S.C.) ("An act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."); STAFF OF THE S. COMM. ON FOREIGN RELATIONS, 107TH CONG., STRATEGIES FOR HOMELAND DEFENSE 5 (Comm. Print 2001).

89. Martin, *supra* note 81, at 157.

90. ADAMS & BLINKA, *supra* note 62, at 19.

For all the alleged good that the Patriot Act accomplished, such as improving communication between the intelligence and law enforcement communities, those in favor of protecting civil liberties vehemently oppose it.[91] In 2002, Gerald Waldron, a former litigator for groups opposed to CALEA, said, "I see the Patriot Act as in some ways an extension of CALEA. Law enforcement is trying to get things they couldn't get under CALEA," such as roving wiretaps.[92] The Patriot Act also amended ECPA by expanding the types of non-content information the government could access from just telecommunications data to records of all electronic communication providers and remote computer services.[93] Finally, the Patriot Act broadened FISA's scope to include investigations when foreign intelligence gathering is "a significant purpose," rather than the primary purpose as was previously required.[94]

II. ANALYSIS

A. Fourth Amendment Constitutional Law

Merriam-Webster's dictionary defines "privacy" as "the quality or state of being apart from company or observation" and the "freedom from unauthorized intrusion."[95] The word "privacy," however, never actually appears in the U.S. Constitution.[96] Despite this implied assertion, the makers of our Constitution:

---

91. USA Patriot Act, 50 U.S.C.S. § 1806(k), 1825(k)(1) (2012); Beryl A. Howell, *Seven Weeks: The Making of the USA Patriot Act*, 72 GEO. WASH. L. REV. 1145, 1146–47 (2004); Davis, *supra* note 86, at 218–19.

92. George A. Chidi, Jr., *Privacy, Money Issues Delay New FCC Wiretapping Rules*, IT WORLD (Jan. 14, 2002), http://www.itworld.com/article/2793070/business/privacy—money-issues-delay-new-fcc-wiretapping-rules.html.

93. ADAMS & BLINKA, *supra* note 62, at 46. As a result of changing FISA's language from "purpose" to "a significant purpose," the USA Patriot Act "eliminated any justification for the FISC to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses." Solove, *supra* note 46, at 1291 (quoting *In re* Sealed Case, 310 F.3d 717, 735 (FISA Ct. Rev. 2002)). "Only if the 'government's sole objective [is] merely to gain evidence of past criminal conduct . . . the application should be denied.'" *Id.*

94. Solove, *supra* note 46, at 1290–91.

95. *Privacy*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/privacy (last visited Dec. 15, 2016).

96. Henry F. Fradella, Weston J. Morrow, Ryan G. Fischer, & Connie Ireland, *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38

> conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[97]

More specifically, the Fourth Amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[98]

The Supreme Court first discussed Fourth Amendment privacy protections in *Olmstead v. United States* in 1928. As decided in *Olmstead*, if the government intrudes into an individual's spatial privacy, it is required to obtain a warrant based on probable cause.[99] Almost forty years later in *Katz v. United States*, the Supreme Court expanded privacy protections to encompass people, and not just places.[100] Notably, Justice Harlan provided a two-part test in the concurrence of *Katz* that has now been adopted as the contemporary framework for analyzing Fourth Amendment protections: first, the person seeking Fourth Amendment protection must "exhibit an actual (subjective) expectation of privacy;" and second, the subjective expectation of privacy needs to be "one that society is prepared to recognize as 'reasonable.'"[101] If there is no reasonable expectation of privacy, then there is no Fourth Amendment protection, and thus, the

---

AM. J. CRIM. L. 289, 291 (2011).

97. *Id.* (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

98. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

99. Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 9 (2013).

100. *Id.* at 10.

101. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protections*, 73 MINN. L. REV. 583, 593 (1989).

"search" does not require a warrant based on probable cause.[102] In an era where technology is constantly expanding, deciding whether an expectation of privacy is reasonable has created a great deal of debate and ambiguity.[103]

1. Subjective Expectations of Privacy

To satisfy the first part of the *Katz* test, an individual must demonstrate that he personally had "an actual (subjective) expectation of privacy."[104] For example, in *United States v. Chadwick*, several men placed drugs in a solid footlocker, which was sealed with both a regular trunk lock and padlock.[105] After arresting the owners of the footlocker, the government opened the footlocker without receiving consent from the owners and without obtaining a search warrant.[106] The Court concluded "by placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination."[107] Therefore, agents were required to obtain a search warrant before they could constitutionally open the footlocker.[108] Additionally, in *Bond v. United States*, a bus passenger exhibited an intent to preserve the privacy of his carry-on luggage when he used an opaque canvas bag and placed the bag directly above him.[109] Although the bag could be subjected to casual touching and handling, the petitioner did not expect the bag to be physically manipulated by police in an exploratory manner.[110] Consequently, the court held the border patrol agent violated the passenger's Fourth Amendment rights when the officer squeezed the passenger's bag.[111]

---

102. Smith v. Maryland, 442 U.S. 735, 738 (1979).
103. *See* Mitchell Waldman, Annotation, *Expectation of Privacy in Internet Communications*, 92 A.L.R. 5th 15, § 2(a); 68 AM. JUR. 2D *Searches and Seizures* § 5 (2015).
104. *Katz*, 389 U.S. at 361.
105. United States v. Chadwick, 433 U.S. 1, 3–4 (1977).
106. *Id.* at 4.
107. *Id.* at 11.
108. *Id.*
109. Bond v. United States, 529 U.S. 334, 336, 338 (2000).
110. *Id.* at 338–39.
111. *Id.* at 335, 339.

Encryption is analogous to the locker in *Chadwick* or closing the telephone booth door in *Katz*.[112] Just as the locker kept its contents sealed except to those with the key, encryption similarly keeps a communication private by unrecognizably scrambling the content, which can only be descrambled by an authorized key.[113] It would therefore be illogical to deny an expectation of privacy to a person who uses encryption on his computer before sending a document, when sending a sealed letter in an envelope or keeping an item in a lockbox suffices to establish an expectation of privacy.[114] In addition, the mere fact that an encrypted document is nearly impossible to decipher without the proper key further demonstrates that the individual who encrypted the document expects that the document will remain private, except to those with a corresponding key.[115] Therefore, in situations where the court determines an individual maintains a subjective expectation of privacy, such as when an individual chooses to use encryption, the Fourth Amendment requires law enforcement to secure a warrant, and not just probable cause, before a search can be completed.[116]

2. Expectations of Privacy that Society Recognizes as Reasonable

Despite an individual's subjective expectation of privacy, the Supreme Court must also determine whether society is ready to find a certain privacy expectation "reasonable."[117] For example, one may have a legitimate expectation in keeping the contents of his luggage private, but that subjective expectation is limited by society if a

112. *See Chadwick*, 433 U.S. at 4; Katz v. United States, 389 U.S. 347, 361 (1967); Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 J. TECH. L. & POL'Y 123, 168 (2002).

113. Sean J. Edgett, Comment, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339, 350 (2003).

114. *Id.* (analogizing the reasonable expectation of privacy achieved through encryption to someone locking an item in a "briefcase, home, or trunk").

115. *Id.* at 365. *But see* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?*, 33 CONN. L. REV. 503, 523 (2001) (explaining the reasonableness of an expectation of privacy when using encryption depends on the strength of encryption, which begs the question: "How strong an encryption is strong enough for a person to have a reasonable expectation that it will remain private?").

116. Edgett, *supra* note 113, at 364.

117. Kerr, *supra* note 115, at 507.

customs officer decides to inspect the luggage at an international border.[118] This particular example demonstrates a scenario where society has refused to recognize a reasonable expectation of privacy, supported by the fact that permissible inspection of containers by border inspectors has been codified.[119] Although "the Fourth Amendment grants protection to the owner of every container that conceals its contents from plain view[,] . . . the protection afforded by the Fourth Amendment varies in different settings."[120]

Another example where Courts have distinguished expectations of privacy is their differing treatment of postcards and sealed letters.[121] Although both instruments are used to deliver communications, postcards present numerous opportunities for their messages to be read by others before arriving to their intended recipients, thereby disqualifying postcards from any reasonable expectation of privacy.[122] On the contrary, courts have afforded sealed letters a reasonable expectation of privacy ensuring that the police will not intercept the letter's message.[123] Once the letter is delivered, however, the sender's expectation of privacy terminates.[124]

In regard to technology and surveillance, the Court often considers whether an expectation of privacy is reasonable by balancing citizens' right to feel secure with law enforcement's need to investigate a situation effectively and efficiently.[125] Proponents of

118. United States v. Ross, 456 U.S. 798, 822–23 (1982).

119. 19 U.S.C. § 482 (2012).

120. *Ross*, 456 U.S. at 822–23 (holding that although an individual may expect privacy in his luggage, his expectation of privacy is irrelevant when the luggage is checked by a customs officer as the traveler crosses into another country). The court reasoned through analogy:

> For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.

Id. at 822.

121. *See* Scott A. Sundstrom, Note, *You've Got Mail! (And The Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2082–84 (1998).

122. *See generally* Robert L. McArthur, *Reasonable Expectations of Privacy*, 3 ETHICS & INFO. TECH. 123–28 (2001).

123. Sundstrom, *supra* note 121, at 2084.

124. United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005) (citing United States v. King, 55 F.3d 1193, 1195–96 (6th Cir. 1995)).

125. Daniel T. Pesciotta, Note, *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st*

civil liberties would ideally like all citizens to be "free from secret government surveillance at all times."[126] This ideology is unfeasible, however, in a world that also must maintain "adequate levels of effective law enforcement and national security."[127]

Although the Court has used the *Katz* framework for several electronic surveillance cases,[128] it has not applied *Katz* to the Internet, or more specifically, encryption.[129] Nonetheless, other courts have issued opinions regarding the expectations of privacy afforded to text messages and emails.[130] For example, a few courts, most notably the Ninth Circuit, ruled that individuals do in fact hold an expectation of privacy in their phones and text messages.[131] Similarly, some courts have analogized sealed letters to emails, noting that both are sent and lie private until opened.[132] Both letters and emails maintain an expectation of privacy until the messages are accessed.[133] Based on the inconclusive and sparse court rulings, the Ninth Circuit acknowledged "the recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored."[134] It is evident that as technology develops and changes, so too must reasonable expectations of privacy in order to adequately balance competing interests.[135] Even without a Court ruling on

Century, 63 CASE W. RES. 187, 200 (2012); Brenner, *supra* note 112, at 166.

126. Pesciotta, *supra* note 125, at 224–25.

127. *Id.*

128. United States v. Jones, 132 S. Ct. 945, 950 (2012) (holding the Fourth Amendment protected the defendant from a warrantless GPS search of his vehicle); United States v. Knotts, 460 U.S. 276, 280–81, 285 (1983) (rejecting Fourth Amendment challenges to a beeper that had been placed in a container of chloroform since it only allowed law enforcement to monitor the location of the container).

129. *See* Pesciotta, *supra* note 125, at 215.

130. *Individual Lacks Expectation of Privacy in Text Messages or Numbers Dialed, No Standing to Object to Subpoena*, BLOOMBERG (Sept. 19, 2011), http://www.bna.com/individual-lacks-expectation-of-privacy-in-text-messages.

131. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2485 (2014); Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 910 (2008), *rev'd sub nom*, City of Ontario v. Quon, 560 U.S. 746, 763 (2010).

132. United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996).

133. *Id.*

134. *Quon*, 529 F.3d at 904.

135. *See generally* Brenner, *supra* note 112.

encryption, some scholars suggest that society, in some instances, would be ready to recognize such an expectation of privacy.[136]

B. The Path to CALEA

To enact CALEA, lawmakers and relevant parties were diligent and cooperative in finding a way to balance the interests of law enforcement with those of the telecommunications industry and the civil liberties of Americans.[137] The goal, after all, was not to reverse telecommunications growth, but to ensure the industry's cooperation with law enforcement as the industry developed new technology.[138] Therefore, one of law enforcement's biggest compromises in CALEA was to explicitly permit subscribers to use encryption while also not requiring communication carriers to decrypt communications.[139] Communication carriers are only required to decrypt communications if they have the means to do so.[140] In fact, no section of CALEA prohibits a carrier or technology company, such as Apple, from "deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access."[141]

With law enforcement "increasingly handcuffed in preventing and solving crimes due to the encryption that protects the perpetrators,"[142]

136. David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2223, 2232 (2009) ("Cloud computing has added an 'anywhere-access' function to Internet usage which provides a reasonable justification for storing private materials in the cloud. . . . Certainly in many ways the Internet remains, as one court put it, 'an indisputably, public medium,' but even that court qualified its statement with an acknowledgment that measures could be taken to protect information stored there. The evolving, anywhere-access function of the Internet makes the cloud a public medium into which private items are increasingly - and reasonably - placed, interacted with, and stored.").

137. *See* H.R. REP. NO. 103-827, pt. 1, at 13 (1994).

138. *Id.* at 13, 15.

139. 47 U.S.C. § 1002(b)(3) (2012) (specifying that "a telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication"); Lillian R. BeVier, *The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T*, 51 STAN. L. REV. 1049, 1075, 1079 (1999).

140. Jeffrey Yeates, *CALEA and the RIPA: The U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World*, 12 ALB. L.J. SCI. & TECH. 125, 141 (2001).

141. H.R. REP. NO. 103-827, pt. 1, at 24 (1994).

142. *Scripps News/Toronto Star Investigation Reveals How Encryption Technology Hampers Law*

the FBI currently suggests amending CALEA to require compliance from Internet communication providers and exclude the encryption exception found in the 1994 version of the Act.[143] Valerie Caproni, general counsel for the FBI, stated, "We're not talking [about] expanding authority. We're talking about preserving our ability to execute our existing authority in order to protect the public safety and national security."[144] Essentially, law enforcement would be "prevent[ing] the erosion of their investigative power," which encryption currently challenges.[145]

Although the FBI conceded on encryption when CALEA was originally passed in 1994, the FBI is now fighting to include an encryption provision that would again enable them to effectuate authorized wiretap orders.[146] Those opposed to expanding CALEA maintain that mandatory encryption key access is not within CALEA's reach[147] because such an expansion of CALEA will "fundamentally chang[e] how the government regulates technology."[148] Opponents also argue that by requiring a back door to encryption, the FBI is arguing for weaker encryption when they should actually be helping Americans increase device security to prevent breaches.[149]

Enforcement, BUS. JS. (Nov. 5, 2015, 9:00 AM), http://www.bizjournals.com/prnewswire/press_releases/2015/11/05/CL48792; *see* Cory Bennett, *Apple Couldn't Comply with Warrant Because of Encryption*, HILL (Sept. 8, 2015, 9:42 AM), http://thehill.com/policy/cybersecurity/252896-apple-rebuffed-warrant-because-of-encryption.

143. Scott Brady, Note, *Keeping Secrets: A Constitutional Examination of Encryption Regulations in the United States and India,* 22 IND. INT'L & COMP. L. REV. 317, 333 (2012); Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y. TIMES (May 7, 2013), http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?ref=charliesavage&_r=0.

144. Brady, *supra* note 143, at 334; Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, N.Y. TIMES (Sept. 27, 2010), http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all&_r=0.

145. Brady, *supra* note 143, at 334.

146. *Id.* at 333.

147. *Id.*

148. Christopher Soghoian, *CALEA and Encryption*, SLIGHT PARANOIA BLOG (Sept. 28, 2010, 3:59 PM), http://paranoia.dubfire.net/2010/09/calea-and-encryption.html.

149. Cindy Cohn, *EFF Response to FBI Director Comey's Speech on Encryption*, ELEC. FRONTIER FOUND. (Oct. 17, 2004), https://www.eff.org/deeplinks/2014/10/eff-response-fbi-director-comeys-speech-encryption.

III. PROPOSAL

Although no simple comprehensive solution exists on which parties on either side of the issue will unanimously agree, neither side's policies should go unchecked. As the debate currently stands, the FBI and NSA seem to be the only side receiving backlash, while technology firms have resisted compromise by deeming potential solutions counter-productive to their interests.[150] Technology firms certainly have a strong position in defending secured communications,[151] but their policies should not dominate, especially considering the potentially severe and adverse side effects for law enforcement and the public. Congress should therefore propose an amendment to CALEA that prevents technology companies from automating encryption on smartphones without the ability to decrypt the same data. More specifically, if a user opts into encryption, technology firms should be mandated to develop the requisite technology to decrypt text messages and emails upon receiving a valid warrant or court order.

A. Does Mandated Encryption Fit Within Katz?

A discussion of how courts may analyze mandated encryption under *Katz* is appropriate to determine whether an individual has an expectation of privacy for his encrypted smartphone data. As mentioned previously, to have a defensible expectation of privacy, an individual must have a subjective expectation of privacy that society is prepared to accept as reasonable.[152] If either one or both of the elements required under *Katz* fail, law enforcement can conduct a search without a warrant based on probable cause.[153]

150. *See* Bennett, *supra* note 142. "Technologists have pushed back, arguing any such requirement would weaken encryption worldwide, lowering cybersecurity standards and leaving customers exposed to cyber spies and cyber criminals." *Id.*

151. *Id.*

152. *See infra* Part II.A.1; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

153. Smith v. Maryland, 442 U.S. 735, 738 (1979).

1. Under Apple's New Encryption Systems, Do Smartphone Owners Have A Subjective Expectation of Privacy in their Electronic Communications?

Part one of *Katz*'s two-part test requires an individual to maintain an actual, subjective expectation of privacy.[154] Arguably, under Apple's encryption system on iOS 8 devices, courts may no longer recognize an individual's subjective expectation of privacy in his communications or data on his smartphone if an individual is unaware Apple is encrypting his data.[155] With Apple's iOS 8 operating system, all communications are now automatically encrypted and inaccessible by Apple simply by using an iPhone with a passcode.[156] In contrast, Apple's previous operating systems required users who wanted secure, unbreachable encryption to download additional software or use a messaging application that utilized encryption, such as WhatsApp.[157] If an iPhone user is unaware of the automated encryption software utilized when he establishes a passcode, his phones could be analogous to the locker in *Chadwick*, except one lock—the passcode—exists rather than two.[158] If the user is aware of Apple's additional security, the password and encryption would be more comparable to *Chadwick*'s double-lock, where respondents believed the locker's contents would remain free from public examination.[159]

If individuals want to keep their communications private by encrypting their data, then nothing should stop them from doing so, and courts should appropriately find that an individual has a legitimate subjective expectation of privacy.[160] However, if a user lacks knowledge of Apple's new encryption software that makes it

154. *Katz*, 389 U.S. at 361.

155. *Id.*

156. Ken Gude, *The FBI is Dead Wrong: Apple's Encryption Is Clearly in the Public Interest*, WIRED (Oct. 17, 2014, 6:30 AM), http://www.wired.com/2014/10/fbi-is-wrong-apple-encryption-is-good/.

157. David Schuetz, *A (Not So) Quick Primer on iOS Encrytpion*, DARTHNULL.ORG (Oct. 6, 2014), http://www.darthnull.org/2014/10/06/ios-encryption; *End-to-End Encryption*, WHATSAPP, https://www.whatsapp.com/faq/en/general/28030015 (last visited Dec. 15, 2016).

158. *See* United States v. Chadwick, 433 U.S. 1, 11 (1977).

159. *See id.*

160. *See id.*

mathematically impossible for Apple to unlock an iPhone's operating and encryption systems, then the court may potentially find the user did not subjectively believe that his information was encrypted and entirely inaccessible. Nonetheless, a court is exceedingly more likely to find any smartphone owner, especially one whose phone requires a passcode to access, maintains a subjective expectation of privacy in the phone's contents.[161]

2. Is Society Prepared to Recognize a Privacy Expectation in Electronic Communications?

The second step taken from *Katz* requires that an expectation of privacy be recognized by society as reasonable.[162] Most often, courts determine this analysis by weighing a citizen's right to privacy and his need to feel secure against the legitimate needs of law enforcement.[163] Thus, police activity may not constitute a "search" if it seems "to invade relatively less significant privacy interests" and promotes a legitimate governmental interest.[164] The appropriate analysis applied to Apple's new encryption system is whether the encrypted communications, specifically email and text, have the same privacy interest as other traditional communications, such as postcards and sealed letters, and whether society is ready to protect those privacy interests at the cost of less effective law enforcement investigations.[165]

When thinking about the purpose of text messages, the most common use seems to be for casual, yet sometimes personal, conversation. Although not a perfect comparison, text messages are most categorically similar to the informal use of a postcard, which

161. *See id.*; Riley v. California, 134 S. Ct. 2473, 2493 (2014).

162. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

163. Pesciotta, *supra* note 125, at 200; *see*, *e.g.*, Terry v. Ohio, 392 U.S. 1, 20–22 (1968).

164. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 729; *Riley*, 134 S. Ct. at 2485.

165. Ryan A. Ray, *The Warrantless Interception of Email: Fourth Amendment Search or Free Rein for the Police?*, 36 RUTGERS COMPUTER & TECH. L.J. 178, 199–200 (2010). *But see* Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 503–04 (2012).

are not granted a reasonable expectation of privacy.[166] This categorization is drawn more distinctively when comparing texts to more formal mediums of communications such as emails. Unlike text messages, emails are the proper means to send more delicate matters, for instance, a business's financial records or an individual's medical records. Consequently, emails are comparable to sealed letters.[167] For both postal mail and emails, the envelope information, such as the "to" and "from" address, is not protected while the communication's contents are safeguarded.[168] In further applying the analogy of sealed letters, once an individual opens an email, his expectation of privacy is similarly terminated.[169] Therefore, an email is likely to have stronger privacy interests when compared to traditional forms of communication than a text message.

Additionally, court decisions discussing whether "reasonable expectations of privacy" exist have not always been congruent with society's perceptions.[170] Since encrypted text messaging imposes a significant setback for police investigations, the court should consider additional factors to determine whether such a privacy expectation is reasonable.[171] For example, the FBI or NSA's argument that encrypting text messages puts the public's safety at

166. *See* McArthur, *supra* note 122, at 127.

167. Ray, *supra* note 165, at 202. *But see* McArthur, *supra* note 122, at 127 (analogizing e-mails to postcards, "where there are numerous opportunities for the message to be read by others on its way to its intended recipient").

168. Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1049–50 (2008).

169. United States v. Jones, 149 Fed. Appx. 954, 959 (11th Cir. 2005) (citing United States v. King, 55 F.3d 1193, 1195–96 (6th Cir. 1995)).

170. Slobogin & Schumacher, *supra* note 164, at 733–34 (stating that most people disagree with the ruling in *United States v. Miller*, 425 U.S. 435 (1976), that when one gives information to a bank, they assume the risk that the information will be turned over to the government).

171. *Id*. at 754. Slobogin and Schumacher described Professor LaFave's argument:

> [T]he Court probably does not really believe that a person feels free to leave when confronted by a uniformed police officer, but that its holdings to the contrary can still be justified on the ground that, as a matter of policy, the police "should be allowed 'to seek cooperation, even where this may involve inconvenience or embarrassment for the citizen, and even though many citizens will defer to this authority of the police because they believe—in some vague way—that they should.'"

Id. at 754 (quoting Wayne R. LaFave, *Pinguitudinous Police, Pachydermatous Prey: Whence Fourth Amendment "Sizures"?*, 1991 U. ILL. L. REV. 729, 741 (quoting MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE § 110.1, commentary at 258 (1975))).

risk could be a legitimate interest that the court would consider in determining whether encrypted texts maintain a reasonable expectation of privacy.[172]

Despite these arguments, with our nation currently in the "post-Snowden" era, it is unlikely that society would actually reject individuals having a reasonable expectation of privacy in any aspects of their phone, including text messages and emails.[173] Even when an individual believes the main goal of the criminal justice system is to convict the guilty, individuals are not willing to give up their privacy rights to effectively prosecute the guilty.[174] Consequently, a warrant would be required for law enforcement to access encrypted text messages and emails, which is the current operating procedure for law enforcement agencies.[175]

B. Amending CALEA

Regardless of law enforcement's compliance with *Katz*, agencies lack the capability to access encrypted data on Apple's new software.[176] Currently, one of law enforcement's only options to access encrypted communications on smartphones is to purchase expensive computers—with taxpayer money—that *may* successfully carry out a brute force attack.[177] Therefore, a compromise should be negotiated between technology firms and law enforcement agencies to balance competing interests.

President Obama commented during a 2016 interview that he favored finding a solution supporting law enforcement.[178] Yet, when

172. Comey, *supra* note 25.

173. Gude, *supra* note 156.

174. Slobogin & Schumacher, *supra* note 164, at 772–73.

175. Danny Yadron, Spencer Ackerman & Sam Thielman, *Inside the FBI's Encryption Battle with Apple*, GUARDIAN (Feb. 18, 2016), https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple.

176. *Id.*

177. It can take as little as thirty minutes to correctly guess a four-digit password combination, but up to five years for a six-digit alphanumeric password containing lower-case letters and numbers. Selyukh, *supra* note 33.

178. Michael D. Shear, *Obama, at South by Southwest, Calls for Law Enforcement Access in Encryption Fight*, N.Y. TIMES (Mar. 11, 2016), http://www.nytimes.com/2016/03/12/us/politics/obama-heads-to-south-by-southwest-festival-to-talk-about-technology.html.

draft legislation was released early that same year, the technology community fiercely opposed it because it would introduce vulnerabilities in encryption.[179] With the CALEA framework already in existence, one possible solution is an amendment requiring carriers who offer encryption to also have the capability to decrypt requested data or specific communications, such as text messages, when served with a valid warrant or court order.

In 1994, during the CALEA committee hearings, Clinton Brooks, an assistant to the Director of the NSA, said the following words that still ring true today, "We conclude that it would be irresponsible for the government to promulgate excellent encryption for secure communications and privacy that would preclude law enforcement and national security authorities from protecting our Nation."[180] More recently, Sally Yates and James Comey stated that because of the advances in electronic communication "the Government has lost ground in its ability to execute court orders on communications not covered by CALEA … we must work … to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate."[181] As illustrated in the floor debate for CALEA in 1994, the competing concerns included privacy protection, law enforcement capabilities, and the telecommunication industry's freedom to advance technologically.[182] In the past, Congress stepped in on two occasions prior to CALEA being enacted to preserve an appropriate balance between privacy and law enforcement as telecommunications technology continued to

179. Daniel Castro, *The One Change That Would Make the Burr-Feinstein Encryption Bill Tenable*, HILL (Apr. 19, 2016, 6:30 AM), http://thehill.com/blogs/pundits-blog/technology/276768-the-one-change-that-would-make-the-burr-feinstein-encryption.

180. *Communications and Computer Surveillance, Privacy and Security: Hearing Before the Subcomm. on Tech., Env't & Aviation of the H. Comm. on Sci., Space, and Tech.*, 103d Cong. 28 (1994) (statement of Clinton Brooks, Special Assistance to the Director, National Security Agency).

181. Mark Bohannon, *Encryption Back Doors: Is There More to This Debate?*, OPENSOURCE.COM (Sept. 25, 2015), http://opensource.com/government/15/9/encryption-back-doors-debate.

182. 140 CONG. REC. 27,707 (1994) (statement of Henry Hyde, member of the H. Subcomm. on Civil Liberties and Civil Rights); *Id.* at 27,709 (statement of Rep. Don Edwards, Chairman of the H. Subcomm. on Civil Liberties and Civil Rights).

advance.[183] Currently, this same balance may need to be preserved by amending CALEA.[184]

The current scope of CALEA ensures that "telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it."[185] Although encryption was deliberately excluded when CALEA was passed in 1994, the debate as to whether that provision should now be excluded gathers strength.[186] A current example of a proposed CALEA amendment is a change that would require communications services that encrypt communications, such as text messages, to also have the technology to unscramble the message so that law enforcement can carry out their authorized wiretaps.[187] This could also be facilitated by Apple creating a software that would allow the FBI to try an unlimited number of brute force attacks without delays between passcode attempts.[188] Rather than pushing an improbable sweeping policy on encryption, a more focused proposal should be specific to companies who automate encryption for text messages on their system, such as Apple's "Data Protection" which separately, yet automatically, encrypts messages, mail, and contacts.[189]

Conversely, critics of expanding CALEA make a strong policy argument against requiring access to encrypted communications.[190] Opponents contend that in order to adequately protect businesses from large data breaches, businesses should use stronger security measures like robust encryption rather than weakening encryption by requiring backdoors.[191] It is critical to imagine, however, the unlikely scenario where a company sends large amounts of highly sensitive

183. H.R. REP. NO. 103-827, pt. 1, at 11–12 (1994).
184. *But see* Swire & Ahmad, *supra* note 9, at 473.
185. Soghoian, *supra* note 148.
186. Martin, *supra* note 81, at 158–60.
187. Soghoian, *supra* note 148.
188. *See* APPLE, INC., IOS SECURITY: IOS 9.3 OR LATER 12 (2016), https://www.apple.com/business/docs/iOS_Security_Guide.pdf.
189. *Id.* at 11.
190. *See generally* Cohn, *supra* note 149.
191. *Id.*

data over a text message.[192] Thus, advocating for robust encryption for email and text messages seems inappropriate when the result would more readily affect victims of unsolved crimes rather than the security of large companies. The effect of Apple throwing away the key, whereas before Apple maintained a key,[193] is even more objectionable since Apple already requires a search warrant based on probable cause before disclosing any customer's information.[194]

Importantly, just as CALEA did not expand law enforcement's authority in 1994,[195] neither would this proposed amendment seek to do so now.[196] Law enforcement agencies would still be required to obtain a warrant before being granted authority to access an individual's text messages or emails. It would simply extend CALEA's reach to encompass a lower security level of communications so that law enforcement can continue conducting effective surveillance on criminals despite changing and emerging technologies.[197] Additionally, amending CALEA to encompass encryption regulations would only give critics of CALEA more leverage to add other provisions to the amendment that would favor greater privacy protections.[198] By enacting a CALEA amendment that seeks to protect the public's safety by reinforcing law enforcement's access to electronic communications conducted on smartphones, privacy advocates can continue to maintain and

192. *But see* Gude, *supra* note 156. The author suggests that such a scenario is not far-fetched:

> It is possible to construct a hypothetical scenario in which the only evidence of criminal activity is stored on a suspect's personal device, consists only of data not backed up in cloud storage, and is not in the possession of third parties like telecommunications carriers or app developers. But none of the criminal cases cited by Comey meet that hypothetical because in real life those instances would be extremely rare and far outweighed by the clear public benefit of preventing the very real threat of a large-scale data breach that could affect millions of Americans.

Id.

193. *See Apple's Commitment to Customer Privacy*, APPLE (Jun. 16, 2013), http://www.apple.com/apples-commitment-to-customer-privacy/.

194. *Privacy: Government Information Requests*, APPLE, https://www.apple.com/privacy/government-information-requests/ (last visited Dec. 16, 2016).

195. *See* Swire & Ahmad, *supra* note 9, at 421.

196. *Going Dark*, *supra* note 9, at 6–16.

197. Gene D. Park, *Internet Wiretaps: Applying the Communications Assistance for Law Enforcement Act to Broadband Services*, 2 J.L. & POL'Y FOR INFO. SOC'Y 599, 609 (2006).

198. *See* BeVier, *supra* note 139, at 1091.

promote electronic security in more compelling and critical circumstances such as business transactions.

CONCLUSION

One of Congress's greatest current challenges is "to balance the competing demands of law enforcement, privacy rights, and technological innovation."[199] Thus, as technology continues to develop, courts must use existing frameworks and Congress must adjust statutes to encompass emerging issues. With the recent government abuses and ever-present data breaches, technology firms have responded by mandating encryption on smartphones.[200] Although the "post-Snowden" society may appreciate this response, law enforcement agencies are handcuffed from adequately protecting the public from both stateside and international threats.[201] As a result of embracing such a strict stance in favor of privacy, society may be haunted by the negative consequences of protecting such a low security level of communication such as text messages from being accessed with a valid warrant or court order. Therefore, CALEA should be amended to require Internet service providers and telecommunication carriers who mandate encryption to also provide the means to decrypt certain data and communications when law enforcement has an authorized court order. Although the technology firms are strongly opposed to such legislation, Congress may have no choice but to weigh in on the matter by establishing a compromise through CALEA to balance competing interests between civil liberties, law enforcement needs, and public safety.[202]

---

199. Martin, *supra* note 81, at 159.

200. *See, e.g.*, Gude, *supra* note 156 (discussing Apple's increased encryption in response to data breaches).

201. *See generally* Aaron Homer, *The Director of the FBI Thinks Your iPhone's Encryption Protects Kidnappers, Terrorists and Pedophiles*, INQUISITR (Oct. 13, 2014), http://www.inquisitr.com/1538694/the-director-of-the-fbi-thinks-your-iphones-encryption-protects-kidnappers-terrorists-and-pedophiles/; *Scripps News/Toronto Star Investigation Reveals How Encryption Technology Hampers Law Enforcement*, *supra* note 142.

202. Martin, *supra* note 81, at 158–60.