The Privacy of "Things": How the Stored Communications Act Has Been Outsmarted by Smart Technology

Donald L. Crowell III *

TABLE OF CONTENTS

I. INTRODUCTION 213

II. FOURTH AMENDMENT JURISPRUDENCE RELATING TO DIGITAL COMMUNICATIONS 216

A. Katz v. United States Establishes the Foundation for Modern Privacy Expectations 216

B. Miller and Smith Evolve Katz into the "Third-Party Disclosure Doctrine" 217

C. Courts are Conflicted as to Whether a Reasonable Expectation of Privacy Exists in Electronic Communications 219

III. THE STORED COMMUNICATIONS ACT 221

A. Applicability of the Required Disclosure Section of the SCA is Broad as to the Entities and Records It Governs 222

IV. THE FOURTH AMENDMENT OFFERS PROTECTION FOR INFORMATION STORED IN THE CLOUD—FEDERAL LAW MUST REPRESENT THIS 224

* J.D. Candidate, The George Washington University Law School, May 2018. Senior Managing Editor, *Federal Communications Law Journal*, Vols. 69–70. B.A. Political Science, *cum laude*, University of California, Riverside, 2015. This Note is dedicated to both of my loving parents, whose support and sacrifices throughout my life have made it possible for me to pursue a career in law; to my inspiring friends and family who encourage the best in me; and to the Staff of the *Federal Communications Law Journal* who have been exceptional with their editorial work this year, and with whom I've had a sincere pleasure in having worked with.

A. Classifying Cloud Document Storage Services under the SCA 225

B. Classifying Mobile Applications Under the SCA 226

C. Classifying Security and Smart Home Services under the SCA 227

D. A General Analysis of Cloud Service Providers Under the Fourth Amendment Framework 228

V. A THREE-PRONGED SOLUTION TO ESTABLISH CLEAR CONSTITUTIONAL PROTECTIONS FOR INFORMATION STORED IN THE CLOUD 230

A. The Supreme Court Should Expand Riley v. California to Require Warrants for Any Government Access of User Data Held in the Cloud 230

B. Legislating to Replace or Amend the SCA 233

C. An Industry Effort to Promote Privacy Rights 234

VI. CONCLUSION 235

I. INTRODUCTION

Meet Barbara, a modern business professional who is one of three managing partners at a well-known investment firm. Working from home, she prepares for a meeting with a client by connecting to her firm's Cloud-based remote desktop application on Amazon's S3 platform. The application replicates her work computer's desktop and allows her to access all her files just the same as if she was at the office. At the same time, her firm enjoys the benefit of having all its documents maintained in a secure backup location. Barbara finishes reviewing her client's documents and gets into her car—a BMW 3 Series. She opens Google Maps on her iPhone to get directions to her client's office, and, meanwhile, her phone has automatically connected via Bluetooth to her car's infotainment system and has begun synchronizing her contacts list, emails, and text messages. As she pulls out of the driveway—just far enough to disconnect from her home Wi-Fi network—her Nest smart-home system notes that she has left. Immediately, the thermostat adjusts to save energy, and the camera system turns on its motion sensors.

Meanwhile, unbeknownst to Barbara, one of the other partners at her investment firm has just made some illegal investments based on inside information. The partner's trades automatically triggered alarms at the Securities and Exchange Commission ("SEC"), Enforcement Division, based on his position at the investment firm. The SEC does a routine investigation into the trades over the next 90 days, ultimately finding a high probability that Barbara's partner made trades using inside information. However, their investigation thus far has only produced enough to muster "reasonable suspicion" that a crime has been committed; further information would be necessary to meet the standard of "probable cause" required to issue a search warrant against Barbara and her firm. The enforcement team, through their counsel, learns of the ability to issue an administrative subpoena under the Stored Communications Act ("SCA"). While it does not allow them to request any digital content newer than 180 days without having probable cause, they are able to request content from service providers for content that has been in storage for 180 days or longer.

The enforcement team first issues a subpoena to the Cloud service provider for Barbara's firm, Amazon, requesting all the electronic documents held in storage by the provider that are older than 180 days. They also make two other requests under the statute: (1) that the firm not be notified of the subpoena request for a minimum of 90 days, and (2) that the provider preserve the entirety of the firm's electronic documents, also for a period of 90 days.

As the team reviews the documents, including sifting through client lists, business strategies, and emails between the firm and its attorney, among other things, it discovers two sets of emails that it finds particularly interesting, although unrelated to their initial investigation against Barbara's partner. The first is a conversation between Barbara and her attorney. The discussion included questions about what constituted insider trading, and whether Barbara could be liable for trading on information that she receives

from a client. The second email is a message that Barbara had forwarded herself from her personal e-mail. While the substance of the second e-mail is irrelevant, the team now had the domain of Barbara's personal email account.

The investigators issue a subpoena to Barbara's personal email provider, Google, identical to the one sent to Amazon. What they receive from Google in return is far more than just her e-mail communications. Because of Google's multifaceted list of services, they receive her e-mails, GPS navigation history, web search history, photographs, and personal documents in her Google Drive storage. Her navigation history shows the specific dates and times she navigated to her client's office, in addition to regular visits to a nearby mosque, the local Democratic National Committee offices, her psychiatrist, a hotel, and an abortion clinic. Her photograph backups included those with family, friends, and on vacation trips, but also deeply private, fully-nude photos of Barbara. Similarly, her Google Drive records contained seemingly harmless collections of internet pages and random web-musings, but among them was a collection of scanned purchase receipts, tax records, private contracts, and her personal diary.

The investigation team thoroughly reviewed all the documents before issuing a final administrative subpoena to Barbara's smart-home system provider, Nest. The electronic records they received from Nest included a history of every single time, to the second, when Barbara either left or arrived home. More importantly, provided to the SEC were video recordings of Barbara's home beginning from when the system was installed 6 years ago, essentially capturing every person that has ever been inside her home, and all activities that have taken place inside of it.

They continued reviewing Barbara's personal electronic records until just before the 90-day delay notice and preservation request expired, after which they issued a 90-day extension for both requests, as allowed by the statute. A few days later, just after the 181-day mark since the start of their investigation, the SEC re-issues subpoenas to each of the original providers, this time capturing all electronic records leading to the incident. Reviewing the new navigation history production from Google Maps, as well as the calendar records stored in Amazon's Cloud, they see that Barbara had a meeting with her client on the day of the incident. Audio and video security camera footage from the night before the incident revealed that a client of Barbara's had been over at her home for dinner, during which highly confidential information was discussed regarding her client's expected product release. None of this information was enough to bring formal charges against Barbara, although her partner was ultimately prosecuted. However, Barbara's very intimate and confidential information was now in the public's hand because of her tangential relationship to someone under investigation.

This illustration with Barbara is just one very possible example of the shortcomings that digital privacy law faces under an outdated Stored Communications Act ("SCA"). This Note argues a three-pronged solution to resolve these shortcomings through a case-study analysis of different

technologies: (1) extending a broader application of *Riley v. California*,[1] (2) legislative amendments to the SCA,[2] and (3) private-sector data encryption advancements. Part II will consider the current jurisprudence of privacy in electronic records and communications by first exploring the foundational elements of modern privacy law, before diving into the more field-specific cases and circuit splits relating to expectations of privacy in digital information. Part III will look at the Electronic Communications Privacy Act ("ECPA") and SCA, examining both their legislative history and amendments, as well as the contradictions and flaws that are revealed when considering their applicability to modern Cloud-based technologies. Part IV will analyze three different Cloud technologies, specifically ones that have the capability of holding the most confidential information of individuals, and demonstrate how the use of administrative subpoenas under the SCA, as well as the delay and preservation notice provisions, directly violate Fourth Amendment protections and are in conflict with prior court rulings that have prohibited the same type of information gathering by other means.

Part V will lay out the three-pronged federal solution to establish new standards for businesses and the government to follow. The first prong will argue why it is necessary to extend the *Riley* Court's decision (finding constitutional protections in information stored in the Cloud)[3] to situations beyond arrests. The second prong will propose an amendment or replacement to the ECPA and SCA that limits the ability of law enforcement to perform warrantless searches of individuals who are not under investigation, as well as eliminating the time restriction requirements of the acts. Further, the proposed amendments enable National Telecommunications & Information Administration ("NTIA") to regulate electronic communications service providers ("ECSPs") and remote computing service providers ("RCSPs"). This will include a more technical determination of their definitions, as well as requiring those categories of providers to register with NTIA, thereby limiting the discretionary use of administrative subpoenas by law enforcement. The third prong is not a government solution, but rather a proposal that ECSPs and RCSPs eliminate or reduce their own ability to access sensitive consumer data. This, along with continuing advancements in encryption technology, will allow law enforcement access to encrypted data, but not necessarily to the content of the data itself.

1. *See generally* Riley v. California, 134 S. Ct. 2473 (2014).
2. *See* Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).
3. *See Riley*, 134 S. Ct. at 2491–93.

II. FOURTH AMENDMENT JURISPRUDENCE RELATING TO DIGITAL COMMUNICATIONS

A. *Katz v. United States Establishes the Foundation for Modern Privacy Expectations*

Modern-day Fourth Amendment jurisprudence finds its foundation in *Katz v. United States*, which laid the groundwork for what is now referred to as the "reasonable expectation of privacy" test.[4] In *Katz*, FBI agents attached an electronic listening device to a public phone booth that they suspected Katz was using to gamble across state lines.[5] Unaware of the device, Katz made phone calls placing bets with contacts in Miami and Boston—unaware that the call was being recorded.[6] The Government introduced the telephone recordings as evidence to successfully convict Katz of the wagering charges in district court.[7]

On appeal, the U.S. Supreme Court reconsidered its previous reliance on the "trespass doctrine"[8] and held that the Fourth Amendment grants a right to "privacy against certain kinds of governmental intrusion…."[9] This protection follows a person wherever they go, and is not limited to particular places or things.[10] However, it was Justice Harlan, in a concurring opinion, who enunciated the two-part "reasonable expectation of privacy" test that the Court would rely on in a handful of Fourth Amendment cases following *Katz*.[11] This test requires that an individual have a "subjective expectation of privacy" in their belongings and/or information, and that society would objectively find the individual's subjective expectation of privacy to be reasonable.[12]

4. *See* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 987–89 (2016).

5. *See* Katz v. United States, 389 U.S. 347, 348–49 (1967).

6. *See id.*

7. *See id.*

8. The "trespass doctrine" was based on the common law tort of trespass, requiring the Government to physically trespass on to property before Fourth Amendment protections could be invoked. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001); Olmstead v. United States, 277 U.S. 438, 463–65 (1928).

9. *See Katz*, 389 U.S. at 350.

10. *See id.* at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

11. *See Katz*, 389 U.S. at 360–62 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual subjective expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

12. *See id.*

B. *Miller and Smith Evolve Katz into the "Third-Party Disclosure Doctrine"*

The Court in *United States v. Miller*, weighing both prongs of the *Katz* test, determined that the Fourth Amendment does not protect an individual's privacy interest in non-confidential information that was voluntarily conveyed to a third-party.[13] In *Miller*, law enforcement had gathered, over the course of several months, evidence of illegal that Miller was engaging in distilling activity.[14] Included in this evidence were bank records that the Treasury Department had recovered under grand jury subpoenas issued to Miller's bank.[15] Miller sought to suppress the bank records, arguing successfully at the appellate court level that the Government had illegally acquired access to those records from his bank.[16]

The Court reversed, finding that there was "no intrusion into any area in which [Miller] had a protected Fourth Amendment interest."[17] Essentially, there was no intrusion into a "zone of privacy."[18] The Court found that while it had previously held the Fourth Amendment protects people from "compulsory production of a man's private papers,"[19] the bank records in question in *Miller* did not actually belong to the defendant.[20] Rather, they belonged to the bank, who maintained those records as a party to the transactions between it and Miller.[21] When Miller participated in transactions with the bank, he knowingly took the risk that the bank could reveal any resulting information to the Government.[22] The Court ruled, therefore, that Miller held no "Fourth Amendment interest" in the bank records, even if it were assumed that they would only be used for a specific purpose.[23] The Government's subpoena, as well as the bank's action in turning over the records, was constitutionally permissible.[24]

---

13. *See* United States v. Miller, 425 U.S. 435, 441–43 (1976).
14. *Id.* at 436.
15. *Id.*
16. *Id.* at 439 ("[T]he court [of appeals] held that the Government had improperly circumvented *Boyd's* protections of [Miller's] Fourth Amendment right against 'unreasonable searches and seizures' by 'first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal processes, calling upon the bank to allow inspection and reproduction of those copies.'" (citations omitted)).
17. *Id.* at 440.
18. *Id. at* 440 ("'[N]o interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'" (quoting *Hoffa v. United States*, 385 U.S. 293, 301–02 (1966))).
19. *Id.* (citing *Boyd v. United States*, 116 U.S. 616, 528 (1886)).
20. *Id.*
21. *Id.* at 441–42.
22. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).
23. *Id.* at 445–46.
24. *Id.*

The Court in *Smith v. Maryland* developed the third-party disclosure doctrine to encompass the use of pen registers[25] in determining both that its use was not a "search" within the meaning of the Fourth Amendment, and that no legitimate expectation of privacy existed in phone numbers.[26] Similar to *Katz*, law enforcement identified Smith as their prime suspect in a robbery.[27] Without first acquiring a warrant, law enforcement installed a pen register with the telephone company used by Smith to record all phone numbers that he dialed, which ultimately showed that only a few days earlier he had dialed the robbery victim's phone number.[28] This evidence was used to acquire a search warrant for Smith's home, where police found evidence that identified him as the robber.[29]

Like in *Miller*, the Court in *Smith* found that the defendant had no expectation of privacy in his telephone records because he did not own them.[30] Smith had "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[31] By doing so, Smith "assumed the risk that the company would reveal to the police the numbers he dialed."[32] Smith could, therefore, hold no legitimate expectation of privacy in those records.[33] *Smith* reaffirmed the Court's decision in *Miller*, and the validity of the third-party disclosure doctrine, which would control the decisions of other similar Fourth Amendment cases until only very recently.[34]

25. *See* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed. A pen register is 'usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached.'" (citations omitted)).

26. *Id.* at 745–46.

27. *Id.* at 737.

28. *Id.*

29. *Id.*

30. *Id.* at 741 ("Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'").

31. *Id.* at 744.

32. *Id.*

33. *Id.*

34. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 948 (2012) (monitoring of an individual's location patterns over the course of an extended period of time—in this case 28 days—by attaching a GPS device to track an individual's vehicle movements constituted a "search" within the meaning of the Fourth Amendment); United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (applying Voluntary/Third-Party Disclosure Doctrine to e-mail metadata); United States v. Forrester, 512 F.3d 500, 509 (9th Cir. 2008) (finding that computer surveillance of an individual, and introduction of website history information gathered through such surveillance, did not amount to a search under the Fourth Amendment).

C. Courts are Conflicted as to Whether a Reasonable Expectation of Privacy Exists in Electronic Communications

In 2010, the Sixth Circuit in *United States v. Warshak* strengthened Fourth Amendment protections over digital technologies when it held that individuals have a "reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial[internet service provider] ["ISP"]."[35] Applying the two-part *Katz* test, the court first found it highly likely that the defendant did not expect his e-mail communications to be public, given their "sensitive and sometimes damning substance."[36] As to the second part of the test, the court analogized an e-mail to a "letter or a phone call," and noted that simply because an ISP can access the content of those e-mails is not enough to "extinguish a reasonable expectationof privacy."[37] Similarly, the "rented space" that a subscriber uses to store the e-mail on the ISP's server is similar to the renting of a hotel room or apartment, where guests and tenants have a reasonable expectation of privacy even though maids or maintenance workers may enter on occasion.[38]

This case is distinguishable from *Miller* for several reasons.[39] *Miller* dealt with the disclosure of very particular business records, as opposed to the "potentially unlimited variety of 'confidential communications'" that might be contained in e-mail and electronic content.[40] And although in *Miller* the bank needed to use the information in their ordinary course of business, the ISP in *Warshak* was simply an "*intermediary* and not the intended recipient of the e-mails."[41]

The Eleventh Circuit's decision in *Rehberg v. Paulk* came at nearly the same time as *Warshak*, but delivered an opposite ruling: that "[a] person … loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party."[42] *Rehberg*'s analysis is similar to the earlier line of "voluntary/third-party disclosure doctrine" cases.[43] Citing several other circuit decisions, the Eleventh Circuit found that "Rehberg's voluntary delivery of emails to third parties constituted a voluntary relinquishment of the right to privacy in that information" once the third party had received them.[44]

---

35. *Warshak*, 631 F.3d at 288 (internal citation and quotation omitted).
36. *Id.* at 284 ("[Defendant's] entire business and personal life was contained within the . . . emails seized.") (citation omitted).
37. *Id.* at 286.
38. *Id.* at 287 (citing United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997) and United States v. Washington, 573 F.3d 279, 284 (6th Cir. 2009)).
39. *Id.* at 288.
40. *Id.*
41. *Id.* (emphasis in original) (citations omitted).
42. Rehberg v. Paulk, 598 F.3d 1268, 1281 (11th Cir. 2010), *vacated*, 611 F.3d 828 (11th Cir. 2010).
43. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745–46 (1979); United States v. Miller, 425 U.S. 435, 444–45 (1976).
44. *Rehberg*, 598 F.3d at 1282.

More recently, it appears that the Supreme Court has tipped the discussion in favor of protecting digital content, when in *California v. Riley* it ruled that "a warrant is generally required before [searching information on a cell phone], even when a cell phone is seized incident to arrest."[45] The Court considered many factors, but relied heavily on the distinction between cell phones and their content from "other objects that might be kept on an arrestee's person."[46] A cell phone allows individuals to carry around "every piece of mail they have received . . . every picture they have taken, [and[every book or article they have read."[47] Keeping this quantity of records on one's person is not something that previously was feasible, and, even if done, would have likely required storing them in a container that a police officer would need a warrant to search.[48] This, coupled with the nature of content stored on cell phones—including internet search history,[49] as well as the types of mobile applications one uses[50]—potentially allows for broad and pervasive intrusions into one's privacy.[51]

These factors, however, only address content that is physically stored on a cell phone. The Court also found the argument in favor of searching cell phones incident to arrest to be essentially futile when accessing data in the Cloud:[52]

> Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. This is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing.". . . Cell phone users often may not know whether particular information is stored on the device or in the [C]loud, and it generally makes little difference. Moreover, the same type of data may be stored locally on the device for one user and in the [C]loud for another.[53]

While *Riley* did appear to broadly expand privacy rights to digital information, the Supreme Court found it necessary to limit its holding. For

45. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).
46. *See id.* at 2489.
47. *Id.*
48. *Id.* at 2491 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house.").
49. *See id.* at 2490. ("An Internet search and browsing history . . . could reveal an individual's private interests or concerns–perhaps a search for certain symptoms of diseases, coupled with frequent visits to WebMD.").
50. *Id.* ("There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life.").
51. *See id.*
52. *See id.* at 2491.
53. *Id.* (citations omitted).

example, before making its analogy between cell phone content and physical records, it noted, albeit in a footnote, that *Riley* only addresses searches of cell phones incident to arrest.[54] Further, the limitations on law enforcement do not apply in cases where exigent circumstances necessitate the expedited retrieval of information from a cell phone, such that "a warrantless search is objectively reasonable under the Fourth Amendment."[55] Therefore, it is not entirely clear whether *Riley* amounts to more than *persuasive* authority when applied to situations other than cell phone searches incident to arrest—such as in the scenario with Barbara demonstrated above.[56]

III. THE STORED COMMUNICATIONS ACT

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA"), which included, in part, the Stored Communications Act ("SCA"), which governs the privacy of electronic data.[57] Although its main purpose was to provide protection for "new forms of [ ] communications . . . against improper interception," a secondary goal was to assist law enforcement by providing them with "investigative techniques which involve the interception of communications."[58] The following discussion will focus on section 2703 of the SCA, which requires businesses that provide particular types of electronic services to the public to disclose a customer's records to law enforcement when requested, after meeting certain procedural requirements.[59]

Yet, Section 2703 of the Act, in particular, has failed to develop in tandem with the digital technology market. The results have revealed an economic and constitutional vulnerability that will grow with the increasing use of digital technology by consumers in the coming years. Section 2703 allows government agencies, at both the state and federal level, to issue administrative subpoenas to electronic service providers for essentially all types of stored electronic information held on behalf of consumers.[60] These administrative subpoenas do not require the agency to show probable cause

54. *Id.* at 2489 n.1 ("Because the United States and California agree that these cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

55. *Id.* at 2494 (quoting Kentucky v. King, 131 S. Ct. 1849, 1856 (2011)).

56. *See supra* Part I (Introduction).

57. *See* Electronic Communications Privacy Act of 1986, Pub L. No. 99–508, 100 Stat 1848 (codified as amended in scattered sections of 18 U.S.C.); Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012); *see also* Erik C. Shallman, *Up in the Air: Clarifying Cloud Storage Protection*, 19 INTELL. PROP. L. BULL. 49, 66 (2014); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

58. *See* 132 Cong. Rec. H8977–02 (1986) (statement of Rep. Kastenmeier).

59. *See* 18 U.S.C. § 2703 (2012).

60. *See id.*

that an act was being committed, nor do they require that the administrative subpoena be issued against the specific person being investigated.[61]

A. Applicability of the Required Disclosure Section of the SCA is Broad as to the Entities and Records It Governs

The types of records governed under the SCA ranges from those containing actual content—e-mails, electronic documents, pictures, etc.—to basic subscriber information, such as name and contact information.[62] The SCA distinguishes between records containing substantive information and records containing basic subscriber information by referring to the records in two different categories–content and non-content information ["records concerning" ECS or RCS customers].[63] Compelling disclosure of the two categories varies, for example, can use state or federal administrative subpoena power to access non-content information, such as credit numbers, usernames, network addresses, physical addresses, among other information.[64] In most cases, the use of administrative subpoenas do not require any suspicion of a crime being committed, and, depending on the state, can be used by local governments.[65]

Of equal importance is the SCA's distinction between electronic records that are in storage for under and for over 180 days.[66] For documents in storage under 180 days, "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction" is always required to compel disclosure.[67] Records that have been in storage for longer than 180 days are subject to far less burdensome requirements.

---

61. Lacking in § 2703 is language indicating that *any* of the methods used by law enforcement to gather records may only be used to obtain records of the person that is actually being investigated. *See generally* § 2703. The only consistent requirement in the statute relates to notification of the *customer* of the records, which may not necesarilly be the individual under investigation. *Id.*

62. *See* §§ 2510, 2711.

63. *See* § 2703.

64. *See id.* § 2703(c)(1)(E), (c)(2) (to compel disclosure the government must only "seek[] [non-content] information").

65. *See, e.g.*, NEWPORT BEACH, CAL., MUN. Code § 5.04.300 (2018) ("The Finance Director, or any authorized employee, is hereby authorized to examine the books, papers and records of any person subject to this chapter . . . . Every licensee or supposed licensee is hereby directed and required to furnish to the Finance Director the means, facilities and opportunity for making such examination and investigation as are hereby authorized. The Finance Director is hereby authorized to examine any person, under oath, for the purpose of verifying the accuracy of any return made, or, if no return is made, to ascertain the license fees due under this title, and for this purpose may compel the production of books, papers and records and the attendance of all persons before him or her, whether as parties or witnesses, whenever he or she believes such persons have knowledge of such matters.").

66. *See id.*

67. *See* § 2703(a).

Under § 2703(b), a governmental entity can compel disclosure of documents stored longer than 180 days in two different ways:

> (A) [W]ithout required notice to the subscriber or customer, if the governmental entity obtains a warrant . . . by a court of competent jurisdiction; or
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
> (ii) obtains a court order for such disclosure under subsection (d) of this section;
> except that delayed notice may be given pursuant to Section 2705 of this title.[68]

Therefore, it is important to determine who exactly is required to comply with these provisions of the SCA. The Act provides two types of service providers that must disclose customer records–(1) electronic communications service providers ("ECSP"),[69] and (2) remote computing service providers ("RCSP"),both of which are required to disclose content and non-content records.[70] One significant difference between the two categories is that if a provider is classified as an ECSP, then the government can only acquire documents that are less than 180 days old through the use of a warrant.[71] If the provider is classified as an RCSP, or the documents sought from an ECSP are older than 180 days, then the government can use other methods to compel disclosure (such as an administrative subpoena).[72]

These categories appear very broad, encompassing an increasing number of businesses when considering the definition of "electronic communication,"[73] and how common it is for businesses to provide services

68. *See* § 2703(b)(1). Additionally, § 2705 allows governmental entities attempting to compel disclosure under § 2703(b) to delay giving required notice to subscribers for renewable 90-day periods where an adverse outcome may occur as a result of giving notice. *See* § 2705(a). An adverse result includes "endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying trial." *Id.*

69. *See* 18 U.S.C. § 2510(15) (2012) ("'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications.").

70. *See* 18 U.S.C.§ 2711(2) (2012) ("the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.").

71. *See* § 2703(a).

72. *See id.*

73. *See* §2510(12) ("'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, or electromagnetic, photoelectronic or photooptical system….").

that involve electronic communications today.[74] As electronic communication technologies continue to advance, companies and consumers are increasingly transitioning to the use of the Cloud to store information.[75] This growth is one particularly strong reason why SCA reform is so pressing, and critical to ensuring equal application of the Fourth Amendment's property protections.

IV. THE FOURTH AMENDMENT OFFERS PROTECTION FOR INFORMATION STORED IN THE CLOUD—FEDERAL LAW MUST REPRESENT THIS

For both consumers and businesses, the trend seems to be heading to a default of using the Cloud for storage of documents and other media, such as music, pictures, and even medical records.[76] The Cloud provides many advantages over other forms of data storage, including increased accessibility, security, and backup redundancy.[77] Developing a framework for constitutional protections of digital property and information is difficult, in part because there is still debate over what kind of protections e-mail deserves, which is a more basic form of electronic communication compared to the multitude of products on the market today.

Applying the *Katz* framework to Cloud storage services ultimately demonstrates that electronic media storage should be protected by the Fourth Amendment, although ambiguities remain as with *Katz*'s application to similar digital technologies. Initially, the Supreme Court assumed that the Fourth Amendment framework used to analyze the propriety of physical searches applies similarly to searches of electronic property or information.[78] Taking this assumption as valid, it is still necessary to analogize the use of Cloud storage to something physical for Fourth Amendment's protection over "persons, houses, papers, and effects"[79] to be properly applied.

74. *See* S. Rep. 99–541, at 10-11 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555 ("Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing.")

75. *See* Leo Sun, 10 *Cloud Computing Statistics That Will Blow You Away*, MOTLEY FOOL (Nov. 29, 2016, 3:08 PM), https://www.fool.com/investing/2016/11/29/10-cloud-computing-stats-that-will-blow-you-away.aspx [https://perma.cc/EH5Q-Y2FY].

76. *See, e.g.*, *Are Consumers Better Off Putting Everything in the Cloud?*, WALL ST. J.:J. REPORTS: LEADERSHIP (May 11, 2014, 5:05PM ET), http://www.wsj.com/articles/are-consumers-better-off-putting-everything-in-the-Cloud-1399644099 [https://perma.cc/2S2A-ZBMA].

77. *See* Ian Paul, *Why you need a cloud backup service, and how to use one*, PCWORLD (Jan. 12, 2016, 3:30 AM PST), https://www.pcworld.com/article/3020270/security/why-you-need-a-cloud-backup-service-and-how-to-use-one.html [https://perma.cc/V3VM-M45K].

78. *See* City of Ontario, Cal. v. Quon, 560 U.S. 746, 748 (2010).

79. *See* U.S. CONST. amend. IV.

A. Classifying Cloud Document Storage Services under the SCA

One of the first steps in using a Cloud storage service, such as Google Drive or Dropbox, is uploading files into the Cloud.[80] This action, in and of itself, falls neatly within the definition of an electronic communication under the SCA.[81] By providing the public with the ability to upload documents into the Cloud, the Cloud storage provider allows users to send or receive wire or electronic communications, not to mention the numerous tools that are available for users to send documents in the Cloud to other individuals.[82] When users begin to "collaborate" with others on documents stored in the Cloud, they are also sending and receiving "electronic communications" through the Cloud storage service provider. Thus, looking at the most basic function of uploading files to Cloud storage, in addition to the more advanced functions of Cloud storage devices, it is evident that Cloud storage providers can fall within the ECSP category of the SCA.

Yet, one highly technical question regarding the timeliness requirement remains: what does it mean for a document to be in electronic storage for 180 days? Often, users of Cloud storage services upload documents and work on them from the Cloud. Every time a user saves a change to the document, the file is no longer the same original one. Currently, there is no guidance as to whether a document would need a warrant if it had been originally uploaded more than 180 days prior to law enforcement's request, but had been updated within that time period. In strictly technical terms, it can be argued that anytime a document has been edited this countdown resets because the process of saving an edited document involves deleting the original and replacing it with the changed version.[83]

Cloud storage services also can just as easily fall under the definition of "remote computer service providers." To qualify as a remote computer service provider, the business must provide computer storage or processing services to the public "by means of an electronic communications system."[84] As discussed earlier, the use of Cloud storage services inherently falls under the definition of electronic communication services.[85] As the main function of Cloud storage providers is to allow individuals to store documents on remote servers, they appear to fall even more neatly within this second category of the SCA.

---

80. *See generally Meet Google Drive*, GOOGLE DRIVE https://www.google.com/intl/en_us/drive/ [https://perma.cc/YKX3-PD3K](last visited Jan. 15, 2018).

81. *See* 18 U.S.C. § 2510 (2012).

82. *See generally How Dropbox Works,* DROPBOX https://www.dropbox.com/help/sign-in/how-security-works [https://perma.cc/L5CC-VY74] (last accessed Mar. 19, 2018)

83. *See View Activity & File Versions*, GOOGLE, INC., https://support.google.com/drive/answer/2409045?co=GENIE.Platform%3DDesktop&hl=en [https://perma.cc/U4FQ-FTRE] (last visited Jan. 15, 2018).

84. *See* 18 U.S.C. § 2711 (2012).

85. *See supra*, Part III (The Stored Communications Act).

What this means for users of Cloud storage services is that their documents are more vulnerable to government-compelled disclosures because they fall under both categories. Remote computer service providers can be compelled by the Government to hand over user data, regardless of whether it is older/newer than 180 days, without the use of a warrant.[86] The Government can simply use a subpoena or court order to access the data as long as they give notice to the subscriber. [87]Yet, the Government can delay this notice for multiple 90-day periods, even while receiving access to the information held by the subscriber's service provider.[88] Unfortunately, the state does not address whether a provider may be classified under one or both categories of the SCA.[89] However, the lack of such a limitation indicates that potentially the least-restrictive category with regard to law enforcement's ability to access records would apply.

B. Classifying Mobile Applications Under the SCA

More common than the use of Cloud storage is the use of mobile applications on smartphones. These applications range from news, politics, and healthcare, to almost anything else.[90] While its content and use may vary dramatically, a commonality among "apps" is that they collect and store information both gathered from, and owned by, the user. [91] Often this information is not stored on the local memory of a cell phone, for both technological and economic reasons.[92] Regardless of where the information used by the app is stored, most apps transmit data from the cellular device to the company that owns the app.[93] This data is then analyzed and processed to accomplish a particular task, such as fulfilling a search request in a news app for "Washington, D.C."[94]

Classifying mobile applications is a very fact-specific analysis that largely depends on the particular application in question. For example, an application that does not store or process any data in the Cloud would not likely fall under either category of the SCA. Take, for example, a game application that functions entirely from the data stored on the cell phone (offline)—it would not qualify under either category. If the same application

86. *See* 18 U.S.C. § 2703(b)(1) (2012).
87. *Id.*
88. *See* § 2703(b)(1)(B)(ii).
89. This is likely due to the state of e-mail technology present at the time the SCA was enacted, which was very simplistic and not at all like the multi-functional software technologies that currently exist. *See* Outlook.com, *The* 41*-Year History of Email*, MASHABLE (Sept. 20, 2012), http://mashable.com/2012/09/20/evolution-email/#DWPJqRdF7sq2 [https://perma.cc/L9BC-U4A5].
90. *See generally Choosing A Category*, APPLE, INC., https://developer.apple.com/app-store/categories/ [https://perma.cc/B22U-3456] (last visited Mar. 12, 2017).
91. *See generally Understanding Mobile Apps*, FTC (Feb. 2017), https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps#basics [https://perma.cc/JP7W-2PWC].
92. *See id.*
93. *See id.*
94. *See id.*

allowed you to purchase additional features, or stored user data in the Cloud, then that would change how the game application is classified. The ability to purchase additional features within the game app, for example, would mean that some sort of transmission occurred between the cell phone and the developer's server. Records of these transactions are likely stored with the developer, and at minimum, are stored with the purchase facilitator (e.g., Apple or Google). Similarly, a game requiring an online connection communicates information to and from the device in order to allow the game to function. A mobile application of this type would likely fall under both categories, as some sort of processing likely occurs on the remote servers, and there likely is some information stored relating to any account or profile made by the consumer for the game.

The application store from which user download an application (e.g., the App Store or the Google Play Store) is likely to fall under the ECSP category of the SCA, because there are electronic communications transmitted between the device and the store when purchasing an application. In contrast, the application store would likely not be considered an RCSP because it is not processing any information for the user—unless one considers the processes involved in facilitating the download of the application to fall under the definition.

Generally, however, it can be argued that if an application functions entirely from the files it stores locally on a person's cell phone, and requires no further online access, then it would not fall under either category. Such an argument seems appropriate, as the application would fail to send electronic communications, which is an essential part of both ECSP and RCSP classifications.[95] But, if an application requires access to the internet (more than just needing it to access online content, like a web browser might), it would likely fall under one or both categories of the SCA because of the broad language, although classification as an RCSP might be difficult depending on what is done with the data in the Cloud. This distinction is important because if a provider falls under the category of an RCSP, any records, even those less than 180 days–old, are subject to compelled disclosure without a warrant.

C. Classifying Security and Smart Home Services under the SCA

Smart home services, such as Nest throw an interesting wrench into the mix of Cloud service providers, both because they require a physical existence within the home of an individual, and because of the uniqueness of the businesses that own them.[96] These services can work in many ways. For example, Nest sells "smart" security cameras, thermostats, and smoke detectors that can link together with other smart-home technologies, including

95. *See* 18 U.S.C. § 2510 (2012).

96. Here, uniqueness is meant to describe the vast portfolio of companies and holdings owned by major technology companies, as well as the variation and multitude of services that they provide.

Google devices, Nest's parent company.[97] Technologies like Apple's Siri, or Amazon's Alexa, function similarly by requiring a connection to a Cloud server to process verbal requests made by the user.[98] Based on the definitions provided in the SCA, these companies seem to neatly fall under both categories of service providers, as they both transmit data electronically between the local device in a person's home and Cloud servers, and then process the data in the Cloud to recognize things like camera movement, sounds, smoke levels, and even the user's location.[99]

What is most interesting about these products is how the SCA's framework can be applied to their parent companies. The statute is silent as to whether a certain percentage of a company's services must be in devoted to electronic communications in order to be classified as an ECSP or RCSP. This becomes tricky when a company is involved in many types of business areas. Take Amazon as an example—Its Alexa device is one of its first devices in the smart-home category. However, Amazon's major business is retail through its e-commerce website.[100] It is not entirely clear if a company that provides Cloud services as one small part of its business—say five percent—would be classified as an ECSP or RCSP, or whether the government can request documents from such a company relating to products or services that are unrelated to SCA jurisdiction. With some companies, like Google, it may not matter because generally all of its products or services are in the form of electronic communications. However, for companies like Amazon, or any other business that only provides a miniscule amount of service or products as electronic communications, it is not entirely clear how the SCA would be applied. Because of the lack of technical language and guidance in the SCA, it appears that any company that provides those types of services at all, would be considered under either category, regardless of the percentage that Cloud services make up of its business.

D. A General Analysis of Cloud Service Providers Under the Fourth Amendment Framework

In *City of Ontario v. Quon,* the Supreme Court presented the idea that digital property should be treated identical to its physical counterparts with regard to Fourth Amendment protections.[101] Some commentators, as well as the Sixth Circuit in *Warshak*, have likened electronic media storage to the renting of physical property, although it differs slightly, because with most

97. *See generally Get more from you Nest with Google*, GOOGLE, INC. (last visited Mar. 12, 2017), https://workswithnest.google.com/ [https://perma.cc/Z9EM-EHMX].

98. *See, e.g.*, Brian Barrett, *What Amazon Echo and Google Home Do With Your Voice Data*, WIRED (Nov. 24, 2017, 7:00 AM), https://www.wired.com/story/amazon-echo-and-google-home-voice-data-delete/.

99. *Id.*

100. Amazon is particularly unique because it has been marketing and developing other services that primarily serve as a benefit to its "Prime" membership base including music and video streaming services, as well as Cloud storage.

101. *See geneally* City of Ontario v. Quon, 560 U.S. 746 (2010)

Cloud services, the data can reside in multiple locations aside from servers owned by the provider.[102] Using the rental property analogy, users can expect to have a reasonable expectation of privacy because courts have determined that such an expectation exists in physical rental properties.[103] The analogy highlights the direct conflict with provisions of the SCA that allow the government to access both content and non-content data through less restrictive mechanisms (e.g., administrative subpoenas and court orders), as that would be akin to allowing the use of administrative subpoenas to search an individual's home.[104]

Even when using the rental property analogy, the third-party disclosure doctrine continues to raise issues and is likely one of the main factors for the failure of courts to reach a consensus. Setting aside agreements on the comparison between Cloud storage and physical records, some courts still choose to apply the third-party disclosure doctrine's analysis, which weakens the argument for constitutional protections.[105] The third-party disclosure doctrine is premised on the notion that an individual's right to privacy in certain information is waived when that information is collected by a service provider or other third-party businesses as a necessary means to provide services or to comply with the law.[106] The equivalent to this waiver occurs either by means of voluntary disclosure when uploading documents for use with an ECSP or RCSP, or through signing user license agreements that have the effect of a waiver.[107]However, this argument is flawed, because in many cases when one uses a Cloud service, the service provider does not necessarily have access to the contents of the records due to encryption.[108]

Even when a service provider does have access to the content of information stored in its Cloud service,[109] there is no reason the Fourth Amendment would not require a warrant to be issued before the government could access any of the content. As mentioned previously,[110] several circuit courts have found that a reasonable expectation of privacy exists in a storage unit.[111] Under this line of thinking, it would be a violation of the Fourth Amendment for the government to access a rental storage unit without a warrant in the same way it would be impermissible for it to access a person's

---

102. *See, e.g.*, Shallman *supra* note 57, at 54; *See also* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010).

103. *See, e.g.*, United States v. Washington, 573 F.3d 279, 284 (6th Cir. 2009); United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997).

104. *See* 18 U.S.C. § 2703 (2012).

105. *See, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 843 (11th Cir. 2010).

106. *See* United States v. Miller, 425 U.S. 435, 444–45 (1976).

107. *See Rehberg*, 611 F.3d at 843.

108. *E.g.*, *Security, Trust + Compliance*, CODE 42 (last visited Mar. 12, 2017), http://www.code42.com/security/ [https://perma.cc/P6RY-P7Q2].

109. *See* Jose Pagliery, *Apple Promises Privacy—But Not on iCloud*, CNN: TECH (Feb. 22, 2016, 1:28PM EST), http://money.cnn.com/2016/02/22/technology/apple-privacy-icloud/ [https://perma.cc/YC4B-M3AW].

110. *Supra* Part IV, Section D.

111. *See E.g.*, United States. v. Johnson, 584 F.3d 995, 1001 (10th Cir. 2009) ("People generally have a reasonable expectation of privacy in a storage unit, because storage units are secure areas that 'command a high degree of privacy.'" (citations omitted)).

digital locker.[112] By using administrative subpoenas and court orders under Section 2703(b), which does not require the same degree of inference that a crime is being committed, the government may violate the Constitution.[113]

V. A THREE-PRONGED SOLUTION TO ESTABLISH CLEAR CONSTITUTIONAL PROTECTIONS FOR INFORMATION STORED IN THE CLOUD

There are several ways to improve the privacy protections for digital information stored in the Cloud. Along with the private sector, each of the three branches of government may offer a different way of establishing clear constitutional protections for digital information. The courts, for example, can determine what limits must be placed on law enforcement's ability to search and seize digital content, in order to comply with the Fourth Amendment. Congress, on the other hand, can amend the current Act to implement the changes this Note proposes. The Executive Branch, through the Department of Justice, or a specialized agency, like the National Telecommunications and Information Administration, can use its expertise to determine how to classify ECSPs and RCSPs, and when warrantless compelled disclosure is appropriate.[114] Finally, the private sector can continue to develop technologies that rely on stronger and novel encryption methods, as well as providing services that cannot be accessed by the provider itself.

A. The Supreme Court Should Expand Riley v. California to Require Warrants for Any Government Access of User Data Held in the Cloud

Riley v. California was a substantial step in setting the limitations of Fourth Amendment protections as they relate to property stored in the Cloud. By holding that police officers did not have a right to access the contents of an individual's phone, even in a search incident to arrest, the Supreme Court held there was an inherent value in one's digital records.[115] Of further importance was the Court's discussion relating to information stored in the Cloud, where it found significant privacy interests existed in digital data that

112. Such as a monthly subscription service like Google Drive, which is used to store electronic information remotely. *See, e.g.*, *Using Drive*, GOOGLE, https://www.google.com/drive/using-drive/ (last visited Apr. 18, 2018).

113. *See* U.S. CONST. Amend. IV; 18 U.S.C. § 2703(b) (2012); Fed. R. Civ. P.41(d).

114. Should an agency like the FCC be used, these determinations would remain independent from the President's policy directions.

115. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014) ("We therefore decline to extend Robinson to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.").

is accessible from a cell phone, but physically located elsewhere.[116] Unfortunately, the Court failed to extend the holding to situations other than searches incident to arrest, which is why it is now necessary to do so.

What is particularly unusual about the holding in *Riley* is that the Court seemedto reason that digital content stored in the Cloud deserves more constitutional protection in instances of a search incident to arrest than physical objects in possession of an individual.[117] This is unconventional because, generally, the Court has found that less constitutional protections exist incident to arrest, especially when officer safety is at issue.[118] In fact, this was the reasoning for the holding in the *Chimel v. California* series of cases that allow officers to rightfully search an individual's person incident to an arrest. The Supreme Court held:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.[119]

It may be that the Court does not expect the contents of a cell phone to be of significant risk to an officer's safety. However, it does not explain why a search of the cell phone's contents would not be permissible after an individual is arrested. Searches already occur regularly with cars that need to be impounded because of an individual's arrest.[120] In fact, one of the arguments made by the Court in *Riley* was that an individual would need a particularly large storage box to carry the number of records stored in a cell phone, and accessing such a box would require a warrant anyway.[121]

---

116. *Id.*at 2491 ("Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter.; See New York v. Belton, 453 U.S. 454, 460, n. 4, (1981) (describing a 'container' as 'any object capable of holding another object'). But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen.").

117. *Id.* at 2491 ("The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files . . . stored in the cloud. Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." (citations ommitted)).

118. *See generally, e.g.*, United States v. Robinson, 414 U.S. 218 (1973)

119. *Robinson*, 414 U.S. at 226 (quotation marks omitted) (quoting Chimel v. California, 395 U.S. 752, 762–763 (1969)).

120. *See e.g.*, *Belton*, 453 U.S. at 460–62 ("[W]e hold that when a policeman has made a lawful custodial arrest of the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of that automobile.").

121. *See Riley*, 134 S. Ct. at 2489 ("Most people cannot lug around every piece of mail that they have received for the past several months, every picture they have taken, or every book or article they have read . . . if they did, they would have to drag behind them a trunk of the sort held to require a search warrant . . . .").

However, a car could easily fit this type of description and is searched regularly without a warrant.

In *Riley*, he Court is limits its holding to a very particular set of circumstances, possibly to limit the restrictions that it places on law enforcement's efforts. However, the Court's detailed analysis of why information stored in the Cloud requires such significant protections is inconsistent with its decision to limit the holding. Applying *Riley*'s holding much more broadly would set clear standards as to the protections digital information held in the Cloud should receive. In essence, this type of information should be treated the same way that most other property is treated under the Fourth Amendment: requiring a warrant to "search and seize." As noted in *Riley*, the argument in favor of allowing officers access to even the local contents (i.e. content stored on the phone as opposed to in the Cloud) of a cell phone in emergency situations requires extraordinary and even life-threatening circumstances.[122] The Court does not appear to apply the same logic to data accessible from a cell phone, but stored remotely.[123]

Apart from extending the holding in *Riley* to other situations, it is also time for the Supreme Court to hear any one of the number of cases dealing with electronic data, and set some type of precedent as to how different digital communications will be protected under the Fourth Amendment. The Court should look to the concurring opinion by Justice Sotomayor in *United States v. Jones*, which discusses the need to reconsider *Miller's* third-party disclosure doctrine in response to the use of modern technology.[124] The Court should also draw upon its assumptions in *City of Ontario v. Quon*, that digital property should be treated the same as its physical counterparts, to find in favor of equal protection for digital communications more generally.[125] In setting a standard, the Court will likely guide any legislative amendments to the SCA, as well as designate the limits of warrantless searches and seizures of digital property. If these changes had been implemented for Barbara in the earlier scenario,[126] she most likely would not have suffered from the public embarrassment and aftermath of the dissemination of her sensitive, private

122. *Id.* at 2493–94 ("[T]here is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, . . . is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone.").

123. *See id.* at 2491.

124. *See* United States v. Jones, 565 U.S. 400, 417 (2012) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." (citation omitted)).

125. *See* City of Ontario, Cal v. Quon, 560 U.S. 746, 760 (2010) ("Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City . . . . [P]rinciples applicable to a government employer's search of an employee's physical office apply with at least the same force . . . in the electronic sphere.").

126. *Supra* Part I.

records because the SEC would not have been able to access the firm's records held by Amazon in the first place.[127]

B. Legislating to Replace or Amend the SCA

The Email Privacy Act is one piece of legislation circulating through Congress, which would amend the SCA.[128] Among other things, the bill amends the SCA such that a warrant would be required for every disclosure of content-based information held by a "third party [service provider] for any length of time."[129] The bill has been passed in the House of Representatives at the time this Note was written, and it is currently being considered by the Senate Committee on the Judiciary.[130] Should it pass, the bill would be an important step towards improving the current state of the SCA, but would not be a complete solution.

While an amendment requiring a warrant for every content-based disclosure may prove effective to significantly increase privacy rights, it would not limit law enforcement from using blanket warrants to access all digital content in possession of a service provider, even when the records are entirely irrelevant to the investigation. A better approach would be to also require some identifying information of the digital content being requested. For example, law enforcement can currently obtain any content-based information from RCSPs through administrative subpoenas, court orders, and with a warrant.[131] Additional requirements should be added that require warrants to specify certain properties of the digital records (e.g. file name, size, type, etc.) before a service provider would be compelled to disclose them. For example, if a bookie was under investigation, the government might list spreadsheet files as the document type in an attempt to find the suspect's client list. Adding this prerequisite would be more consistent with the Fourth Amendment's requirement that the government specify the places and things to be searched and seized.[132] The Email Privacy Act's warrant requirement is a favorable change to the current statute, but it would still need the additional requirements suggested here to ensure that law enforcement is not simply accessing documents through a catch-all method, as is currently allowable.

---

127. At least through the use of Section 2703, although the SEC may have other methods through which it can obtain records from regulated entities.

128. *See* Email Privacy Act, H.R. 387, 115th Cong (2017). At the time this Note was written, the Bill has passed the House of Represantatives, and has been referred to the Senate Judiciary Committee for further action. *See H.R.*387*—Email Privacy Act*, CONGRESS.GOV https://www.congress.gov/bill/115th-congress/house-bill/387/all-actions?q=%7B%22search%22%3A%5B%22email+privacy+act%22%5D%7D&r=1 [https://perma.cc/KT39-DFL7] (last visited Apr. 11, 2017).

129. *See* H.R. 387; *see also, e.g.*, James Stiven, *ECPA Reform Will Protect Privacy and Meet Law Enforcement Needs*, THE HILL:PUNDITS BLOG (June 02, 2016, 3:00 PM EST), http://thehill.com/blogs/pundits-blog/technology/281987-ecpa-reform-will-protect-privacy-meet-law-enforcement-needs [https://perma.cc/3ARW-BA5M].

130. *See See* Email Privacy Act, H.R. 387, 115th Cong (2017).

131. *See* 18 U.S.C. § 2703(b) (2012).

132. *See* U.S. CONST. amend. IV.

Additional amendments should be made to the SCA (or by enacting a new law) that gives NTIA the authority to regulate and classify who is considered as an ECSP or RCSP. Granting such authority to NTIA would create flexibility in regulation and enable the definition of ECSPs and RCSPs to adapt as technology continues to evolve. It would also serve as a way to limit law enforcement from overreaching in its use of warrantless searches and seizures. The NTIA, in particular, would be well suited to handle the classification of providers as it is an agency specializing in communications technology, and already regulates other areas of the Internet and communications law.[133] The SCA and ECPA categories overlap with the use of mobile phones and Internet, both of which are within NTIA's policy purview.[134] Also significant is that NTIA already works with public safety personnel, including law enforcement, through the FirstNet program to regulate emergency telecommunications networks, among other things.[135]

C. An Industry Effort to Promote Privacy Rights

Possibly the most effective solution to solve the lack of Fourth Amendment protection in developing technologies is a formal coalition among technology companies and Cloud service providers to encrypt data, such that not even the providers themselves can access it. This practice is already occurring on occasion, including some instances where the consumer is allowed to use his or her own private encryption key for data access and synchronization with the Cloud.[136] The encryption key is only known to the customer, and the company cannot access it even if it wanted to.[137] Apart from the privacy aspect of this solution, it would also have a secondary benefit of highly increased security for digital information, as the common mantra is that if a backdoor exists, it will eventually be accessible by more people than by which it was intended to be (e.g., hackers).

---

133. *See, e.g.*, *About NTIA*, NAT'L TELECOMM & INFO. ADMIN., https://www.ntia.doc.gov/about (last visited Apr. 18, 2018) ("[NTIA], located within the Department of Commerce, is the Executive Branch agency that is principally responsible by law for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth. . . . Specific NTIA activities include: . . . Developing policy on issues related to the Internet economy, including online privacy, copyright protection, cybersecurity, and the global free flow of information online . . . In addition to working with other Executive Branch agencies to develop Administration positions, NTIA represents the Executive Branch in both domestic and international telecommunications and information policy activities.").

134. *See* 47 U.S.C. § 902 (2012).

135. 47 U.S.C. § 1424 (2012) (titled "Establishment of the First Responder Network Authority").

136. *See, e.g.*, *Features*, CRASHPLAN, https://www.crashplan.com/en-us/features/ [https://perma.cc/9MAF-AYC5] (last visited Apr. 04, 2017).

137. *See Public and Private Keys*, COMODO GROUP, INC., https://www.comodo.com/resources/small-business/digital-certificates2.php [https://perma.cc/F5YQ-8Q4W] (last visited Apr. 2, 2017).

This solution does have its flaws. For one, it would require broad acceptance across the technology and Cloud communities. For those companies that do have access to the Cloud content information of their clients, it would mean losing valuable, marketable information that is often sold or used to improve and develop products—and for smaller companies, such a practice would likely be economically unfeasible. Second, as seen with the Department of Justice breaking into the iPhone of the San Bernardino shooter, [138] it is likely that the government may find its own way to break the encryption.[139] However, the industry may respond by developing stronger encryption standards. Overall, this solution appears to be more of an ideal objective for Cloud service providers to continue working towards rather than a comprehensive solution to resolve the issues with the SCA. This type of solution may also serve as a competitive advantage for companies that can provide privacy assurances to its customers, and even sell them for a fee.

VI. CONCLUSION

When the Stored Communications Act was originally enacted in 1986, digital technology was much simpler than in today's world. Where e-mail was at the frontier of communications technology then, it is now commonplace, and is, for the most part, beginning to overtake mail as the primary form of official communication. Today, people use apps, messaging services, web pages, and other technologies to communicate, both formally and informally, with one another—most of which rely on Cloud technology in some way. Lacking in this technological evolution have been revisions to the SCA that take into consideration how older technologies are being used in new ways, and how new technologies change the behavior of society. Elucidated by the lack of reform is just how vulnerable an individual's private and sensitive information is to intrusion by the government, and to dissemination to the public. It is vital that SCA reform be implemented immediately, so that situations like Barbara's do not prevent individuals from embracing technology and all the benefits that it brings to society.

138. Kevin Johnson et al., *FBI hacks into terrorist's iPhone without Apple*, USATODAY (Mar. 28, 2016) https://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/ [https://perma.cc/8W3E-78U5]

139. Cloud service providers would still likely be accountable for providing the encrypted files to the government without amending the current form of the SCA.