UPDATES READY TO INSTALL: HOW CALIFORNIA'S ELECTRONIC COMMUNICATIONS PRIVACY ACT PROVIDES A BETTER FRAMEWORK FOR AGING FEDERAL PRIVACY LAWS

Comment

I. INTRODUCTION

As the internet continues to become further ingrained in everyday life, consumers are storing increasingly vast amounts of personal data with online service providers. The proliferation of social media websites and cloud computing services has resulted in vast treasure troves of personal information outside of an individual's physical control. Unfortunately, federal privacy laws have failed to keep pace with this trend.

In 2013, Edward Snowden, a former Booz Allen Hamilton contractor working for the National Security Agency (NSA), brought to light the extent that certain government agencies have been accessing personal information.[1] In particular, the NSA's "Prism" program allowed officials "to collect material including search history, the content of emails, file transfers and live chats."[2] Among the internet companies involved in this program were Yahoo, Google, Microsoft, Facebook, and Apple.[3] The fallout from the Snowden revelations marked a drastic change in the cooperation between these companies and governmental agencies.[4] These same internet companies are now pushing back against the NSA and other intelligence agencies in an effort to show consumers that they are protecting their information.[5] Companies like Google, Apple, and Microsoft are making it harder for intelligence agencies to intercept and read data that they process for customers, and at the same time, pushing back against these surveillance programs in court.[6]

However, even with this renewed charge by internet companies to push back against pervasive surveillance by governmental entities, current federal legislation has lagged behind in ensuring consumers' constitutional protections

---

1. Mark Mazzetti and Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html [http://perma.cc/U3QS-WRLK].

2. Glenn Greenwald and Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013, 3:23 PM), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [http://perma.cc/Y9CV-YNBY].

3. *Id.*

4. David E. Sanger, *New N.S.A. Chief Calls Damage From Snowden Leaks Manageable*, N.Y. TIMES (June 29, 2014), http://www.nytimes.com/2014/06/30/us/sky-isnt-falling-after-snowden-nsa-chief-says.html [http://perma.cc/RQ2J-C5YR].

5. David E. Sanger and Nicole Perlroth, *Internet Giants Erect Barriers to Spy Agencies*, N.Y. TIMES (June 6, 2014), http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html [http://perma.cc/MMA2-LRDC].

6. *Id.*

respected in this new digital age.[7] Federal law (the Electronic Communications Privacy Act of 1986 in particular) has "stagnated for nearly 30 years."[8] A few state legislatures—backed by the same internet companies once part of the NSA's intelligence programs—have moved to correct these deficiencies by enacting their own improved electronic communications privacy legislation.[9] Among these states is California and its recently enacted Electronic Communications Privacy Act.[10]

This comment provides an analysis of California's Electronic Communications Privacy Act (CalECPA) and its impact on Fourth Amendment protections with regard to consumers' digital information. Part II of this comment will provide an overview of the current body of judicial and federal legislative authority concerning Constitutional protections of stored internet data and electronic communications. Part III provides an analysis of the California Electronic Communications Privacy Act. Finally, part IV provides an analysis of possible changes to current federal privacy laws to close the gap between the federal Electronic Communications Privacy Act and the statutory framework that California has adopted.

II. THE FOURTH AMENDMENT AND STORED DIGITAL INFORMATION

The Fourth Amendment of the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[11]

Applying this constitutional right during the Founder's time may have been relatively straightforward, but application in modern times becomes more difficult when taking into account the intangible nature of digital data. For example, cloud storage, a growing internet service, allows an individual to store their files

---

7. Shahid Buttar, *California Leads the Way in Digital Privacy*, ELEC. FRONTIER FOUND. (Oct. 21, 2015), https://www.eff.org/deeplinks/2015/10/california-leads-way-digital-privacy [http://perma.cc/2PAV-Z2QB].

8. *Id.*

9. Kim Zetter, *California Now Has The Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015) https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ [http://perma.cc/H5LE-DC6T].

10. *Id.*

11. U.S. CONST. amend. IV.

on a service provider's servers.[12] "Cloud computing is the act of using global storage facilities to store information electronically and grant access to uploaded information using any electronic device from any location at any time."[13] Moreover, e-mails are also customarily stored on off-site servers. As these services become more pervasive in everyday life, the need to use them becomes more important than the potential risk to privacy for many individuals and businesses.[14] "[Most technology experts] predict that users will share and store information through remote server networks, rather than depend on information housed on personal and office computer hard drives."[15] In analyzing the Fourth Amendment in regards to data stored on an internet service provider's servers, it is important to first understand the history of the third party doctrine and its likely impact on digital privacy.[16]

A. *The Third Party Doctrine and Judicial Ambiguity*

In *United States v. Miller*, the United States Supreme Court found that documents held by a bank for Miller were exempt from Fourth Amendment protections.[17] Miller was under investigation for defrauding the government of tax revenues.[18] In proving its case, the government sought to use bank records on file with Miller's bank.[19] However, the subpoenas used to acquire the bank records were deficient.[20] Miller objected and attempted to suppress the records on the grounds that his Fourth Amendment rights were violated when the government acquired records from a third party through a defective subpoena.[21]

In coming to its conclusion, the Court held that "no interest legitimately protected by the Fourth Amendment is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy."[22] The Court defined the zone of privacy as "the security a man relies upon when he places himself or his

---

12. Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need A Warrant for That": The Fourth Amendment,* Riley's *Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154, 161 (2014).
13. *Id.*
14. *Id.* at 162.
15. *Id.* at 161.
16. *Id.* at 166.
17. United States v. Miller, 425 U.S. 435, 444 (1976).
18. *Id.* at 436.
19. *Id.* at 437.
20. *Id.*
21. *Id.*
22. *Id.* at 440.

property within a constitutionally protected area."[23] The court reasoned that because these were not Miller's "private papers," and because Miller had no ownership or possession of them, they were not subject to Fourth Amendment protections.[24] "The Court, adopting an assumption of the risk rationale, stated that a 'depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.'"[25]

In *Smith v. Maryland*, the Supreme Court used the third party doctrine established in *Miller* and held that the installation and use of a pen register on a telephone was not a search under the Fourth Amendment.[26] The Court found that the exposure of the information to the service provider and the fact that no communication was involved illustrated no reasonable expectation of privacy.[27] These two cases have had a substantial impact on loosening the protections under the Fourth Amendment for digital technologies.[28] "The third-party doctrine has been used as the legal basis for the government's easy access to information stored by individuals or businesses contracting with third-party ISPs."[29] It has also allowed government access to cell-site data held by cellular telephone providers, stored Internet Protocol address information, and data files voluntarily transferred over closed peer-to-peer networks.[30]

However, the courts have recognized some restrictions on searches of communications technologies. In *Katz v. United States*, the Supreme Court held that the recording and listening of Katz's private communication using a public telephone violated his Fourth Amendment right.[31] The FBI had placed a listening device outside of the enclosed public phone booth and used it to record Katz's telephone conversations.[32] The government attempted to justify the electronic recording device by implying it had not physically intruded into the "area occupied" by Katz.[33] The government further stressed that no physical penetration of the booth occurred and "the fact that the telephone booth from which

---

23. *Miller*, 425 U.S. 440 (citing Hoffa v. United States, 385 U.S. 293).
24. *Id.* at 440–41.
25. Serafino, *supra* note 12, at 167.
26. *Id.*
27. *Id.* at 167.
28. *Id.* at 168.
29. *Id.*
30. *See* Serafino, *supra* note 12, at 168–69.
31. *See* Katz v. United States, 389 U.S. 347, 353 (1967).
32. *See id.* at 348.
33. *Id.* at 349.

[Katz] made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside."[34] However, the Court stated that the government's actions "violated the privacy upon which [Katz] justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment."[35] *Katz* broadened the "definition of what constitutes a search to account for technological advancements by holding that the Fourth Amendment protects intangible interests."[36]

In *United States v. Jones*, the Supreme Court held that the use of data gathered from a Global-Positioning-System (GPS) tracking device attached to a car was "search within the meaning of Fourth Amendment."[37] Jones, who was under suspicion for trafficking in narcotics, had a GPS tracking device placed on his car by the FBI.[38] The device was attached outside the parameters of the warrant that was obtained by government officials.[39] The Court held that this was a search under the Fourth Amendment because of the physical intrusion.[40] The Court explained that "the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."[41] It went on to state that "*Katz* did not repudiate that understanding."[42] "The key inquiry is how the Court characterizes the search, whether location-based (trespass) or situation-based (*Katz* test), and whether it believes an individual has a reasonable expectation of privacy in the information being revealed."[43] The Court states that "situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[44]

In *Riley v. California*, the Supreme Court addressed warrantless searches of data found in cell phones seized during an arrest.[45] *Riley* dealt with two consolidated cases involving the same motions to suppress data collected from cell phones seized

34. *Id.* at 352.
35. *Id.* at 353.
36. Serafino, *supra* note 12, at 165.
37. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012).
38. *See id.* at 402.
39. *See id.*
40. *See id.* at 404.
41. *Id.* at 406.
42. *Id.* at 406–07.
43. Bryan Davis, *Prying Eyes: How Government Access to Third-Party Tracking Data May Be Impacted by* United States v. Jones, 46 NEW ENG. L. REV. 843, 857 (2011).
44. *Jones*, 565 U.S. at 410.
45. *See* Riley v. California, 134 S. Ct. 2473 (2014).

during an arrest.[46] Both cases involved police seizing cell phones and subsequently searching the data held on each phone.[47] The government argued that the searches were justified under the search incident to arrest doctrine.[48]

The Court analyzed this argument under the two risks identified in all custodial arrests: (1) harm to officers, and (2) destruction of evidence.[49] The Court first determined that "digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[50] Therefore, the first risk was not present.

The government's primary argument involved the possible destruction of evidence present on the cell phones.[51] While the government conceded "that officers could have seized and secured their cell phones to prevent destruction of evidence," the possibility of remote wiping the data on cell phones was still present.[52] Additionally, it argued the possibility that cell phone locks, which render the data practically unreachable without a password, essentially amounts to destruction of evidence.[53] The Court, however, found these arguments unpersuasive.[54] The risk for destruction of evidence is primarily concerned with the physical device during the immediate arrest.[55]

The Court ultimately held that a search warrant was necessary for the police to search data held on the cell phones.[56] "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[57] The Court also stated that the sheer amount of data that a cell phone holds should prompt privacy concerns under the Fourth Amendment.[58] The Court reasons that the sheer capacity that a modern cell phone contains with the ability to store a broad range of different data is enough to prompt protections from unreasonable searches.[59] Furthermore, the Court addressed the

---

46. *See id.* at 2480–82.
47. *See id.*
48. *See id.* at 2484.
49. *See id.* at 2484–85.
50. *Id.* at 2485.
51. *See id.*
52. *Id.* at 2486.
53. *See id.*
54. *See id.*
55. *See id.* at 2486.
56. *See id.* at 2497.
57. *Id.* at 2489.
58. *See id.* at 2482.
59. *See id.* at 2490–91.

issue of cloud data accessible from cell phones.[60] Allowing a search of cloud data "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[61]

In light of these cases, one can see how difficult it is in applying precedence to emerging technologies which rapidly outpace the court's ability to address them. "Pursuant to the third party doctrine, an overwhelming number of courts have held that individuals have no reasonable expectation of privacy in information voluntarily disclosed to an ISP."[62] It has been argued that the third party doctrine should not apply to data stored on a service provider's servers because there is a reasonable expectation of privacy.[63] This expectation of privacy, however, can be undermined by service agreements in effect for various internet service providers.[64] The Court in *Riley* discusses cloud data access from cell phones but does not address accessing that data without the initial arrest and seizure of the phone.[65] Because the Supreme Court has not addressed all issues related to searches of digital technologies, jurisdictions have applied their own standards resulting in "inconsistent judicial outcomes."[66]

Based on the rapid advancement of technology, it is almost impossible for courts to address every available internet service. Furthermore, the diversity of internet services hinders courts from establishing easy rules that could be universally applied. Congress sought to address some of this ambiguity when it enacted the Electronic Communications Privacy Act in 1986.[67]

B. *The Electronic Communications Privacy Act: Last Year's Model*

The Electronic Communications Privacy Act (ECPA) was initially a response by Congress to "the emergence of wireless services and the digital era."[68] It was enacted in order to rebalance the scales between privacy and law enforcement needs because of the rapid advancement of new technologies such as cell phones,

---

60. *See* Shaun B. Spencer, *The Aggregation Principle and the Future of Fourth Amendment Jurisprudence*, 41 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 289, 290 (2015).

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

62. Serafino, *supra* note 12, at 171.

63. *See id.* at 171.

64. *See id.* at 162.

65. *See Riley*, 134 S. Ct. at 2491.

66. Davis, *supra* note 43, at 858.

67. *See* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L. J. SCI. & TECH. 65, 73 (1997).

68. *Id.*

pagers, and e-mail.[69] This concern was not only in response to civilian technological advances; rapid advancements in law enforcement surveillance technology and techniques prompted a concern for privacy.[70] Congress had become aware that these advances had made "it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others . . . ."[71] The bill was meant to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[72]

But just like Congress' original intent, the ECPA has itself become outdated with the rapidly advancing landscape of internet services.[73] "In drafting ECPA, Congress assumed that it would be adequate to extend to electronic communications the constitutional conclusion that underpinned Title III in 1968: that capture of electronic communications would not be an unreasonable intrusion if there were stringent ex parte judicial review before the fact, minimization during a search, and equally stringent adversarial review after the investigation had been completed."[74] In 1986, however, Congress did not foresee the incredible technical advances that would occur including the "interactive nature of the internet, with the rapid emergence of features such as home banking, telecommuting and even telemedicine . . . produc[ing] an environment in which many people spend hours each day 'on-line.'"[75] "In this context, to intercept all of a person's electronic communications means a lot more today than it did in 1968 or 1986."[76]

Take for example the increasingly mobile nature of banking. A survey prepared by the Consumer and Community Development Research Section of the Federal Reserve Board's Division of Consumer and Community Affairs found that in 2014, "eighty-seven percent of the U.S. adult population has a mobile phone" and "seventy-one percent of mobile phones are smart-phones (internet-enabled)."[77] This access to internet enabled smart-phones has led

69. *See id.* at 73–74.

70. *See id.*

71. S. Rep. No. 99-541, at 3 (1986).

72. *Id.* at 1.

73. *See* Dempsey, supra note 67, at 85.

74. *Id.*

75. *Id.* at 85–86.

76. *Id.* at 86.

77. Board of Governors of the Federal Reserve System, *Consumers and Mobile Financial Services 2015*, http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf (last visited Mar. 6, 2015) [http://perma.cc/6E7L-YCXK].

to an increase in online and mobile banking.[78] Compare this to 1984, where only five percent of households owned personal computers.[79] "Mobile computers are spreading faster than any other consumer technology in history."[80] When the ECPA was enacted, Congress did not foresee that every-day Americans would be walking around with what are essentially computers with access to a vast array of online information at the tip of their fingers. "Wireless smartphones and tablets allow the Internet and its digital affordances to flow into every hand, everywhere, in every circumstance."[81] Such ubiquitous access has spurned innovation and prompted businesses to offer a growing array of new services.[82]

The ECPA itself is incorporated into title 18 of the United States Code.[83] The statutes encompassed by the ECPA include the "Wiretap Act, 18 U.S.C. §§ 2511–2522; the Pen Register statute, 18 U.S.C. §§ 3121–3127; and the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–2711."[84] All three sections were amended to provide protection against unauthorized access; however, the scope and content of each section differs in what is protected.[85]

The changes made by Title 1 of the ECPA to the Wiretap Act, extended protections to "in-transit interception" of wireless voice communications and to non-voice electronic communications.[86] More specifically, the provisions deal with protecting the unlawful interception, attempt to intercept, or procurement of another person to intercept any wire, oral, or electronic communication.[87] The ECPA defines electronic communication systems as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[88] This provision was

78. *See id.*

79. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1560 (2004).

80. Antonio Regalado, *Mobile Computing Is Just Getting Started*, MIT TECH. REV., (Mar. 1, 2013), http://www.technologyreview.com/news/511766/mobile-computing-is-just-getting-started/ [http://perma.cc/M56J-6M63].

81. *Id.*

82. *See* Mulligan, *supra* note 79, at 1559–60.

83. *See id.* at 1565.

84. *Id.*

85. *See id.* at 1565–66.

86. *Id.*

87. *See* 18 U.S.C. § 2511 (2015).

88. 18 U.S.C. § 2510 (2015).

particularly important because it granted protections to e-mail and other forms of digital communications that previously may not have had them.[89] Law enforcement needs to "obtain a warrant-like order based on probable cause" to access e-mails in transit.[90] However, subsequent court decisions have put limitations on the amount of protections that the Wiretap Act provides.[91]

In *Fraser v. Nationwide Mutual Insurance Company*, the Court of Appeals for the Third Circuit addressed whether the changes made by Title 1 of the ECPA concerned stored communications, particularly stored e-mails.[92] Fraser was working as an independent insurance agent for Nationwide Mutual Insurance Company which subsequently terminated his employment.[93] Nationwide became concerned that Fraser was sending company secrets to competitors.[94] Because of this concern, Nationwide began a search of its main file server which contained all of Fraser's stored e-mails.[95] From the search, Nationwide deduced that Fraser was indeed disloyal and therefore terminated his employment.[96] Fraser claimed that this was a prohibited search and sued for "damages under the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. § 2510."[97] In analyzing the Title 1 issue, the court noted that "when Congress amended the Wiretap Act in 1986 (to create what is now known as the ECPA) to extend protection to electronic communications, it 'did not intend to change the definition of "intercept."'"[98] Since the e-mails were not "in transit" but rather stored on Nationwide's server, they could not be "intercepted" within the meaning of Title 1.[99] Essentially the court stated that unless Nationwide obtained the e-mail while it was being sent to the addressee, then Fraser cannot claim that Nationwide violated Title 1 by intercepting his e-mail if it was obtained from a stored state.[100] E-mails are frequently backed up and stored on servers by e-mail service providers.[101] "As the communication traverses the network, it leaves replicas of itself, in whole or in pieces, in the

89. *See* Mulligan, *supra* note 79, at 1566.
90. *Id.*
91. Mulligan, *supra* note 79, at 1585.
92. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113–14 (3d Cir. 2003).
93. *Id.* at 109.
94. *Id.* at 110.
95. *Id.*
96. *Id.*
97. *Id.*
98. *Id.* at 113.
99. *See id.* at 113–114.
100. *Id.* at 114.
101. *See* Mulligan, *supra* note 79, at 1563.

hands of any number of third parties."[102] Knowing this, if an entity wanted to bypass the protections found in Title 1 of the ECPA, they would simply wait for the e-mail to be sent and then try to acquire it after it has been stored on a third party file server. This would appear to be a major oversight by Congress, and the Court in *Fraser* notes this by stating, "while Congress's definition of 'intercept' does not appear to fit with its intent to extend protection to electronic communications, it is for Congress to cover the bases untouched."[103]

Title III of the ECPA addresses pen registers and trap and trace devices.[104] Prior to the passing of the ECPA, the holding in *Smith* meant that phone numbers were not covered by the Fourth Amendment.[105] Under the ECPA, an order is required to collect both outgoing and incoming phone numbers.[106] This was in direct response to the *Smith* holding.[107]

Finally, Title II of the ECPA addresses stored communications and encompasses the Stored Communications Act (SCA).[108] Here, Congress modeled the statute after the Right to Financial Privacy Act.[109] This is also where "Congress had the least guidance from the Court and where the technical differences between electronic data and voice communications are most pronounced."[110]

The SCA deals primarily with stored communications, or in other words, electronic communications not in transit.[111] "'Electronic storage' is defined as 'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,' and 'any storage of such communication by an electronic communication service for purposes of backup protection of such communication.'"[112] Section 2701 states that unless an exception in subsection (c) applies,

> whoever: (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents

---

102. *Id.*
103. *Fraser*, 352 F.3d at 114.
104. 18 U.S.C. § 3123 (2015); Mulligan, *supra* note 79, at 1566–67.
105. Mulligan, *supra* note 79, at 1566.
106. *Id.* at 1566–67.
107. *See id.*
108. 18 U.S.C. § 2701 (2015).
109. S. Rep. No. 99-541, at 3 (1986).
110. Mulligan, *supra* note 79, at 1567.
111. *See id.* at 1567.
112. *Id.* at 1568.

> authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished . . . ."[113]

Because of the exceptions,[114] the SCA essentially "provides two different levels of protections to the content of electronic communications."[115] To determine what level of protection is afforded, it must first be determined if the communication is held by an electronic communication service, a remote computing service, or neither.[116] An electronic communication service (ECS) is a service that "provides another with the ability to send or receive wire or electronic communications."[117] A remote computing service (RCA), on the other hand, "provides a service that supports communications to its systems that either store and/or process information on the senders' behalf."[118] If the electronic communication is held by an ECS for less than 180 days and it has not been opened by the intended recipient, then the SCA requires government officials to obtain prior judicial approval and meet the standard of probable cause.[119] "The search warrant need only be issued by a federal court with jurisdiction over the offense under investigation, even if the records are held in another district."[120] The level of protection becomes significantly weaker if the electronic communication is held by an ECS for more than 180 days.[121] Once the electronic communication has been stored for greater than 180 days, then it can be obtained by only a mere subpoena.[122] The standard becomes relevance, and it can be issued without judicial oversight.[123] This becomes problematic when a government agency chooses to wait until 180 days lapses and then accesses electronic communications with only a subpoena without any sort of judicial oversight.[124] This is further complicated by conflicting case law on what constitutes "electronic storage."[125] With the focus on electronic communication, the SCA also fails to adequately address other forms of online storage provided by internet service providers. It is unclear whether items stored on a

---

113. 18 U.S.C. § 2701(a) (2015).
114. 18 U.S.C. § 2701(c) (2015).
115. Mulligan, *supra* note 79, at 1568.
116. *See id.* at 1568.
117. *Id.*
118. *Id.*
119. *Id.* at 1570.
120. *Id.*
121. Mulligan, *supra* note 79, at 1571.
122. 18 U.S.C. § 2703(a)–(b) (2015).
123. Mulligan, *supra* note 79, at 1570.
124. *Id.* at 1570–71.
125. *Id.* at 1571.

service provider's servers that are not meant to be delivered to another recipient are included in the definition of electronic communication. If not, then they would fall out of the purview of the SCA and not be subject to its Fourth Amendment protections.

C. *The Laboratories of Democracy*[126]

Considering the shortcomings of the ECPA, it is not surprising that some states have chosen to enact their own legislation to extend additional protections for their citizens. Among them, California is now the largest state to enact legislation that further protects the digital privacy of its citizens.[127] This should not come as a surprise, considering California hosts some of the world's largest technology firms and is the seat of Silicon Valley.[128] However, what should be surprising is the support from California law enforcement organizations.[129] In order to see why this bill has garnered support from such a broad base, it is important to analyze the scope and limits that the bill puts into place for law enforcement and the citizens of California.

III. THE CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT

California Senate Bill 178 was signed by the governor of California on October 8, 2015, and incorporates additions to the California Penal Code effective January 1, 2016.[130] Colloquially referred to as the California Electronic Communication Privacy Act (CalECPA),[131] the bill states its intent to "prohibit a government entity from compelling production of or access to electronic communication information or electronic device information . . . , without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant under

126. "It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments . . . . " New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

127. Buttar, *supra* note 7.

128. In support of the bill, Twitter stated, "[c]urrent federal law that extends fourth amendment right to electronic communications is nearly 30 years out of date." *Privacy: Electronic Communications: Search Warrants: Hearing on S.B. 178 Before the S. Comm. On Pub. Safety*, 2015–2016 Reg. Sess. (Ca. 2015).

129. Buttar, *supra* note 7.

130. S.B. 178, 2015–2016 Reg. Sess. (Ca. 2015).

131. Tracey Lien, *Everything You Need to Know About California's New Electronic Communications Privacy Act*, L.A. TIMES (Oct. 9, 2015, 12:44 PM), http://www.latimes.com/business/technology/la-fi-tn-california-electronic-privacy-20151009-story.html [http://perma.cc/UQ79-B63D].

specified conditions. . . . "[132] It is important to note, that the purpose behind both the existing federal ECPA and the CalECPA is to guard against arbitrary use of government surveillance.[133] The difference between the two lies in their execution.

A. *Provisions of the CalECPA*

The CalECPA consists of chapter 3.6 in Title 12 of Part 2 of the California Penal Code.[134] The CalECPA provides Fourth Amendment protections for essentially two areas of electronic information.[135] First, a government entity is otherwise prohibited from compelling the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device unless the government entity obtains a warrant, wiretap order, order for electronic reader records, or a subpoena if such subpoena is not sought for the purpose of investigating or prosecuting a criminal offense.[136] The CalECPA defines "electronic communication information" as,

> any information about an electronic communication[137] or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address.[138]

How the CalECPA defines this is incredibly important because it not only includes the content of the electronic communication, but also its metadata.[139] To illustrate, a government agency would be prohibited under this statutory scheme from even acquiring the time or date an e-mail was sent,

---

132. S.B. 178, 2015–2016 Reg. Sess. (Ca. 2015).

133. S. Rep. No. 99-541, at 1-2 (Ca. 1986) (explaining that when the Framers of the Constitution acted to guard against the arbitrary use of government surveillance, current capabilities of electronic surveillance did not exist).

134. S.B. 178, 2015–2016 Reg. Sess. (Ca. 2015).

135. *See* CAL. PENAL CODE § 1546.1 (West 2016).

136. *See id.*

137. "Electronic communication means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in party by a wire, radio, electromagnetic, photoelectric, or photo-optical system." PENAL § 1546(c).

138. PENAL § 1546(d).

139. Metadata is defined as data about data. OXFORD https://en.oxforddictionaries.com/definition/metadata (last visited Mar. 4, 2017) [http://perma.cc/W3G3-ULGF]; *see Penal* § 1546(d).

much less its actual contents or the parties involved in the communication without first obtaining a warrant.[140] This is an important limitation considering the recent concerns of widespread metadata collection by government agencies.[141]

Second, a government entity is prohibited from accessing "electronic device information" through physical interaction or electronic communication with the electronic device unless that government entity (1) obtains a warrant, (2) obtains a wiretap order, (3) has consent from the authorized possessor[142] of the device, (4) has consent from the owner of the device when that device has been reported as lost or stolen, (5) believes in good faith that access is necessary because of an emergency involving danger of death or serious physical injury to any person,[143] (6) believes in good faith that the device is lost, stolen, or abandoned and wishes to use that information solely to identify, verify, or contact the owner, or (7) if the device is seized from an inmate's possession and not known or believed to belong to an authorized visitor of the correctional facility.[144] "Electronic device information" is defined as "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device."[145] This essentially provides protections for information stored on devices like cellphones and laptops. Additionally, the information protected appears to be much broader as it would purport to include all digital data stored on the device regardless if it is classified as "electronic communication."[146]

Not only are the protections under these two areas far more comprehensive than the federal ECPA, but the CalECPA establishes additional requirements when obtaining a warrant. Under the CalECPA, any warrant for electronic information must "describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or

---

140. PENAL § 1546.1(b)(1).

141. Greenwald, *supra* note 2.

142. Defined as "the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device." PENAL § 1546(b).

143. However, after obtaining information through this exception, within three days the government entity must file with the appropriate court for a warrant or order. If the court determines that the emergency did not warrant obtaining the information, it shall order the immediate destruction of all information obtained. PENAL § 1546.1(c)(1)–(6).

144. PENAL § 1546.1(c)(7)–(8).

145. PENAL § 1546(g).

146. *See* PENAL § 1546.1(c)–(d).

services covered, and the types of information sought."[147] Furthermore, any information gained using a warrant that is unrelated to the objective of the warrant must be sealed and cannot be used without a court order.[148]

Finally, the CalECPA provides additional protections when an electronic communications service provider voluntarily discloses electronic communication information or subscriber information.[149] If a government entity receives electronic communication information voluntarily, it must destroy that information within ninety days unless: (1) the government entity has or obtains the specific consent of the sender or recipient of the electronic communications, (2) the government entity obtains a court order authorizing the retention of the information, or (3) the government entity reasonably believes the information obtained relates to child pornography.[150] This provision is important considering revelations of the amount of data that some internet companies had willingly provided to the National Security Agency.[151] While it cannot stop government entities from making voluntary requests for data,[152] the statute does provide protection from long-term collection of electronic information.[153]

Based on the preceding, it is clear that the CalECPA provides Fourth Amendment protection which surpasses the current federal statutes, not only in the scope of the electronic information protected, but in the manner in which a government entity can obtain that information without judicial oversight. This statute is a giant leap forward for privacy laws. However, it is still important to note several areas where the CalECPA is limited.

B. *Not Perfect Yet*

While being a substantial step forward in the extension of Fourth Amendment protections to electronic information in the digital age, it is still important to note several key shortcomings

---

147. PENAL § 1546.1(d)(1).

148. PENAL § 1546.1(d)(2).

149. PENAL § 1546.1(f)–(g).

150. PENAL § 1546.1(g)(1)–(3).

151. Steven Levy, *How the NSA Almost Killed the Internet*, WIRED (Jan. 7, 2014, 6:30 AM), http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/ [http://perma.cc/FF2X-7JAD].

152. Lien, *supra* note 131 ("According to the authors of [S.B. 178] . . . AT&T received more than 64,000 demands for location information in 2014.").

153. *Tech's Big Guns Back Up Apple in Encryption Battle*, CBS NEWS (Feb. 19, 2016, 8:13 AM), http://www.cbsnews.com/news/techs-big-guns-back-up-apples-encryption-battle/ (explaining the trend for large internet services companies to push back against government requests for customer data has continued to hold) [http://perma.cc/8VEV-S444].

with the CalECPA. First, considering that this is a state statute, it only applies to state governmental entities.[154] Federal governmental agencies are still only bound by the restrictions found in the ECPA.[155]

Second, the CalECPA still does not extend Fourth Amendment protection to non-communication electronic information stored by a cloud storage service.[156] For example, using services such as Google's Dropbox or Microsoft's OneDrive[157] in order to store digital copies of family photos would not be considered electronic communication and would thus not appear to be covered by the CalECPA.[158] While its protection of electronic information on digital devices is broad enough to cover non-communication electronic information, that protection does not apply to non-communication electronic information stored on a third party's servers.[159] It is likely that the third-party doctrine could still apply in such a situation, leaving individuals with no Fourth Amendment protection for personal data left on a service provider's server.

However, even with these shortcomings, the privacy protections granted by the CalECPA are vastly more forward looking and comprehensive than current Federal law. That is why it should be used as a framework for future amendments to the current federal ECPA.

IV. A WAY FORWARD

Future federal legislation should adopt the language and scope that the California Legislature used when they drafted the framework for the CalECPA. However, that should only be the start. Technology has continued to advance, and it is necessary to make sure statutory language reflects these advances.

First, the ECPA should be amended to provide the same scope of protection over electronic communications as the CalECPA. The CalECPA includes both the content of electronic communications as well as the metadata of such communication.[160] The ECPA only defines electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any

---

154. *See* Buttar, *supra* note 7.

155. *See id.*

156. CAL. PENAL CODE § 1546.1 (West 2016).

157. These are two examples of cloud storage services which allow individuals to back up personal digital content on off-site servers managed by a third-party.

158. *See* PENAL § 1546.1.

159. *See id.*

160. *Id.*

nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system . . . ."[161] The ECPA fails to provide any distinction for the metadata of electronic communications. The metadata itself can be almost as revealing as the content of the message.[162] The way we communicate on technology today generates far more metadata then in the past and collection of metadata has become exponentially easier.[163]

Second, the ECPA should be amended to include Fourth Amendment protection for the data stored on electronic devices. The CalECPA provides protections for any information stored on an electronic device and that information also includes "the current and prior locations of the device."[164] So not only does the CalECPA extend to any personal data stored on a cellphone, but also to any geolocation data it contains. Furthermore, the ECPA should be amended to remove any distinction between an e-mail stored on a server, and that same e-mail in transit.

Third, the ECPA should be amended to remove the 180 day distinction regarding the storage of electronic communication. "The ECPA was adopted at a time when e-mail, for example, wasn't stored on servers for a long time."[165] Today, it is not unlikely that an e-mail will be stored on a third-party's server for extended periods of time, even if the sender believes otherwise.[166] "E-mail often remains stored on cloud servers indefinitely, in gigabytes upon gigabytes."[167] This can even include text messages sent by cellphones.[168] By allowing a government agency, using only a subpoena, to acquire these communications after they have been sitting for over 180 days leaves a substantial loophole in Fourth Amendment protections under the ECPA. A passage of time should not remove the requirement for a warrant.

---

161. 18 U.S.C. § 2510 (2015).

162. Timothy B. Lee, *Here's How Phone Metadata Can Reveal Your Affairs, Abortions, and Other Secrets*, WASH. POST (Aug. 27, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/08/27/heres-how-phone-metadata-can-reveal-your-affairs-abortions-and-other-secrets/ [http://perma.cc/KD4L-NSBA].

163. Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, WIRED.COM (Jun. 19, 2013, 9:30 AM), http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/ [http://perma.cc/H2VG-2KH8].

164. S.B. 178, 2015–2016 Reg. Sess. (Ca. 2015).

165. David Kravets, *Aging 'Privacy' Law Leaves Cloud E-Mail Open To Cops*, WIRED.COM (Oct. 21, 2011, 6:30 AM), http://www.wired.com/2011/10/ecpa-turns-twenty-five/ [http://perma.cc/9B3X-89AZ].

166. *Id.*

167. *Id.*

168. Lance Ulanoff, *Messages Can Be Forever*, PCMAG (August 11, 2004), http://www.pcmag.com/article2/0,2817,1634503,00.asp [http://perma.cc/RD4C-WN2F].

Fourth, the ECPA should be amended to include the destruction provisions found in the CalECPA for a third-party's voluntary disclosure of another individual's electronic data. If a government entity has received electronic information through a request to an internet service provider, that government entity should be required to destroy that electronic information after a period of time, unless it can obtain a court order allowing it to retain it.[169]

Finally, the ECPA should be amended to extend Fourth Amendment protection to any electronic data stored by an individual on a third-party's server. With the continued proliferation of cloud computing, more and more electronic data will be stored, not on an individual's device, but on servers maintained by internet services companies.[170] The ECPA should be amended to reflect this trend and extend Fourth Amendment protections to more than just electronic communications.

V. CONCLUSION

The Electronic Communications Privacy Act was supposed to bring the Fourth Amendment into the digital age. While it may have succeeded in doing that in 1986, the statutory provisions that it implemented have become rapidly outpaced by advancing technology. California is the most recent state to provide its citizens with modern and comprehensive privacy protection for electronic information.[171] Its statutory framework should be a model for future federal amendments to the ECPA to bring the ECPA back into the digital age.

Jeremiah Clark

169. According to Twitter's Transparency Report, it received a total of 4,363 information requests from government entities. More than half the time, at least some information was produced. *Transparency Report, Information Requests*, TWITTER, https://transparency.twitter.com/en/information-requests.html#information-requests-jan-jun-2015 (last visited Feb. 3, 2017) [http://perma.cc/TQZ9-UT34].

170. Serafino, *supra* note 12, at 161.

171. Lien, *supra* note 131 (Maine and Utah have similar statutes).