Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud

ABSTRACT

The advent of new communications technologies has generated debate over the applicability of the Fourth Amendment's warrant requirement to communications sent through, and stored in, technologies not anticipated by the Framers. In 1986, Congress responded to perceived gaps in the protections of the warrant requirement as applied to newer technologies, such as email, by passing the Stored Communications Act (SCA). As originally enacted, the SCA attempted to balance the interests of law enforcement against individual privacy rights by dictating the mechanisms by which the government could compel a particular service provider to disclose communications stored on behalf of its customers. However, technological advances since 1986—especially the advent of cloud computing—have rendered the SCA unworkable and unpredictable.

This Note examines how the SCA's compelled disclosure provisions apply to cloud computing services. It begins by discussing the historical precedents for the SCA and its basic provisions. It then demonstrates the complexity of the SCA and shows that cloud computing services may lie beyond the scope of the Act. This Note concludes by examining the current debate over the SCA and recommending that Congress require the government to obtain a warrant to compel service providers to disclose communications stored in the cloud.

TABLE OF CONTENTS

While millions of people rely each and every day on cloud-based computing services, such as Gmail and Facebook,[1] cloud computing probably seems esoteric to laymen. Microsoft Corporation's recent slate of television commercials exploits the technology's mystique to bring "cloud computing" into users' lexicons, juxtaposing superhero-esque comedy with seemingly abstruse cloud computing.[2] In one commercial, a woman sits at an airport with her male companion.[3] She appears distraught over the news that her flight is delayed.[4] To the cue of superhero music, her male companion has an epiphany and saves the day by declaring, "to the cloud!"[5] Despite the woman's newfound serenity, however, she will face limited privacy protections when she goes "to the cloud."[6]

1. DIGITAL DUE PROCESS, COMMENTS ON INFORMATION PRIVACY AND INNOVATION IN THE INTERNET ECONOMY 5 (June 14, 2010), *available at* http://www.digitaldueprocess.org/files/NTIA_NOI_061410.pdf.

2. *See, e.g.*, WindowsVideos, *Airport—To the Cloud—Windows 7*, YOUTUBE (Oct. 25, 2010), http://www.youtube.com/watch?v=Lel3swo4RMc.

3. *Id.*

4. *See id.*

5. *Id.*

6. *See infra* notes 168–190 and accompanying text.

Microsoft's commercials paint cloud computing as a more efficient model for end-users to "create and share. Anywhere."[7] However, the advertisements do not define the "cloud" or warn customers of the privacy implications of storing data there.[8] This Note explores the privacy concerns users face when transmitting and storing communications in the cloud. Additionally, it seeks to determine when the government may compel cloud service providers to disclose the communications they maintain on behalf of end-users.

To ensure the privacy of communications transmitted and stored electronically via new technologies—except when the government followed proper judicial procedures—Congress enacted the Stored Communications Act (SCA) as part of the Electronic Communications Privacy Act of 1986 (ECPA).[9] The SCA provides a web of "Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and [Internet] service providers (ISPs) in possession of users' private information."[10] When Congress enacted the SCA in 1986—four years before the introduction of the World Wide Web in 1990, and eight years before the first web browser in 1994[11]—it did not foresee the advent of cloud computing.[12]

The recent proliferation of cloud computing has generated considerable uncertainty regarding the applicability of the SCA's privacy protections to communications stored in the cloud.[13] The technology industry is increasingly turning away from the personal computing model—in which users access, store, and manage their data and processing locally on their own PCs—and toward cloud computing[14]—in which users go online to access and manage their

7. WindowsVideos, *supra* note 2.

8. *See id.*

9. 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.).

10. Orin S. Kerr, *A User's Guide to the Stored Communication Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004).

11. TIM BERNERS-LEE WITH MARK FISCHETTI, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB 69 (1999); NICHOLAS CARR, THE BIG SWITCH: REWIRING THE WORLD, FROM EDISON TO GOOGLE 17 (2008).

12. *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 2 (2010) [hereinafter *September 23 Hearing*] (statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP) (stating the SCA was based on the assumption that users download their emails to their computers, whereas now emails typically remain on the server after being read by the recipient).

13. *See infra* notes 168–190 and accompanying text.

14. Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 362–63, 364 (2010).

data stored for them on remote servers.[15] As of September 2008, 69 percent of Americans reported having accessed the cloud at least once, either by storing data online or by using web-based software applications.[16] Additionally, a survey conducted in 2010 of 895 technology insiders and critics found that 71 percent of respondents believed most people will employ cloud-computing technologies for work by 2020.[17] Only 27 percent of respondents thought that the most important applications would continue to run on PC operating systems.[18] Unfortunately, the SCA's failure to adequately address privacy issues presented by technologies not anticipated by Congress will likely become more problematic as users increasingly employ cloud computing services.[19]

This Note argues that the SCA may not protect cloud-computing technologies and proposes that Congress amend the Act to rectify this omission. Part I discusses the historical background and basic provisions of the SCA. Part II demonstrates that the SCA, and current interpretations of it by the courts, have created a confusing set of privacy protections, and that the Act's framework may not protect communications stored in the cloud. Part III discusses the current debate and suggestions for reform, and proposes that Congress amend the SCA to ensure that communications stored in the cloud are subject to a warrant requirement, regardless of the characterization of the service or the duration of storage.

I. CLOUD COMPUTING AND THE NEED FOR PROTECTION

A. What is Cloud Computing?

The definition of "cloud computing" is the subject of considerable debate.[20] The National Institute of Standards &

15. *Cloud Computing*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/cloudcomputing/#introduction (last visited Feb. 19, 2011).

16. JANNA QUITNEY ANDERSON & LEE RAINE, THE FUTURE OF CLOUD COMPUTING 8 (2010), *available at* http://www.elon.edu/docs/e-web/predictions/expertsurveys/2010survey/PIP_Future_of_Internet_2010_cloud.pdf.

17. *Id.* at 2.

18. *Id.*

19. *See* DIGITAL DUE PROCESS, *supra* note 1, at 5–6 (explaining that the SCA [ECPA] has not kept up with advances in technology and arguing that the lack of robust privacy protection for data stored in the cloud does not accord with the central role technology plays in communications); *see also* ROBERT GELLMAN, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING 6 (2009), *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf ("While storage of user data on remote servers is not a new activity, the current emphasis on and expansion of cloud computing warrants a more careful look at the privacy and confidentiality consequences.").

20. Soghoian, *supra* note 14, at 364.

Technology (NIST) defines cloud computing as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[21] Essentially, users store or share their information on the Internet and third-party providers maintain that information on remote servers owned or operated by the provider.[22] Users do not own the technology; instead, they rent time or space from the cloud provider.[23] The "cloud" refers to the image depicted on computer network diagrams, which depict the Internet as a "vast cloud at the top of a network chain."[24]

The emergence of cloud computing reflects a paradigm shift from the mainframe and personal computing models of previous decades.[25] Initially, the mainframe computing model allowed users to "operate on slices of a central server's time and resources." [26] In the mainframe era, companies backed by Wall Street purchased mainframes and then sold computer time to other firms.[27] Companies that did not purchase their own mainframes would lease time from the owner and effectively time-shared the computer with other businesses.[28] Mainframe computers had several limitations; for example, only experts operated the enormous machines, which filled entire floors of buildings.[29] Mainframe computing gave way to the personal computing model, which returned to the user physical control over his data.[30] The PC paradigm required users to upgrade their own hardware if they ran out of storage space or needed more computing

21. Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, NIST.GOV (Oct. 7, 2009), http://csrc.nist.gov/groups/SNS/cloud-computing (follow "NIST Definition of Cloud Computing v15" hyperlink).

22. Gellman, *supra* note 19, at 4.

23. *Cloud Computing*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/cloudcomputing/#introduction (last visited Jan. 21, 2011).

24. *Id.*

25. Offline (local) computing and cloud computing are not mutually exclusive, as users today store data locally as well as in the cloud. *See* R. Bruce Wells, Comment, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content*, 12 U. PA. J. CONST. L. 223, 233 (2009) (analyzing applications "blurring" the distinction between offline and online content, like Google's Chrome web browser, enabling a user to "create" a desktop version of an online application).

26. Soghoian, *supra* note14, at 362.

27. PAUL E. CERUZZI, A HISTORY OF MODERN COMPUTING 210 (2d ed. 2003). An early mainframe complex, IBM 7094, could be purchased for $1.6 million, or leased for $30,000 a month. *Id.* at 74.

28. *Id.* at 200.

29. M. Scott Boone, *What Ifs and Other Alternative Intellectual Property and Cyberlaw Story: The Past, Present, and Future of Computing and its Impact on Digital Rights Management*, 2008 MICH. ST. L. REV. 413, 416–17.

30. *Id.*

power.[31] In contrast to the PC model, cloud computing leverages economies of scale:

> In the cloud, everyday processes and information that are typically run and stored on local computers—email, documents, calendars—can be accessed securely anytime, anywhere, and with any device through an Internet connection. Rather than invest in expensive and specialized IT equipment and personnel, customers can rely on the scale and security offered by the cloud providers to access data anywhere Internet access is available.[32]

Businesses have shifted from local to cloud computing to capture a variety of efficiencies, which they can then pass on to end-users.[33] First, businesses entrusting customer and other data to cloud service providers benefit from the providers' ability to aggregate large volumes of data electronically,[34] which enables targeted advertising to customers.[35] Second, businesses storing information in the cloud reap cost savings, because they need not invest in information-technology (IT) infrastructure,[36] and can instead "customize and rapidly scale their IT system for their particular needs."[37] Cloud computing allows businesses to buy only the services they want, and offers the flexibility to set and reset their computing capacities within seconds.[38] These attributes of cloud computing lower market barriers, and help stimulate innovation among developers and small businesses.[39]

Third, cloud services enable businesses and other users to access their data "anytime, anywhere," through the Internet.[40] Fourth, cloud computing services are typically free for the user or at least less expensive than local computing services,[41] and the costs, if

---

31. *Id.* at 363.

32. *September 23 Hearing*, *supra* note 12, at 20–21 (statement of Richard Salgado, Sr. Counsel, Law Enforcement and Information Security, Google, Inc.).

33. *See generally id.* (discussing the various efficiencies cloud computing affords).

34. *Id.* at 26 (statement of Kevin Werbach, Associate Professor of Legal Studies & Business Ethics, University of Pennsylvania).

35. Soghoian, *supra* note14, at 364.

36. *September 23 Hearing*, *supra* note 12, at 47 (statement of David Schellhase, Executive Vice President and General Counsel, Salesforce.com).

37. *Id.* at 29 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation).

38. *Id.* at 29–30 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation); *see also id.* at 14 (statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University) ("[I]f the start-up's business grows rapidly and it needs to expand its computing capacity dramatically to handle a flood of new customers, this is easily done in the cloud, by simply increasing the number of servers the start-up is renting from the provider.").

39. *Id.* at 30 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation).

40. *Id.* at 48 (statement of David Schellhase, Executive Vice President and General Counsel, Salesforce.com).

41. Soghoian, *supra* note14, at 366.

any, are often more predictable.[42] Finally, cloud computing providers regularly back up users' files and store them on multiple servers, thereby protecting users from losing data when their hardware fails.[43]

While cloud computing capitalizes on various efficiencies, it also create "dependency," because users must rely on their service providers to maintain and protect their data.[44] Some businesses, therefore, may want to maintain data in-house rather than outsource their computer storage and processing services. Furthermore, once a user shifts to the cloud for his data storage and processing, return to the PC model may be too onerous.[45] Finally, users must depend on the telecommunications infrastructure that transmits their data to and from the cloud.[46] Despite these limitations, cloud computing may present a more efficient model of computing for some businesses and end-users.[47]

B. Historical Protection of Fourth Amendment Privacy Rights

1. Fourth Amendment

The Fourth Amendment to the U.S. Constitution provides that, "[t]he 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 . . . ."[48] New technologies like cloud computing have stimulated vigorous debate over the extent to which the Fourth Amendment protects individual privacy covers technologies not contemplated by its Framers.[49]

Katz v. United States began the Supreme Court's Fourth Amendment jurisprudence as applied to electronic surveillance.[50] In *Katz*, the government attached an electronic listening device to a public telephone booth and heard the defendant's conversation without obtaining a warrant.[51] The Court held that because the government "violated the privacy upon which [the defendant]

42. *September 23 Hearing*, *supra* note 12, at 47 (statement of David Schellhase, Executive Vice President and General Counsel, Salesforce.com).

43. Soghoian, *supra* note14, at 366.

44. *Cloud Computing*, *supra* note 23.

45. *Id.*

46. *Id.*

47. *See supra* text accompanying notes 32–43.

48. U.S. CONST. amend. IV.

49. *See infra* text accompanying notes 72–85.

50. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 19 (noting that courts have used the reasonable expectation of privacy test since *Katz*).

51. Katz v. United States, 389 U.S. 347, 353 (1976).

justifiably relied,"[52] the warrantless electronic surveillance infringed the defendant's Fourth Amendment rights.[53] The Court noted that the "Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[54]

Building on *Katz*, *Minnesota v. Carter* expounded on the test for determining whether an individual may claim Fourth Amendment protection.[55] To raise a Fourth Amendment claim, an individual must establish both a subjective and an objective expectation of privacy in the place searched.[56] In other words, a defendant must demonstrate not only that he personally expected privacy in the place searched, but that a reasonable person would too.[57] An objectively reasonable expectation is "one that has 'a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.'"[58] Though the standard appears sufficient, one commentator argues that the Court's Fourth Amendment decisions in the wake of *Katz* are "conceptually bankrupt," because neither positive law nor societal understandings justify the Court's decisions.[59] Further, the Supreme Court has increasingly narrowed the scope of the Amendment's protections to such an extent that if an activity can "conceivably" be seen through lawful means, the individual cannot have a reasonable expectation of privacy in that activity.[60]

---

52. *Id.* at 353.

53. *Id.* at 359.

54. *Id.* at 351 (footnotes omitted). *Katz* overturned *Olmstead v. United States*, in which the Court held that the Fourth Amendment protects persons or things against search and seizure, and therefore telephone wiretapping could not violate the Fourth Amendment. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

55. Minnesota v. Carter, 525 U.S. 83, 88 (1998).

56. *Id.*

57. *Id.*

58. *Id.* (quoting Rakas v. Illinois, 439 U.S. 128, 143–44 (1978)).

59. Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1591–92 (2010).

60. *Id.* at 1591. For example, in California v. Ciraolo, the Supreme Court held that officers did not conduct a "search" when they rode in an airplane to view a backyard, because any member of the public would have the same view from the vantage point of an airplane. *Id.* at 1591 n.24 (citing California v. Ciraolo, 476 U.S. 207, 213–14 (1986)).

2. Third Parties

The third-party doctrine limits the extent to which an individual can claim a legitimate expectation of privacy.[61] In *Smith v. Maryland*, the Supreme Court held that an individual lacks a legitimate expectation of privacy in the telephone numbers he dials because "telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[62] Therefore, the Court determined, the pen register—a device that captures the numbers dialed but not the contents of the communication—did not constitute a "search" and did not require a warrant.[63]

Similarly, *United States v. Miller* held that a bank customer lacks a legitimate expectation of privacy in his bank record:[64]

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[65]

These counterintuitive assertions by courts about what reasonable people expect in their interactions with banks and telephone companies has come under withering criticism by Fourth Amendment scholars.[66]

3. Mail

Not all communications accessible to third parties, however, lose Fourth Amendment protection. In *Ex Parte Jackson*, the Court distinguished between third-party access to mail intended to remain confidential between the communicants—like a letter or sealed package—from mail "open to inspection"—like newspapers or magazines "purposely left in a condition to be examined."[67] The Court likened the privacy protections for the former category to the

---

61. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442–43 (1976) (reasoning that data maintained by a third-party is not subject to traditional Fourth Amendment protections), *superseded by statute*, Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697.

62. Smith v. Maryland, 442 U.S. 735, 742 (1979).

63. *Id.* at 745–46.

64. *Miller*, 425 U.S. at 442.

65. *Id.* at 443.

66. *See* Slobogin, *supra* note 59, at 1591–92 (discussing survey results finding that "transaction surveillance, as well as overt public camera surveillance are viewed, on average, as more intrusive than a roadblock, and government efforts to access records from websites, ISPs, pharmacies, and banks are perceived to be as intrusive as a search of a car").

67. *Ex Parte* Jackson, 96 U.S. 727, 733 (1878).

protections required when the government seeks to search papers in an individual's home:[68]

> Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.[69]

To examine the contents of a sealed letter or package placed in the mail, the government must either obtain a warrant or gain the consent of the addressee.[70] In contrast, mail "open to inspection" does not implicate the Fourth Amendment, and the Court, in dicta, assumed that Congress could enact legislation permitting the postal service to inspect such mail and even refuse to deliver it.[71]

4. Computers

An additional gloss on Fourth Amendment privacy rights has developed to address the applicability of the Fourth Amendment to PCs.[72] Courts have generally held that individuals have legitimate expectations of privacy in their home computers.[73] However, some courts have found that individuals who store documents on a public computer do not have a reasonable expectation of privacy in those documents.[74] For example, *Wilson v. Moreau* held that a public library employee lacked a reasonable expectation of privacy in documents stored on the library's computer system because the library was open to the public, the computers were available to the public, documents stored on the computer were accessible to other users, and emails stored on the system were transmitted through a shared network.[75]

---

68. *Id.*

69. *Id.*

70. *Id.* at 735.

71. *Id.* at 735–36.

72. *See infra* text accompanying notes 73–75.

73. *See, e.g.*, United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

74. *See* Wilson v. Moreau, 440 F. Supp. 2d 81, 104 (D.R.I. 2006).

75. *Id. Wilson* further acknowledged that courts typically find that individuals have fewer privacy protections in the workplace than in the home. *Id.* at 103; *see also* City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (reasoning that even if government employee had reasonable expectation of privacy in his text messages, the "special needs of the workplace" permit the employer to conduct warrantless search provided that the search is "reasonable").

C. Need for the Law

In the 1980s, the development and growth of new communication technologies created uncertainty regarding the extent to which the Fourth Amendment applied to new technologies like electronic mail.[76] During this time, the government demanded that communications companies disclose email messages, without first seeking a warrant.[77] Recognizing the need to clarify existing privacy protections, as applied to newer technologies, Congress commissioned the Office of Technology Assessment (OTA) to conduct a report on federal government IT and civil liberties.[78]

In October of 1985, OTA issued its report, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties*.[79] The report noted that while the principle behind the Fourth Amendment remained relevant, the existing statutes and common law failed to adequately address new electronic surveillance technologies.[80] For example, although first-class letters enjoyed robust privacy rights, the protection afforded mail transmitted electronically remained "weak, ambiguous, or nonexistent."[81] The OTA therefore recommended that Congress answer the key policy issue of how to balance civil liberty interests with the needs of law enforcement.[82]

Both the House and Senate promulgated bills designed to strike the proper balance.[83] The debates in Congress debates were animated by concerns that the "gap" between privacy protections for traditional mail and email might deter the adoption and development of these new technologies, encourage unauthorized users to access the private communications of others, and threaten the admissibility of evidence.[84] Further, Congress expressed concern that the "precious

76. *See* OFFICE OF TECH. ASSESSMENT, U.S. CONG., FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 21 (1985) [hereinafter OTA REPORT] (noting that the uncertainty led some courts to look to Congress for guidance).

77. 132 CONG. REC. S7987-04 (1986) (statement of Sen. Patrick Leahy).

78. OTA REPORT, *supra* note 76, at iii.

79. *Id.*

80. *Id.* at 3, 22.

81. *Id.* at 45.

82. *Id.* at 12.

83. *See* H. R. REP. NO. 99-647, at 1 (1986) (discussing House Bill 4952); S. REP. NO. 99-541, pt. 3, at 5 (1986) (recommending Senate Bill 2575 as striking "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies").

84. S. REP. NO. 99-541, pt. 3, at 5; H. R. REP. NO. 99-647, at 19.

right" of privacy would diminish without congressional intervention to "ensure the continued vitality of the Fourth Amendment."[85]

D. Stored Communications Act

In light of OTA's findings, Congress enacted the Stored Communications Act (SCA) as part of the Electronic Communications Privacy Act (ECPA) of 1986.[86] Congress touted the SCA as aligning newer forms of technology with the Fourth Amendment and preserving the "vitality" of the Amendment by ensuring that privacy protections "kept pace" with current advances in technology.[87] Congress, under the SCA, enacted privacy measures to protect both the content of communications—"any information concerning the substance, purport, or meaning of the communication"[88]—as well as non-content information[89]—which encompasses both transactional records, such as account logs, and customer information, such as users' names, addresses, and telephone numbers.[90] This Note focuses on the contents of "electronic communications."[91]

1. Different Services

The Act covers two types of services: electronic communication services (ECS) and remote computing services (RCS).[92] An ECS means "any service which provides to users thereof the ability to send or receive wire or electronic communications."[93] Under § 2703(a) of the SCA, the government may require an ECS provider to disclose the contents of a wire or electronic communication in "electronic storage,"[94] which refers to "any temporary, intermediate storage of a

85. H. R. REP. NO. 99-647, at 19.

86. *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.).

87. H. R. REP. NO. 99-647, at 18.

88. 18 U.S.C. § 2510(8) (2006).

89. *Id.* § 2703(c).

90. Thomas Dukes , Jr. & Albert C. Rees, Jr., *Military Criminal Investigations and the Stored Communications Act*, 64 A.F. L. REV. 103, 106–07 (209). *See also* 18 U.S.C. § 2703(c) (2006).

91. "Electronic communication" is "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) (2006). The term "electronic communication" excludes: (1) wire or oral communication; (2) communication through a tone-only paging device; (3) communication from a tracking device; or (4) electronic funds transfer information. *Id.* § 2510(12)(A)–(D).

92. *Id.* § 2703(a)–(b).

93. *Id.* § 2510(15).

94. *Id.* § 2703(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."[95]

An RCS, by contrast, provides computer storage or processing services to the public by means of an electronic communications system.[96] Under § 2703(b), the government may compel disclosure by an RCS provider only if the provider holds or maintains the communication: (1) "on behalf of" its customers;[97] and (2) "solely for the purpose of providing storage or computer processing" to the customers, meaning that the provider is authorized to access the contents of communications only to provide such storage or computer processing services.[98] Law enforcement may compel disclosure of customer communications under different circumstances, depending on how the communication is stored, whether by an ECS or RCS, and the duration of storage.[99] Section 2703 of the SCA dictates what the government must do to compel disclosure of communications and records stored by third-party service providers.[100] Different standards apply to communications stored by ECS and RCS providers.[101] For communications in electronic storage for 180 days or fewer by an ECS provider, the government may require the disclosure of customer communications only with a federal or state warrant.[102]

To compel an RCS provider to disclose the contents of a communication or to compel an ECS provider to disclose communications it has maintained for longer than 180 days,[103] the government may: (1) obtain a court order and provide notice to the customer;[104] or (2) obtain an administrative, grand jury, or trial

95. *Id.* § 2510(17).

96. *Id.* § 2711(2) An "electronic communications system," as used in the definition of an RCS, is "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." *Id.* § 2510(14).

97. *Id.* § 2703(b)(2)(A).

98. *Id.* § 2703(b)(2)(B).

99. *See id.* § 2703(a)–(b).

100. *Id.* § 2703.

101. *Id.* § 2703(a).

102. *Id.*

103. *Id.* § 2703(a)–(b).

104. *Id.* § 2703(b)(1)(B)(ii). The SCA provides for delayed notice of 90 days, provided that the government has "reason to believe that notification of the existence of the court order may have an *adverse result*." *Id.* § 2705(a)(1)(A) (emphasis added). 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 a trial." *Id.* § 2705(a)(2)(A)–(E).

subpoena and notify the customer;[105] or (3) obtain a warrant, with or without notice.[106] For the sake of clarity, this Note will refer to the provisions permitting disclosure pursuant to a court order, subpoena, or warrant as the "tripartite standard."

2. Different Standards

As outlined above, the SCA allows the government to compel service providers to disclose communications after obtaining court authorization—a warrant, court order, or subpoena—depending on the circumstances.[107] However, the government must obtain a warrant to compel an ECS provider to disclose the contents of a communication maintained in "electronic storage" for 180 days or fewer.[108] For the government to obtain a warrant, the Fourth Amendment requires it to show probable cause.[109] The "probable cause" standard ensures that, under the totality of circumstances—including reasonable inferences drawn therefrom—the government has established at least a "fair probability" that the defendant committed the crime.[110] This standard, while more exacting than the standards for court orders and subpoenas,[111] does not require certainty.[112]

The second mechanism is the court order, available only for communications held by an ECS provider in "electronic storage" for not more than180 days, or maintained by an RCS provider for any length of time.[113] The court order requires that the government put forth "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[114] The "specific and articulable facts" standard is an "intermediate" standard,

---

105. *Id.* § 2703(b)(1)(B)(i). Notice may be delayed for 90 days if the government has "reason to believe that notification of the existence of the [administrative] subpoena may have an adverse result." *Id.* § 2705(1)(B). The definition of "adverse result" is the same as for court orders. *Id.*

106. *Id.* § 2703(b)(1)(A).

107. *Id.* § 2703(a)–(b).

108. *Id.* § 2703(a).

109. U.S. CONST. amend. IV.

110. United States v. Valdivieso Rodriguez, 532 F. Supp. 2d 332, 340 (D.P.R. 2007).

111. *See In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010) (citing S. REP. 103-402, at 31 (1994)).

112. *Valdivieso Rodriguez*, 532 F. Supp. 2d at 340.

113. 18 U.S.C. § 2703(a)–(b).

114. 18 U.S.C. § 2703(d).

lower than probable cause but more demanding than the reasonable relevance standard that applies to subpoenas.[115]

The third option is an administrative, grand jury, or trial court subpoena.[116] The standard for issuing a subpoena is "reasonable relevance,"[117] requiring the government to show that the information it seeks is reasonably relevant to a criminal investigation.[118]

The different standards mean that electronic communications are subject to greater or lesser privacy protections depending on the characterization of the service (ECS or RCS) and the duration of the storage.[119] To review, if the service is characterized as providing ECS and the communication has been in "electronic storage" for 180 days or fewer, the government must obtain a warrant by establishing probable cause, the strictest standard. If the service is an RCS, though, the government need only provide notice and establish reasonable relevance to secure a subpoena compelling disclosure. Thus, communications stored by ECS providers receive greater protections against compelled disclosure to the government, provided the communications have been stored for no more than 180 days, because the government must satisfy a stricter standard to obtain the communication. With RCS providers, the government can compel disclosure upon any of the three showings in the tripartite standard, including the most lenient threshold of showing reasonable relevance, to access the communication.

II. THE SCA AS INTERPRETED FAILS TO PROTECT USERS' PRIVACY

The extent of an individual user's privacy in the cloud turns on the characterization of the service provider and the particular content under a complicated analytical framework.[120] The rubric requires two characterizations: First, is the service an ECS or an RCS, and if so, does the communication fall under the requirements for that service?; Second, if the service is an ECS, has the communication been stored

115. *See* In re *Application of the U.S. for an Order*, 620 F.3d at 314; Patricia L. Bellia & Susan Freiwald, *Law in a Networked World: Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 128 (2008).

116. 18 U.S.C. § 2703(b)(1)(B)(i); *see also In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611–12 (E.D. Va. 2008) (holding that 18 U.S.C. § 2703 does not permit disclosure to a governmental entity pursuant to a civil discovery subpoena).

117. Warshak v. United States, 490 F.3d 455, 468 (6th Cir. 2007), *vacated on other grounds*, 532 F.3d 521 (6th Cir. 2008).

118. Bellia & Freiwald, *supra* note 115, at 128. This showing is typically not subject to judicial review. *Id.*

119. *Compare* 18 U.S.C.§ 2703(a) (dealing with ECS), *with* 18 U.S.C. § 2703(b) (dealing with RCS).

120. *See* 18 U.S.C § 2703(a)–(b).

for 180 days or fewer? This Part explores why the SCA's complex framework fails to adequately protect computer users' privacy in the cloud.

A. Distinguishing between Two Types of Services: ECS and RCS

The first step in analyzing whether a particular communication is subject to the warrant requirement under the SCA is to characterize the cloud provider's service as either an ECS or an RCS.[121] This initial characterization is largely a legal fiction, as most cloud-based ISPs provide both ECS and RCS.[122] However, characterizing the service as ECS or RCS remains critical in determining the protections afforded to communications maintained by that service.[123]

The SCA supplements Fourth Amendment protections, and if a given service cannot be characterized as an ECS or an RCS, the content held by the provider receives only the protections of the Fourth Amendment.[124] Although the Fourth Amendment imposes a warrant requirement, the OTA Report found that courts deemed the Warrant Clause inapplicable to newer technologies.[125] Therefore, characterizing the service as either an ECS or an RCS not only determines the protections afforded to a particular communication under the SCA,[126] but also determines whether the particular communication will even receive protection against compelled disclosure to the government.[127]

If the service enables users "to send or receive wire or electronic communications,"[128] and is thus an ECS, the Act protects the communication, so long as the ECS provider maintains the communication in "electronic storage."[129] Two dominant interpretations of "electronic storage" limit the feasibility of characterizing cloud-based email services as maintained therein by an

---

121. *See id.* (demonstrating that the level of protection against compelled disclosure depends on the characterization of the particular service).

122. *See In re* Application of the U.S. for a Search Warrant, for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Commc'n Servs. to Not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009).

123. *Id.* (emphasis added).

124. Kerr, *supra* note 10, at 1213.

125. *See* OTA REPORT, *supra* note 76, at 22 (finding that statutory and common law failed to address new technologies); *see also id.* at 45 (distinguishing between the privacy protections afforded first-class letter mail and that afforded electronic mail).

126. *See* 18 U.S.C. § 2703(a)–(b).

127. Kerr, *supra* note 10, at 1213.

128. 18 U.S.C. § 2510(15).

129. *Id.* § 2703(a); *see also. id.* § 2510(17) (stating that "electronic storage" refers to either "temporary, intermediate storage . . . incidental to the electronic transmission thereof," or storage for backup purposes).

ECS provider.[130] First, according to the self-described "traditional narrow interpretation" of the U.S. Department of Justice (DOJ), a particular communication is not in "electronic storage" unless stored in the course of transmission by a service provider; a communication stored after transmission has been completed cannot be in "electronic storage."[131] Under the DOJ's definition, an email that has been opened by its recipient is no longer in "electronic storage," but an email not yet opened by its recipient remains in "temporary, intermediate storage."[132] Therefore, the ISP provides ECS when it maintains emails on the server, but only until the recipient accesses the message.

The DOJ's distinction between opened and unopened emails presupposes that backup storage is limited to that incidental to transmission,[133] contrary to statements in the legislative history distinguishing between transmission and backup storage. A 1986 House report noted that the House Judiciary Committee distinguished between storage "associated with transmission and incident thereto," and that of a "back-up variety."[134] By differentiating between storage incidental to transmission and storage for backup purposes, this statement undermines the assumption that storage must be incidental to transmission.[135]

The alternative approach, advocated by the Court of Appeals for the Ninth Circuit, concludes that emails remaining on an ISP's server after delivery are in "electronic storage," regardless of whether the recipient has accessed the message.[136] *Theofel v. Farey-Jones*

130. *See infra* text accompanying notes 131–158.

131. COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, 123 (3d ed. 2009), *available at* http://www.cybercrime.gov/ssmanual/03ssma.pdf [hereinafter DOJ SEARCH MANUAL]. Additionally, the DOJ interprets "backup" storage as "protect[ing] the communication in the event the system crashes *before* transmission is complete." *Id.* at 124 (emphasis added). The statutory definition of "electronic storage" includes communications stored incidental to transmission, and storage "for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(A)–(B). According to the DOJ, the words "such communication" imply that "messages that are in post-transmission storage after transmission is complete, are not covered by [the backup storage provision] of the definition of 'electronic storage.'" DOJ SEARCH MANUAL, *supra*, at 124.

132. DOJ SEARCH MANUAL, *supra* note 131, at 123–24.

133. DOJ SEARCH MANUAL, *supra* note 131, at 123.

134. H. R. REP. NO. 99-647, at 68 (1986).

135. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2003) (stating that the DOJ's interpretation renders the "backup" storage provision redundant).

136. *Theofel*, 359 F.3d at 1075, 1077. The DOJ rejects the Ninth Circuit approach, arguing that *Theofel* "confuses 'backup protection' with ordinary storage of a file." DOJ SEARCH MANUAL, *supra* note 122, at 125. Likewise, the Ninth Circuit deems the DOJ interpretation "erroneous," as "prior access is irrelevant to whether the messages at issue were in electronic storage." *Theofel*, 359 F.3d at 1077.

found that ECS providers hold emails after transmission for purposes of backup protection under § 2510(17)(B).[137] According to *Theofel*, the DOJ's interpretation of "backup" would deprive § 2510(17)(B) of independent meaning because almost all messages backed up on a server also lie in "temporary, intermediate storage."[138] The Ninth Circuit's concluded that an ISP provides ECS when it stores email, and that an ISP stores an email on its server after delivery as a second copy of the message in case the user wants to download the message again.[139] *Theofel* accordingly held that an ISP provides ECS when it maintains email on its server after transmission, because the email resides in "electronic storage" for backup purposes and remains there until the underlying message has expired in its "normal course."[140] This holding, if read broadly, appears to encompass both cloud-based and local-storage email systems.[141] The Ninth Circuit in dicta, however, suggested that the opinion may not apply to webmail; that is, cloud-based email.[142]

Although consistent with the legislative history of the SCA, the Ninth Circuit's approach warrants criticism for treating webmail differently from traditional email.[143] A broad reading of *Theofel* would seem to allow emails transmitted through, and stored on, any email system to fall under the "backup" storage provision,[144] thereby providing warrant protection for communications that the DOJ would deny.[145] Yet, dicta in *Theofel*, as well as later opinions by other courts,

---

137. *Theofel*, 359 F.3d at 1075.

138. *Id.* at 1076; *see also* Robert M. Goldstein & Martin G. Weinberg, *The Stored Communications Act and Private E-Mail Communications: The Government's Unconstitutional Policy of Seizing Private E-Mails Without a Warrant or Notice*, 31 CHAMPION 18, 23 (2007) ("The government's interpretation of *electronic storage* essentially guts the warrant requirement of § 2703(a).").

139. *Theofel*, 359 F.3d at 1075.

140. *Id.* at 1076 ("Where the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages."). In the absence of explicit guidance as to what constitutes the "normal course," one commentator argues that the test is "whether the user or employees of the service provider have reason to believe that they may need to access an additional copy of the file in the future." Kerr, *supra* note 10, at 1218 (citing *Theofel*, 359 F.3d at 1075).

141. *See infra* text accompanying notes 148–149 (explaining the difference between webmail and traditional email).

142. *Theofel*, 359 F.3d. at 1077 ("A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes.").

143. *See supra* notes 140–142 and accompanying text (describing in *dicta* how *Theofel* left open whether the holding would apply to cloud-based email systems).

144. *Theofel*, 359 F.3d at 1076.

145. *See* DOJ SEARCH MANUAL, *supra* note 131, at 123–24 (arguing that opened emails are not in "electronic storage").

suggest that communications stored in the cloud are not stored for "backup purposes."

A third approach attempts to reconcile the two dominant interpretations of "electronic storage" advocated by the DOJ and the Ninth Circuit, by adopting the dicta from *Theofel* to find the opinion inapplicable to cloud-based email.[146] The Central District of Illinois held in *United States v. Weaver* that courts may issue a trial subpoena to compel ISPs to produce the contents of opened emails stored by a webmail provider for 180 days or fewer because such emails are not in "electronic storage."[147] *Weaver* narrowly construed *Theofel* as applying only to email systems in which users download messages from the ISP's server onto their own computers.[148] In contrast, *Weaver* reasoned that users of "web-based"—in other words, cloud—email systems, like Hotmail, generally access their email through the server, and if they save a message, they typically leave it on the provider's server.[149] By adopting the dicta from *Theofel*, *Weaver* concluded that cloud-based email does not enjoy the same privacy protections as traditional email and that email stored only in the cloud should not be considered stored for backup purposes.[150]

Furthermore, in *Crispin v. Christian Audigier, Inc.*, a lower court in the Ninth Circuit applied *Weaver* and the dicta from *Theofel* to conclude that once opened, private messages maintained on cloud-based social networking websites Facebook and MySpace are maintained by RCS providers.[151] Again applying *Theofel*, *Crispin* then held that Facebook's wall postings and MySpace's comment services were ECS, and if either the user or the server fails to delete the communication, the communication remains stored for backup purposes.[152] Given the distinction between webmail and traditional email raised in dicta in *Theofel*, the question at least remains open

146. *See* United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009).

147. *Id.* at 771–73.

148. *Id.* at 772.

149. *Id.* at 772 (citing Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 917 (W.D. Wis. 2002)).

150. *See Theofel*, 359 F.3d at 1077 (arguing that if the message remains only on the RCS, then the message is not stored for backup purposes); Weaver, 636 F. Supp. 2d at 772 (arguing that cloud-based emails stored only on the server are not stored for backup purposes).

151. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010). This conclusion is consistent with the DOJ's approach, as any communication once opened is maintained by an RCS provider, if at all. *See* DOJ SEARCH MANUAL, *supra* note 131, at 123–24.

152. *Crispin*, 717 F. Supp. 2d. at 989. *Crispin* applied *Theofel* to wall postings and comments, by applying the rule from *Theofel* that email services are ECS, and then concluding that the comments must be stored for backup purposes because they could not be stored in "temporary, intermediate storage." *See id.* ("Unlike an email, there is no step whereby a Facebook wall posting must be opened, at which point it is deemed received."). However, *Crispin* alternatively held that the wall posting and comment services were RCS. *Id.* at 990.

whether the holding from *Theofel* applies to cloud-based email systems. In sum, whether a user's communication falls under the warrant requirement, or whether a less demanding standard than probable cause could compel its production, depends not only on the characterization of the service, but also on the jurisdiction.[153]

As applied to cloud computing, the extent to which communications—such as emails—sent through cloud-based servers will receive warrant protection remains unclear.[154] The DOJ approach recognizes limited warrant protection, if any, for electronic communications, because any email accessed by the recipient, whether through a traditional email system or the cloud, is not maintained in "electronic storage" by an ECS.[155] In contrast, the Ninth Circuit's approach in *Theofel* appears to provide robust privacy protections for communications stored in any email system by deeming those communications in "electronic storage" by an ECS provider.[156] In dicta, though, it left open whether this rule would actually apply to cloud-based email systems.[157] A third approach, in *Weaver*, cabins *Theofel*'s construction of "backup" storage to traditional email systems.[158] The different approaches to the "electronic storage" provision as applied to cloud computing means that communications sent and maintained in cloud-based email systems may lie outside the statutory protection afforded communications stored by ECS providers.

In contrast to an ECS provider, an RCS provider offers the public computer storage or processing services.[159] Although the SCA does not define "computer storage," the term is generally interpreted to mean remote storage.[160] The term "processing services" is also left undefined, but the legislative history indicates that it means

153. *See* 18 U.S.C. § 2703(a)–(b) (2006) (different protections for ECS and RCS); *Theofel*, 359 F.3d at 1077 (rejecting the DOJ's interpretation of "electronic storage"); DOJ SEARCH MANUAL, *supra* note 122, at 125 (rejecting the Ninth Circuit's interpretation of "electronic storage").

154. *See infra* text accompanying notes 155–158.

155. *See* DOJ SEARCH MANUAL, *supra* note 131, at 123–24 (stating that communications maintained by the service provider after transmission is complete are not in "electronic storage").

156. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2003) (stating that communications maintained after transmission are in "electronic storage" until the copy has expired in the "normal course").

157. *See id.* at 1077 (reasoning that a message is not stored for backup purposes if the RCS is the only place the message is stored).

158. United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009). Under *Weaver*, emails sent through cloud-based systems are not in "electronic storage" by an ECS provider, and thus are not subject to the warrant requirement, because the email is not in "backup" when it remains only on the server. *Id.*

159. 18 U.S.C. § 2711(2).

160. *See* Kerr, *supra* note 10, at 1229–30.

outsourcing functions.[161] To qualify for the protections the statute affords communications stored by an RCS provider, the RCS provider must maintain the communication: (1) "on behalf of" the RCS provider's customer;[162] and (2) "solely for the purpose of providing storage or computer processing" to the customer, such that the provider's authority to access the communication is limited to the extent necessary to provide storage or computer processing services.[163]

One court found that the video upload website YouTube provided RCS for users, though the court did not explain its reasoning.[164] Likewise, although *Crispin* held that Facebook's wall postings and MySpace's comment services constituted ECS, it held in the alternative that the services were RCS.[165] As to RCS, *Crispin* concluded that although Facebook and MySpace maintained communications for display as well as for storage purposes, display was necessary in order to enable users to retrieve their stored messages. [166] Display and storage were therefore inseparable, and thus Facebook and MySpace maintained the communications "solely" for storage purposes.[167]

B. Example

As an example of the practical problems inherent in applying this framework to cloud services, consider Gmail, Google's cloud-based

161. *Id.* at 1230. *See* S. REP. NO. 99-541, at 3 (1986) ("For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services.").

162. 18 U.S.C. § 2703(b)(2)(A).

163. *Id.* § 2703(b)(2)(B).

164. Viacom Int'l, Inc. v. YouTube, Inc., 253 F.R.D. 256, 258, 264 (S.D.N.Y. 2008).

165. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989–90 (C.D. Cal. 2010).

166. *Id.* It is unclear why *Crispin* failed to conclude that Facebook could not provide RCS as it does not maintain communications "solely" for computer processing and storage, given that Facebook's Privacy Policy indicates that it collects "content" information when a user posts on another user's wall, and uses the information to serve personal advertising and other services to users. *See Facebook's Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last updated Dec. 22, 2010). Facebook collects "content" information when the user updates his status, uploads photos or videos, shares a link, creates an event or group, makes a comment, writes on someone's wall, writes a note, or sends a private message to another user. *Id.* Facebook lists the following ways it uses such content information: (i) to manage the service; (ii) to make announcements; (iii) to serve targeted advertising; (iv) to serve social ads; (v) to supplement a user's profile; (vi) to provide suggestions; and (vii) to help a user's friends locate the user. *Id.* Although *Crispin* rejected the display argument because the storage does not have to be for the benefit of the user but can be for the benefit of the ISP, advertising could only be construed as "processing services" under a very broad reading of "processing services." *See Crispin*, 717 F. Supp. 2d at 990.

167. *Crispin*, 717 F. Supp. 2d at 989–90.

email service.[168] The two-step framework first requires characterizing the service and determining whether the communication satisfies the requirements for protection, and then to calculate the duration of storage. The first issue is whether Gmail's cloud services are better characterized as either ECS or RCS, or neither. Gmail's communication services satisfy the definition of an ECS, because users can "send or receive . . . electronic communications" through instant messaging ("chat") and email.[169] However, the storage of emails transmitted through Gmail's server may not qualify as "electronic storage" for a few different reasons.

First, once transmission is complete, the email no longer remains in "temporary, intermediate storage" because its storage is no longer "incidental" to transmission.[170] Second, Gmail encourages users to save their emails even after transmission is complete, by providing users more than 7000 MB of free storage and allowing users to purchase additional storage.[171] Third, Gmail encourages users to archive their messages "so that they are always available and always searchable."[172] Because such storage is neither temporary nor incidental to transmission, an email sent through Gmail's server cannot receive post-transmission protection unless stored for "backup" purposes.

The three different constructions of § 2703(a), discussed previously, probably provide different answers to the question of whether an email sent through Gmail is stored for "backup purposes." Under the DOJ's approach, once the recipient of the email retrieves the message, the email is no longer stored for backup purposes.[173] Although a court following *Theofel* may find that Gmail stores communications on its server for "backup purposes," and therefore

168. *See What Happens to Messages Stored on Gmail's Servers*?, GOOGLE, http://mail.google.com/support/bin/answer.py?answer=13288 (last updated Jan. 24, 2011) (discussing how messages are stored on Gmail's servers, rather than on a user's computer, and the user may download a particular message to his computer).

169. 18 U.S.C. § 2510(15) (2006); *see also Getting Started Guide*, GOOGLE, http://mail.google.com/support/bin/static.py?page=guide.cs&guide=24916 (last visited Feb. 4, 2011) (providing a brief overview of Gmail's email features).

170. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003) (explaining that "temporary, intermediate storage" is limited to storage of messages "pending delivery"); DOJ SEARCH MANUAL, *supra* note 131, at 123 (explaining that "electronic storage" is limited to storage "made in the course of transmission").

171. *Top 10 Reasons to Use Gmail* , GOOGLE, http://mail.google.com/mail/help/about.html (last visited Feb. 4, 2011).

172. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 977 n.20 (C.D. Cal. 2010) (quoting Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 378–79 (2009)).

173. *See* DOJ SEARCH MANUAL, *supra* note 131, at 123–24.

provides "electronic storage,"[174] *Weaver* counsels against applying *Theofel* to web-based email systems.[175] Thus, although Gmail's privacy policy asserts backup protection of email communications,[176] the fact that they remain on the server means that, except under *Theofel*, the communications are not maintained in "electronic storage" for backup purposes.[177] For cloud-based email then, the DOJ and *Weaver* likely would find that the government need not obtain a warrant to compel the ISP to disclose communications stored on the server, because the ISP's services lie outside the Act's provisions for an ECS.[178] Therefore, for emails and other communications on Gmail to enjoy protection under the SCA, they must be deemed stored by an RCS provider.

Assuming for the sake of argument that Gmail's communication services satisfy the definition of an RCS under § 2711(2), by providing public computer storage or processing services,[179] Gmail still fails to satisfy the conditions for protection as communications stored by an RCS.[180] Gmail maintains emails sent by users to process user inquiries and improve Gmail services,[181] thus satisfying the requirement of § 2703(b)(2)(A) that communications be held on a Gmail customer's behalf.[182] However, Gmail's Privacy Policy states that Gmail may access user communications to improve and develop new advertising services.[183] Because Gmail maintains and accesses communications to improve services that constitute neither remote storage nor outsourcing functions, Gmail fails to satisfy the second requirement for an RCS, as it does not maintain communications "*solely* for the purpose of providing storage or computer processing services."[184] This result comports with *Flagg v. City of Detroit*, in which the Eastern District of Michigan concluded that although an RCS provider stored text messages, the communications did not receive protection under the RCS provisions

174. *See Theofel*, 359 F.3d at 1076.

175. *See* United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009).

176. *Privacy Policy*, GOOGLE, http://www.google.com/privacypolicy.html (last modified Oct. 3, 2010).

177. *Weaver*, 636 F. Supp. 2d at 772; DOJ SEARCH MANUAL, *supra* note 131, at 123–24. *But see Theofel*, 359 F.3d at 1076.

178. *See supra* text accompanying note 174. *See also* 18 U.S.C. § 2703(a) (2006) (showing that communication not maintained in electronic storage by an ECS provider does not require a warrant under the SCA).

179. *Id.* § 2711(2).

180. *See infra* notes 182–184.

181. *Privacy Policy*, *supra* note 176.

182. *See* 18 U.S.C. § 2703(b)(2)(A).

183. *Privacy Policy, supra* note 176.

184. *See* 18 U.S.C.S. § 2703(b)(2)(B) (Lexis) (emphasis added).

because the contract between the customer and the service provider allowed the provider to retrieve text messages from its archives.[185] This meant it did not maintain the messages "solely" for storage or computer processing.[186]

Gmail's services are distinguishable from those analyzed in *Crispin* because in *Crispin*, the social networking websites had to display communications to enable users to retrieve them from storage,[187] whereas Gmail provides advertising services that are unnecessary for users to access emails.[188] Thus, when a customer consents to a user agreement which permits the service provider to access his data to provide targeted advertising, the user's emails may not be protected as communications maintained by an RCS provider.[189] As this analysis makes clear, cloud services such as Gmail may not qualify, under the SCA, as either an ECS or RCS, leaving users with the uncertain protections of the Fourth Amendment.[190]

C. Adding a Second Layer: The 180-Day Rule

Even assuming that a particular cloud service could be characterized as an ECS, the 180-day rule imposes an additional layer of complexity as to whether a communication is subject to the warrant requirement.[191] While the government must obtain a warrant to compel a service provider to disclose communications in "electronic storage" for 180 days or fewer, those stored for 181 days or more are obtainable under the tripartite standard.[192]

The legislative history illuminates the basis for the 180-day rule, although without empirical support. According to the 1986 House Report,

> Most—if not all—electronic communications systems (such as electronic mail systems), however, only keep copies of messages for a few months. To the extent that the record is

185. Flagg v. City of Detroit, 252 F.R.D. 346, 359, 363 (E.D. Mich. 2008).

186. *Id.*

187. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 990 (C.D. Cal. 2010).

188. *See Privacy Policy, supra* note 176. There is no suggestion in the privacy policy that advertising services are necessary to enable users to send and receive communications sent through its servers. *See id.*

189. William J. Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1214 (2010).

190. *See* Kerr, *supra* note 10, at 1213 (explaining that when a particular service cannot be characterized as either ECS or RCS then only Fourth Amendment protections apply, but the SCA was enacted to address gaps in applying Fourth Amendment to new technologies).

191. *See* 18 U.S.C. § 2703(a) (2006) (demonstrating that once the service is characterized as an ECS, different protections apply depending on the duration of storage).

192. *Id.*

> kept beyond that point it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.[193]

According to Professor Kerr, the 180-day rule may be a relic of the Fourth Amendment's abandonment doctrine, which holds that abandoning property forfeits any Fourth Amendment protections.[194] If so, the drafters of the 180-day rule may have treated unopened files that had not been accessed for over 180 days as abandoned.[195] An "abandoned" message is then subject to the SCA's limited protections for non-content information, the disclosure of which, under § 2703(c), the government may compel with a court order.[196]

Accepting the DOJ's distinction between opened and unopened email avoids the added protections of § 2703(a), as any opened email is not in "electronic storage" and thus cannot be considered maintained by an ECS provider.[197] Under the DOJ interpretation, once the recipient retrieves the message, the ISP is treated as providing RCS as to that communication, and the government can compel the ISP to disclose the contents of that communication under the more lenient tripartite standard.[198] The DOJ effectively transforms the email, once accessed, to a communication maintained by an RCS provider pursuant to § 2703(b).[199] For unopened emails, those stored for 180 days or fewer are subject to the warrant requirement, while unopened emails stored by the ECS provider in "electronic storage" for more than 180 days may be disclosed pursuant to the tripartite standard.[200] Thus, the same communication is subject to the heightened protections of the probable cause standard when the communication has not yet been opened by the recipient, but obtainable by the government under the tripartite standard once the recipient accesses the message.

The DOJ's approach appears inconsistent with the fact that Congress designed the 180-day rule partly on the assumption that people saved their emails for a few months.[201] In light of this finding, a user's decision to keep an opened message for a few months does not always suggest an intent to abandon the message, but could equally

---

193. H. R. REP. NO. 99-647, at 68 (1986).

194. Kerr, *supra* note 10, at 1234.

195. *Id.* (citing United States v. Jones, 707 F.2d 1169, 1172 (10th Cir. 1983) ("When individuals voluntarily abandon property, they forfeit any expectation of privacy in it that they might have had.")).

196. 18 U.S.C. § 2703(c)(1)(B).

197. *See* DOJ SEARCH MANUAL, *supra* note 131, at 138.

198. *Id.*

199. *See id.*

200. *Id.*

201. *See* H. R. REP. NO. 99-647, at 68 (1986).

reflect the user's intention to save the email for later reference.[202] Further, "opened" and "unopened" do not appear in § 2703 and the DOJ effectively reads in these limitations, although foreign to the statutory language.[203]

In contrast, the Ninth Circuit does not distinguish between opened and unopened emails, but instead tracks the language of § 2703.[204] Specifically, for communications stored by an ECS provider for 180 days or fewer, no governmental entity may compel disclosure unless it obtains a warrant.[205] Communications stored by an ECS provider for 181 days or more may be disclosed if the tripartite standard is met.[206] Whether the recipient accessed the message is irrelevant.[207]

Although the Ninth Circuit's approach appears closest to the apparent policy in the legislative history and to the statutory language, the 180-day rule is itself subject to criticism.[208] At the September 2010 hearings before the House of Representatives, Michael Hintze, Associate General Counsel at Microsoft, argued that the technological assumptions behind the 180-day rule are outdated:[209]

> A decade after the enactment of [the] ECPA, in 1996, Microsoft was offering the first version of Microsoft Exchange—server and desktop software in which a user typically would download email to a local machine for it to be read and stored, after which it would no longer reside on the server. Because email typically was downloaded to a local drive to be read and stored, it was reasonable to conclude that email left with a service provider for more than 180 days was abandoned with little expectation of privacy.[210]

But with the advent of cloud computing and the increase in online storage capacity, users today store their emails and files online for years, while expecting that their data will receive the same privacy protections on day 181 as on day 179.[211] Richard Salgado, Senior

---

202. *See id.*

203. *See* 18 U.S.C. § 2703.

204. *See id.* (citing Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004)).

205. 18 U.S.C. § 2703(a) (2006).

206. *Id.*

207. *Theofel*, 359 F.3d at 1077.

208. *See infra* text accompanying notes 209–213.

209. *See September 23 Hearing*, *supra* note 12, at 32 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation) (noting that the "basic technological assumptions upon which the Act was based and the nature of protection given to user data stored in the cloud have not kept pace with the unprecedented digitization and storage of online data that cloud computing has enabled"); *see also id.* at 124 (statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP) (deeming the 180-day rule "arbitrary and based on a false assumption").

210. *Id.* at 33 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation).

211. *Id.*

Counsel of Law Enforcement and Information Security for Google, Inc., apparently agrees with Hintze, as he could think of no reason to reduce the privacy protections afforded messages that have been opened or stored for 181 days.[212]

Moreover, it is ironic that statutory protection applies primarily to the messages that need it the least, because while "the emails or private messages that are both the most important and the most private are the older messages that you have read through several times and have intentionally decided to save . . . . By contrast, the unopened emails in your inbox are likely to be commercial solicitations that you have not yet had time to delete. [213] Yet courts have found that the SCA requires the government to obtain a warrant to access those unopened emails, while the protection afforded to saved emails remains unclear.[214]

Gmail illustrates the implications of the 180-day versus 181-day distinction. Under the DOJ's approach to opened emails, the effect of the 180-day rule would be limited to unopened messages, [215] because the DOJ restricts "communications in electronic storage"—and thus, the warrant protection for communications maintained by an ECS—to messages stored but not yet accessed by the recipient.[216] By treating the Gmail messages as stored by an RCS, the DOJ approach denies the email warrant protection, which allows the government to compel Gmail to disclose the communication if it satisfies tripartite standard.[217]

In the Ninth Circuit, though, it remains unclear whether the SCA covers communications stored in the cloud.[218] Applying only the holding from *Theofel*, and assuming Gmail provides ECS, the government needs a warrant to compel disclosure of the communication only if stored for 180 days or less, while a court order

212. *Id.* at 21 (statement of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, Inc.) ("It's difficult to imagine a justification for a rule that lowers the procedural protection for a message merely because it is six months old or has been viewed by the user.").

213. *September 23 Hearing*, *supra* note 12, at 123 (statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP).

214. *Id.*

215. *See* DOJ SEARCH MANUAL, *supra* note 131, at 138.

216. DOJ SEARCH MANUAL, *supra* note 131, at 124.

217. *Id. See* 18 U.S.C. § 2703(a)–(b) (stating that the 180–181 day distinction only applies to communications stored by an ECS in "electronic storage").

218. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2003) (stating that communications maintained after transmission are in "electronic storage" by an ECS provider); United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (refusing to apply *Theofel* to webmail).

or subpoena would suffice if stored for at least 181 days.[219] If Gmail provides RCS instead, then the 180-day rule is inapplicable.[220] If, however, the limitation from *Weaver* applies, the 180-day rule may not enter the analysis for communications stored in the cloud.[221] Therefore, the level of privacy protection depends on the service characterization, storage duration, and jurisdiction.

D. Critiquing the Complex Framework

This analysis demonstrates the complexity of the SCA's current framework. When Congress enacted the SCA, it believed that the bill struck a "fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[222] However, as applied to cloud computing technology, the various approaches adopted by the DOJ and the Ninth Circuit strike *different* balances between individual privacy and law enforcement needs.[223] The DOJ approach, by distinguishing between opened and unopened emails, tips the scale in favor of law enforcement, for whom the DOJ views the SCA as a "vital tool."[224] The interpretation of DOJ favors law enforcement by conceptualizing the SCA not as protecting individual privacy, but as regulating how the government can obtain access to stored communications.[225]

In contrast, the Ninth Circuit's approach remains ambiguous as to whether communications stored in the cloud are in "electronic storage."[226] However, the Ninth Circuit has held that emails stored on the servers of email systems after transmission are stored for backup purposes, thereby preserving a sphere of individual privacy.[227]

---

219. *See Theofel*, 359 F.3d at 1075 (reasoning that messages remaining on an ISP's server after delivery are stored for purposes of backup protection and thus are in "electronic storage" subject to the 180-day rule in § 2703(a)).

220. *See* 18 U.S.C. § 2703(b).

221. *See Weaver*, 636 F. Supp. 2d at 772 (stating that *Theofel* only applies to non-webmail systems).

222. H. R. REP. NO. 99-647, at 19 (1986); S. REP. NO. 99-541, pt. 3, at 5 (1986).

223. *See infra* notes 224–228.

224. *The Electronic Communications Privacy Act: Promoting Security and Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 2 (2010) [hereinafter *September 22 Hearing*] (statement of James A. Baker, Associate Deputy Att'y Gen., United States Department of Justice).

225. *See* DOJ SEARCH MANUAL, *supra* note 131, at 115.

226. *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2003) (holding was not limited to traditional email systems), *with* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010) (holding that cloud-based social networking websites provided RCS when they stored private messages previously opened by the recipients), *and Weaver*, 636 F. Supp. 2d at 772 (refusing to apply *Theofel* to webmail).

227. *Theofel*, 359 F.3d at 1075–77.

Because it treats such communications as stored by an ECS provider, the Ninth Circuit's approach provides greater privacy than that of the DOJ, at least for communications stored for 180 days or fewer.[228] Yet, given the uncertainty regarding the applicability of *Theofel* to communications stored in the cloud, it remains unclear whether the 180-day rule applies to already opened email stored in the cloud.[229] Thus, both the DOJ and the Ninth Circuit balance individual privacy interests with government investigative needs, but reach different results based on their different outlooks.[230]

III. PIERCING THE ACT'S CLOUDINESS

A. Current Debate

The preceding discussion demonstrates that the SCA fails to provide a clear framework for understanding whether a user has a reasonable expectation of privacy in his communications stored in the cloud.[231] Because Congress enacted the SCA as part of ECPA in the late 1980s and has not amended it to address cloud computing,[232] the ECPA—specifically, the SCA—needs to be revisited. Digital Due Process (DDP), a coalition of privacy advocates, think tanks, and major corporations, also seeks to amend the SCA.[233] DDP is lobbying Congress to better balance the privacy interests of citizens with the legitimate needs of law enforcement agencies:[234]

> ECPA is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies. ECPA can no longer be applied in a clear and consistent way, and, consequently, the vast amount of personal information generated by today's digital communication services may no longer be adequately protected.[235]

Among its proposals for modernizing the ECPA, DDP recommends that the government only compel a covered service provider to disclose communications with a warrant, "regardless of the age of the

228. *Compare id.* (reasoning that emails remaining on an ISP's server after transmission are in "electronic storage"), *with* DOJ SEARCH MANUAL, *supra* note 131, at 123–24 (stating that any opened email is not in "electronic storage").

229. *See supra* text accompanying notes 136 –144.

230. *See supra* text accompanying notes 224–228.

231. *See, e.g.*, *supra* text accompanying notes 155–158 (discussing the various conflicting approaches and the remaining uncertainty in the Ninth Circuit).

232. *About the Issue*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org (last visited Feb. 4, 2011).

233. *Who We Are*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org (follow "Who We Are" hyperlink at top of page) (last visited Feb. 1, 2011) (noting that DDP members include, Amazon.com, ACLU, AT&T, Facebook, Intel, and Microsoft).

234. *See About the Issue*, *supra* note 232.

235. *Id.*

communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations."[236]

DDP's lobbying efforts have made progress toward amending the SCA.[237] Answering DDP's calls to amend the SCA, on May 5, 2010, the House Subcommittee on the Constitution, Civil Rights, and Civil Liberties, held a hearing on the ECPA.[238] In his opening statement before the Subcommittee, Chairman Jerrold Nadler asserted that the hearing would be the first of many to determine whether and how to amend the Act.[239] Nadler framed the issue as whether the SCA still strikes the appropriate balance between the interests of law enforcement and individual privacy,[240] given the "enormous technological advances" in electronic communications since Congress passed the Act.[241]

All four witnesses testifying before the Subcommittee referenced and supported DDP's elementary principles for reform.[242] James X. Dempsey, Vice President for Public Policy at the Center for Democracy and Technology, argued that the SCA should afford the same protections and standards for government access to data, whether stored locally or in the cloud.[243] Further, Dempsey argued that the probable cause standard should protect the content of communications, regardless of the duration of storage or whether the

---

236. *Our Principles*, DIGITAL DUE PROCESS, http://digitaldueprocess.org (Follow "Our Principles" hyperlink at top of page) (last visited Feb. 4, 2011).

237. *See Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 2 (2010) [hereinafter *May 5 Hearing*] (statement of Mr. F. James Sensenbrenner, Jr., Ranking Member, Subcomm. on the Constitution, Civil Rights, and Civil Liberties) (documenting hearings held in response to calls by the DDP to amend the SCA).

238. *Id.*

239. *Id.* at 1 (statement of Mr. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, & Civil Liberties). Ranking Member of the Subcommittee, Mr. F. James Sensenbrenner, Jr., agreed that this hearing was only the first step. *Id.* at 3 (statement of Mr. F. James Sensenbrenner, Jr., Ranking Member, Subcomm. on the Constitution, Civil Rights, and Civil Liberties) ("There has neither been sufficient time to examine the concepts that are being advanced in any meaningful way, nor has there been time to hear from other stakeholders, including relevant members of the law enforcement community.").

240. *Id.* at 2 (statement of Mr. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, and Civil Liberties).

241. *Id.* at 1 (statement of Mr. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, & Civil Liberties).

242. *See, e.g.*, *May 5 Hearing*, *supra* note 237, at 52 (statement of Annmarie Levins, Associate General Counsel, Microsoft Corporation) (supporting Digital Due Process's efforts at reform).

243. *Id.* at 11 (statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

communication was opened.[244] And Orin S. Kerr echoes Dempsey's recommendation for a warrant requirement, whatever the time stored or service provided.[245]

House and Senate committees held a second round of hearings in September 2010.[246] Unlike the first round in May 2010, the September hearings generated far more debate between proponents seeking privacy protections for citizens and advocates favoring flexibility for law enforcement.[247] Witnesses testifying for greater privacy protections all supported at least the basic DDP principles,[248] but viewed them only as a springboard for future discussions.[249] One such witness criticized the DOJ's distinction between opened and unopened emails, as well as the "arbitrary" 180-day rule, as nonsensical.[250]

On the law enforcement side of the debate, witnesses worried that criminals are now taking advantage of new technologies to create a "cloak of invisibility" from traditional law enforcement detection.[251] Consistent with this concern, James A. Baker, Associate Deputy

244. *Id.* at 14; *see also id.* at 56 (statement of Annmarie Levins, Associate General Counsel, Microsoft Corporation) (noting that "information in the cloud should be protected in the same way that their . . . [h]ard drive would").

245. *Id.* at 37 (statement of Orin S. Kerr, Profesoor, George Washington University Law School). Kerr argued that the warrant requirement could be subject to limited exceptions, including permitting the government to compel disclosure pursuant to a subpoena for corporate crimes and in cases of misconduct by government employees. *Id.* at 38. *See also id.* at 28 (statement of Albert Gidari, Partner, Perkins Coie LLP) (recommending a warrant for all content stored in the cloud).

246. *See September 23 Hearings*, *supra* note 12; *September 22 Hearings*, *supra* note 224.

247. *Compare September 22 Hearings*, *supra* note 224, at 2 (statement of James A. Baker, Associate Deputy Att'y Gen., United States Department of Justice) (arguing that the SCA is a "vital tool" for law enforcement, and that Congress should be cautious in changing the SCA), *with September 23 Hearings*, *supra* note 12, at 38 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation) ("[W]e support the responsible reform of ECPA to ensure that users have the same privacy rights for their data in the cloud as they do for their on-premises data.").

248. *See generally September 23 Hearings*, *supra* note 12, at 3 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation) (supporting DDP principles for reform); *id.* at 22 (statement of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, Inc.) (supporting DDP principles for reform); *id.* at 5 (statement of Paul Misener, Vice President for Global Public Policy, Amazon.com) (agreeing with DDP principles that a warrant should be required to compel a cloud service provider to disclose content of communications stored on its server).

249. *Id.* at 36 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation).

250. *Id.* at 124–25 (statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP).

251. *Id.* at 2 (statement of Kurt F. Schmid, Exec. Dir., Chi. High Intensity Drug Trafficking Area); *see also id.* at 107 (statement of Thomas B. Hurbanek, Senior Investigator, New York State Police Computer Crime Unit) (arguing that certain cloud computing technologies "could create an environment where entire segments of business activity could be conducted outside of the reach of law enforcement").

Attorney General, reframed the issue from ensuring the privacy of citizens to protecting the public from crime:[252]

> [W]e urge Congress to proceed with caution; and to avoid amendments that would disrupt the fundamental balance between privacy protection and public safety. Congress should refrain from making changes that would impair the government's ability to obtain critical information necessary to build criminal, national security, and cyber investigations, particularly if those changes would not provide any appreciable or meaningful improvement in privacy protection.[253]

Two other witnesses supporting the law enforcement perspective echoed Baker's assertion, recommending that Congress tread carefully in reforming the SCA, lest it lose the current balance between privacy and law enforcement.[254]

B. Need for Reform

The SCA has not kept up with the growth of technology since its enactment in 1986.[255] Edward W. Felten, a Professor of Computer Science and Public Affairs at Princeton University, observed that much has changed in twenty-five years:

> In 1986, when ECPA was passed, the Internet consisted of a few thousand computers . . . . There were no web pages, because the web had not been invented. Google would not be founded for another decade. Twitter would not be founded for another two decades. Mark Zuckerberg, who would grow up to start Facebook, was two years old.[256]

Advances in technology spurred important developments in the role the Internet plays in people's everyday lives.[257] While email

---

252. *September 22 Hearings*, *supra* note 224, at 5–7 (statement of James A. Baker, Associate Deputy Att'y Gen., United States Department of Justice).

253. *Id.* at 5–6.

254. *September 23 Hearings*, *supra* note 12, at 105 (statement of Thomas B. Hurbanek, Senior Investigator, New York State Police Computer Crime Unit) (arguing that "any reforms must be carefully weighed to preserve the existing balance between individual privacy and the ability of law enforcement to conduct investigations and protect the public"); *id.* at 6 (statement of Kurt F. Schmid, Executive Director, Chicago High Intensity Drug Trafficking Area) ("Any reform of the ECPA should address new and emerging technologies without unduly hampering or constraining law enforcement in its mission to protect the public.").

255. *See id.* at 7 (statement of Fred H. Cate, C. Ben Dutton Professor of Law and Director of the Center for Applied Cybersecurity Research, Indiana University) (explaining that "dramatic changes in technologies and online services," like cloud computing, have left the SCA "inadequate to protect privacy today").

256. *Id.* at 12 (statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University); *see also* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 972 n.15 (C.D. Cal. 2010) (citing William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act,* 98 GEO. L.J. 1195, 1198 (2010)) (noting that the World Wide Web was not introduced until 1990, and the web browser was not introduced until 1994).

257. *September 23 Hearings*, *supra* note 12, at 12 (statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University).

increasingly replaces first-class mail, there is no reason to believe that such a replacement affects individual privacy expectations.[258]

At best, changes in technology have left cloud-based communications with uncertain protection; at worst—and more likely—they lie outside the protections of the SCA altogether.[259] Cloud-based email, such as Gmail,, does not fit comfortably within either the ECS or RCS characterization, casting doubt on whether the government must obtain a warrant access such communications.[260]

Further, new technology not captured by the SCA has created a "murky legal landscape" that fails to address the interests of customers, service providers, and the government.[261] The lack of guidance inhibits the efficiency of law enforcement, as officials must decide whether to "take the chance of stepping over the line—risking suppression of evidence or even personal sanctions—or shy away from the line to avoid overstepping."[262] A consistent standard would benefit law enforcement by providing a predictable framework that would allow the government to act affirmatively to compel disclosure of electronic communications, without the risk that evidence will be deemed inadmissible.

Service providers would also benefit from a predictable standard. The complexity of the SCA offers insufficient clarity for service providers to structure their conduct appropriately, and in fact, the law is so unclear that service providers "essentially guess" at what the Act requires.[263] A service provider must correctly characterize a particular service as either ECS or RCS, for if it mischaracterizes the service and discloses communications under a less burdensome standard, civil liability could result.[264]

Furthermore, the SCA's obscurity and inconsistent requirements reduces the incentives for businesses and consumers to develop and employ potentially more efficient cloud-based services.[265] Failing to ensure the privacy of communications stored in the cloud deters users from storing their data there. In any event, users likely do not know that they have greater privacy when they store their

258. *Id.* at 5 (statement of Perry Robinson, Associate General Counsel, Rackspace Hosting).

259. *See supra* text accompanying notes 168–190.

260. *See supra* text accompanying notes 168–190.

261. *September 22 Hearings*, *supra* note 224, at 6 (statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

262. *May 5 Hearings*, *supra* note 237, at 75 (statement of J. Beckwith Burr, Partner, Wilmer Cutler Pickering Hale & Dorr, LLP).

263. *Id.* at 22 (statement of Albert Gidari, Partner, Perkins Coie LLP).

264. *Id.* at 27.

265. *September 23 Hearings*, *supra* note 12, at 21–22 (statement of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google, Inc.).

communications locally than in the cloud."[266] Similarly, businesses may decline to develop and invest in new technology without clear guidelines regarding privacy.[267]

C. Constitutionality

The questionable constitutionality of the SCA provides another reason for Congress to reform the Act.[268] Some commentators argue that allowing the government to compel disclosure of email communications without a warrant violates the Supreme Court's "closed container" jurisprudence.[269] The "closed container" doctrine holds that the government must obtain a warrant to search a package "closed against inspection," regardless of its location.[270] An email stored on an ISP's server may constitute a "closed container," as email accounts are typically password-protected, and the ISP has limited access to the contents of the communication.[271] Users thereby possess objectively reasonable expectations of privacy in their emails,[272] and as with first-class mail, emails stored in the cloud should fall within the scope of the Fourth Amendment.[273] Other commentators argue that the SCA's denial of warrant protection for emails stored longer than 180 days by an ECS is unconstitutional, as users reasonably expect the same level of privacy in their communications on day 181 as on day 180.[274]

Courts have approached the constitutionality of the SCA cautiously.[275] In 2006, the Southern District of Ohio, in *Warshak v. United States*, held facially unconstitutional the combination of § 2703(b)(1)(B)(ii) and § 2703(d), which together permit the government to compel disclosure with merely a court order—and without notice.[276] In 2007, the Sixth Circuit affirmed, concluding that users reasonably

---

266. *Id.* at 34 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation).

267. *Id.* at 28.

268. *See infra* text accompanying notes 269–288.

269. Goldstein & Weinberg, *supra* note 138, at 19.

270. *Id.* at 18 (citing *Ex Parte* Jackson, 96 U.S. 727, 73 (1878)).

271. *Id.* at 19, 21.

272. *Id.* at 21.

273. *Id.* at 24.

274. Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1068 (2008); Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 397 (2009).

275. *See infra* text accompanying note 279 (recommending as-applied challenges rather than facial challenges to the constitutionality of the SCA).

276. No. 1:06-cv-357, 2006 U.S. Dist. LEXIS 50076, at *32 (S.D. Ohio July 21, 2006), *aff'd in part*, 490 F.3d 455 (6th Cir. 2007), *vacated on other grounds*, 532 F.3d 521 (6th Cir. 2008).

expect privacy in email transmitted through, or stored on, the server of an ISP.[277] However, after granting a rehearing *en banc* in 2008, the court vacated the decision, holding that the constitutional claim was not ripe.[278] In that opinion, the Sixth Circuit hinted that plaintiffs challenging the constitutionality of the SCA should refrain from facial attacks.[279] When Warshak raised a similar claim in December 2010, the Sixth Circuit found the claim ripe for review[280] and held that a customer has a reasonable expectation of privacy in the contents of his emails stored or transmitted through an ISP, and that the government violates his Fourth Amendment rights when it compels an ISP to disclose his emails without a warrant.[281] Of course, the court found that the authorization of this practice in the SCA did not render it constitutional.[282]

Like *Warshak*, in *United States v. Hart*, the Western District of Kentucky refused to decide whether compelled disclosure by administrative subpoena was unconstitutional on its face.[283] Yet, in contrast to *Warshak*, *Hart* subsequently rejected an email user's as-applied challenge,[284] finding that the provider's service agreement—allowing access of communications to comply with legal process, provide services to the customer, and for other reasons—precluded an inference that the user had a legitimate expectation of privacy in the content of his emails.[285]

As in *Hart*, some commentators assert that the SCA is constitutional.[286] Congress presumably thought so when it passed the Act, which represents Congress's value judgment about the extent to which individual privacy should be protected online.[287] Asking whether a reasonable expectation of privacy exists in the place searched "is essentially a legal fiction that masks a normative inquiry into whether a particular law enforcement technique should be regulated by the Fourth Amendment."[288]

---

277. Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007).

278. Warshak v. United States, 532 F.3d 521, 534 (6th Cir. 2008).

279. *Id.* at 529.

280. United States v. Warshak, No. 10-1294, 2010 U.S. App. LEXIS 25415, at *24 n.12 (6th Cir. Dec. 14, 2010).

281. *Id.* at *43.

282. *Id.*

283. United States v. Hart, No. 3:08-CR-00109-C, 2009 U.S. Dist. LEXIS 72597, at *66 (W.D. Ky. July 28, 2009).

284. *Id.*

285. *Id.* at *68–70.

286. *See* Robison, *supra* note 189, at 1233–34.

287. *Id.*

288. *Id.* at 1233.

Although the SCA may rightfully survive a facial challenge, there is no principled basis for according greater privacy protections for traditional email, as well as traditional mail, than for cloud-based email. Certainly, the Fourth Amendment protects communications sent through first-class mail.[289] Moreover, the same communication, sent via a non-webmail email system, is protected under the SCA, although the protection currently varies depending on the jurisdiction.[290] However, the same message, if sent through a cloud-based email service, may lack protection under the ECS provisions, in light of *Weaver* (and the interpretation of the DOJ), as well as the RCS provisions, if not maintained solely to provide computer storage or processing services.[291] This framework, which provides different standards of privacy protections for the same communication, surely contradicts users' reasonable expectations of their rights. Logically, if a communication deserves the protection of a warrant when sent through the mail, the same communication—even if opened and stored by the user for 181 days—deserves the protection of a warrant when sent through cloud-based servers.

Given that Congress conceived of the SCA as preserving the "vitality" of the Fourth Amendment,[292] the current debate over its constitutionality may imply that the Act no longer comports with the Fourth Amendment. At the very least, it suggests that the SCA may not serve the same functions Congress originally intended,[293] as the warrant requirement offers greater protection than what falls through the cracks of the SCA.

The SCA reflects Congress's attempt to "strike[] the right balance between the interests and needs of law enforcement and the privacy interests of the American people."[294] As the previous discussion demonstrates, the SCA fails to serve the interests of law enforcement, service providers, and customers. In short, the emergence of cloud computing demonstrates that the SCA no longer "strikes the right balance."[295]

---

289. *Ex Parte Jackson*, 96 U.S. 727, 733 (1878).

290. *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003) (explaining that emails stored after transmission are maintained by an ECS provider in "electronic storage" for backup purposes, regardless of whether the email has been opened), *with* DOJ SEARCH MANUAL, *supra* note 131, at 123–24 (stating that opened email is not in "electronic storage").

291. *See supra* text accompanying notes 168–190 (discussing the Gmail example).

292. H. R. REP. NO. 99-647, at 19 (1986).

293. *See* S. REP.. NO. 99-541, at 5 (1986) ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.").

294. *May 5 Hearings*, *supra* note 237, at 2 (statement of Mr. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, and Civil Liberties).

295. *See supra* text accompanying notes 255.

D. Congress Should Require a Warrant to Compel Disclosure of Communications Stored in the Cloud

Even in the absence of constitutional infirmity, the factual basis for the distinctions in the SCA have eroded to such an extent that Congress should amend the SCA.[296] The uneven application of the SCA, as previously discussed, has led to considerable uncertainty and neither reflects the realistic expectations of users of cloud services,[297] nor the primacy email has achieved in digital-age communications.[298]

Congress should amend the SCA to provide clear guidance to courts, law enforcement, businesses, and individual users. Given that courts remain wary of deciding such technology questions, judicial clarification is unlikely.[299] Indeed, the Supreme Court has warned courts to treat lightly where nascent technologies impinge on privacy, because, "[t]he judiciary risks error by elaborating too fully on the *Fourth Amendment* implications of emerging technology before its role in society has become clear."[300] Given the courts' recent struggles with declaring provisions of the law unconstitutional, as in *Warshak*, as well as the continuing debate over the SCA's constitutionality, there may be little prospect for judicial resolution.[301]

Congress must, therefore, reform the SCA to ensure that failing to address new technology does not undermine the balance between individual privacy and the legitimate needs of law

---

296. *See* Gellman, *supra* note 19, at 12 (stating that the SCA "is a difficult law to understand and apply, in part because the law is old and relies on a model of electronic mail and Internet activity that is generations behind current practice and technology"); *see also September 23 Hearings*, *supra* note 12, at 32 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation) ("[T]he basic technological assumptions upon which the [SCA] was based . . . ha[s] not kept pace with the unprecedented digitization and storage of online data that cloud computing has enabled.").

297. *September 23 Hearings*, *supra* note 12, at 28 (statement of Michael Hintze, Associate General Counsel, Microsoft Corporation) (explaining that the SCA does not accord with the realities of technology today, as the SCA has created uncertainty surrounding the privacy protections for data stored in the cloud).

298. *See, e.g.*, *September 23 Hearings*, *supra* note 12, at 12 (statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University) ("[E]ven more important than changes in the [technology] have been the changes in how people use the Internet and the role it plays in their everyday lives."); *see also* Gellman, *supra* note 19, at 7 (arguing that "[t]he law badly trails technology").

299. *See, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 846 (11th Cir. 2010). *Rehberg* noted that whether an individual user has a reasonable privacy expectation in the contents of his emails transmitted through a third-party ISP presents "complex, difficult, and 'far-reaching' legal issues that we should be cautious about resolving too broadly." *Id.*

300. City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

301. *See* Robison, *supra* note 189, at 1233–34 (arguing that the courts cannot declare SCA unconstitutional).

enforcement.[302] While previous commentators have suggested that Congress eliminate the 180-day rule for providers of ECS,[303] Congress should first consider whether the distinction between ECS and RCS even makes sense. As discussed previously, the distinction between the two types of services is no longer practical, and cloud provider may be characterized as providing either ECS or RCS.[304]

In amending the SCA, Congress should adopt the following three reforms. First, Congress should eliminate the distinction between ECS and RCS and subject the content of all communications stored electronically to the warrant requirement. Exceptions may be made, however, for communications the government can show were "abandoned" by the user, or where the user cannot establish that he had an objectively reasonable expectation of privacy in the communication. Second, Congress should clarify that both opened and unopened emails as well as other electronic communications are protected against compelled government disclosure without a warrant. Finally, Congress should discard the 180-day rule and subject all communications stored electronically to the warrant requirement, regardless of how long they remain in the cloud. Congress should consider the following statutory language:

> A governmental entity may only require a provider of communications services to disclose the contents of a wire or electronic communication, if transmitted or stored electronically, only upon the issuance of a warrant by a court of competent jurisdiction, whether or not the provider stores the communication after receipt by the user, and regardless of whether the communication remains on the server after receipt or is downloaded to the user's device.

In implementing these reforms, Congress should respect the principle of technology neutrality, which would ensure each electronic communication receives the same protection, regardless of the particular technology creating, transmitting, or storing that communication.[305] Furthermore, Congress must continue to monitor new technologies, which may undermine the legislative purpose of the SCA. Congress should ensure that the law is responsive to new technologies by committing to periodically reassess the continued vitality of the Act.

This approach has the advantages of providing law enforcement, users, and service providers with a consistent standard for compelled disclosure of electronic communications. The warrant

---

302. *See* S. REP. NO. 99-541, pt. 3, at 5 (1986).

303. Oza, *supra* note 274, at 1070.

304. *See supra* text accompanying notes 168–190. The Gmail example demonstrates the complexity of the various approaches. *See supra* text accompanying notes 168–190.

305. *September 23 Hearings*, *supra* note 12, at 52 (statement of David Schellhase, Executive Vice President and General Counsel, Salesforce.com).

requirement will better comport with the reasonable expectations of users and bring privacy in the cloud more in line with the privacy afforded traditional mail under *Ex Parte Jackson*.[306] Amending the SCA will also preserve the incentives for businesses and users to shift to more innovative and efficient computing models, without fear of losing privacy protections in the process. Congress should act swiftly to update the existing law, which will only become more antiquated as technology advances.

IV. CONCLUSION

The Stored Communications Act (SCA) must be updated in order to accommodate the tremendous technological advances of the last twenty-five years.[307] Congress enacted the SCA to ensure that the method of communication did not compromise the privacy of the message.[308] While Congress—in 1986—touted the SCA as affording privacy protections to new technologies that were not addressed by then-existing law,[309] it has yet to reconsider the Act's structural framework.[310]

Unfortunately, the law has not proven flexible enough to protect communications enabled by new technologies, and it remains unclear whether the SCA even extends to communications stored in the cloud.[311] The distinction between an ECS and an RCS no longer makes sense, yet the characterization of a particular service has significant implications for the user's privacy in the communication.[312] Likewise, the 180-day rule no longer conforms to the practical realities of email storage or the expectations of email users.[313] Congress

306. *See* 96 U.S. 727, 733 (1878).

307. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 972 n.15 (C.D. Cal. 2010) (citing William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act,* 98 GEO. L.J. 1195, 1198 (2010)) (noting that the World Wide Web was introduced in 1990 and web browser introduced in 1994).

308. S. REP. NO. 99-541, pt. 3, at 5 (1986) ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.").

309. S. REP. NO. 99-541, pt. 1, at 1 (1986).

310. *About the Issue*, *supra* note 232.

311. *See also supra* text accompanying notes 168–190 (demonstrating that the Gmail example shows cloud-based email may be outside the scope of the SCA). *See generally* Gellman, *supra* note 19, at 12–13 (discussing the uncertainty as to the applicability of the SCA to cloud computing).

312. *See, e.g.*, 18 U.S.C. § 2703(a) (2006) (requiring warrant to compel ECS providers to disclose communications in "electronic storage" for 180 days or less and describing the tripartite standard that applies to compel RCS providers).

313. *May 5 Hearings*, *supra* note 237, at 74 (statement of J. Beckwith Burr, Partner, Wilmer Cutler Pickering Hale & Dorr, LLP); *see supra* notes 209–213 (describing how the 180-

should, therefore, amend the SCA to ensure that all communications stored in the cloud are subject to the warrant requirement.

Ilana R. Kattan[*]

day rule reflected the short duration of storage in 1986, while users today typically save their most important emails for longer periods of time).

[*] J.D. Candidate, Vanderbilt University Law School, 2012; B.A., Sociology, Vanderbilt University, 2009. The author wishes to thank her parents for their support during her academic career. In addition, the author wishes to thank the editorial staff of the VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW, especially Nathan McGregor, Kevin Lumpkin, and Emily Beverage, for wonderful editing and thoughtful suggestions during the preparation of this Note. Finally, the author wishes to thank Daniel Gervais, Professor of Law, Co-Director, Technology & Entertainment Law Program at Vanderbilt University Law School for his input on this Note.