American University Law Review

Volume 63 | Issue 1 Article 7

2013

The Stored Communications Act: An Old Statute for Modern Times.

Melissa Medina
American University Washington College of Law

The Stored Communications Act: An Old Statute for Modern Times.

Keywords
South Carolina. Supreme Court, Communication -- Law & legislation, Technology & law, E-mail -- Law & legislation, Actions & defenses (Law) -- Cases, Judge-made law, Legislative reform, Statutes -- United States -- States

NOTE

THE STORED COMMUNICATIONS ACT: AN OLD STATUTE FOR MODERN TIMES

MELISSA MEDINA*

TABLE OF CONTENTS

* Senior Staff Member, *American University Law Review*, Volume 62; J.D., May 2013, *American University Washington College of Law*; B.A., Political Science, May 2006, *University of Florida*. I would like to thank Professor Allen Feldman for his guidance and support and the *AULR* staff for their superb editing and helpful suggestions. Finally, a special thank you to my family and friends for their never-ending support, encouragement, and patience.

INTRODUCTION

Google recently asserted that email "users have no 'reasonable expectation' of privacy."[1] Headlines like this fueled outrage when the advocacy group Consumer Watchdog posted Google's motion to dismiss a class action lawsuit online.[2] This statement has been called "a stunning admission,"[3] but how surprising is it? In reality, Google's statement reflects well-established law, which only fairly recently started to receive judicial criticism.[4] Law enforcement agencies can often gain access to email information with little more than a subpoena.[5] This ease of access may surprise many Americans who use email as their primary means of communication. The rapid and exponential growth of the Internet and technology over the past decade has made it easy to communicate with others around the world. However, these advantages have revealed a host of privacy issues.

In the 1980s, manufacturers such as IBM and Apple began marketing more affordable computer systems, which allowed greater

---

1. Dominic Rushe, *Google: Don't Expect Privacy When Sending to Gmail*, GUARDIAN (Aug. 14, 2013), http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit (reporting that Google stated, in a motion to dismiss, that "all users of email" do not have a reasonable expectation of privacy in their email communications).

2. *See* Memorandum of Points and Authorities in Support of Defendant's Motion to Dismiss at 19, 25–26, *In re* Google Inc. Gmail Litig., No. 5:13-md-02430-LHK (N.D. Cal. June 13, 2013), 2013 WL 3297861, *available at* http://www.consumerwatchdog.org/resources/googlemotion061313.pdf; John M. Simpson, *Google Tells Court You Cannot Expect Privacy When Sending Messages to Gmail—People Who Care About Privacy Should Not Use Service, Consumer Watchdog Says*, CONSUMER WATCHDOG (Aug. 12, 2013), http://www.consumerwatchdog.org/newsrelease/google-tells-court-you-cannot-expect-privacy-when-sending-messages-gmail-people-who-care; *see also* Rushe, *supra* note 1.

3. Simpson, *supra* note 2 (emphasis added) ("Google has finally admitted they don't respect privacy.").

4. *See, e.g.*, United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (stating that Fourth Amendment protection is "not absolute, and may be extinguished when a computer user transmits information over the Internet or by e-mail"); United States v. Valdivieso Rodriguez, 532 F. Supp. 2d 332, 339 (D.P.R. 2007) (noting that most courts that have addressed Fourth Amendment concerns in the email context have held that users do not have a reasonable expectation of privacy in email communications). The first federal circuit court to challenge this premise was the Sixth Circuit in 2007. *See* Warshak v. United States, 490 F.3d 455, 467 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

5. *See Warshak*, 490 F.3d at 462 (indicating that federal authorities can access emails sent more than six months prior with only a subpoena); *see also* Rehberg v. Paulk, 611 F.3d 828, 843 (11th Cir. 2010) (surveying several circuits that have held that a person lacks a legitimate privacy expectation in Internet subscriber information and to and from addresses in emails sent with ISPs).

access to computer technology.[6] This increased access spurred the creation of novel and now widely used methods of communication. Concerns that the law did not adequately protect the privacy of those communications prompted Congress to enact the Stored Communications Act[7] (SCA or "the Act") as part of the broader Electronic Communications Privacy Act of 1986[8] (EPCA). The SCA protects communications in three important ways: (1) it provides a private cause of action against anyone who intentionally "obtains, alters, or prevents authorized access" to certain stored communications; (2) it regulates when network service providers may voluntarily disclose customer communications and records; and (3) it outlines specific rules that govern when state actors may compel disclosure of stored communications from network service providers.[9]

The statute was remarkably forward-looking in that it was passed before Congress could fully grasp the complications of emerging technology.[10] At the time of the statute's passage, email systems required users to subscribe to the same email service provider as the sender to receive messages electronically.[11] Moreover, even though access to technology was increasing, it was still prohibitively expensive for individuals and generally only available to businesses, academics, and educational institutions.[12] Surprisingly, the SCA has served its purpose of protecting electronic communications well beyond the limited technology that existed at the time of its passage.[13]

---

6. *Timeline of Computer History*, COMPUTER HIST. MUSEUM, http://www.computerhistory.org/timeline (last visited Sept. 28, 2013) (noting IBM's introduction of its first personal computer in 1981 and Apple's launch of the first successful mouse-driven computer with a graphic user interface in 1984).

7. Pub. L. No. 99-508, tit. II, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–2712 (2012)). The SCA was included in the Electronic Communications Privacy Act of 1986 (ECPA), which (1) amended the Wiretap Act, 18 U.S.C. §§ 2510–2522; (2) created the Pen Register Act, *id.* §§ 3121–3127; and (3) created the Stored Communications Act, *id.* §§ 2701–2712. Thus, the SCA is sometimes referred to as the ECPA.

8. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

9. *See* 18 U.S.C. §§ 2701–2703 (creating causes of action for intentional unauthorized access to, or dissemination of, electronic communications).

10. *See Security and Surveillance: ECPA*, CENTER FOR DEMOCRACY & TECH., https://www.cdt.org/issue/wiretap-ecpa (last visited Sept. 28, 2013).

11. S. REP. NO. 99-541, at 8 (1986).

12. *See id.* at 10 (stating that outsourced marketing was provided to "businesses of all sizes"); *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1572 (2004) (noting that the first consumer Internet providers did not emerge until 1990).

13. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO WASH. L. REV. 1208, 1243 (2004) ("The SCA has weathered intervening technological advances surprisingly well.").

However, diverging judicial interpretations regarding the SCA's applicability to modern technologies, such as Webmail,[14] have created serious concerns as to the statute's continued viability. Some courts interpret the SCA broadly by applying modern conceptions of new technologies, while others strictly follow the statutory language and history of the Act and assess new innovations within the confines of 1986 technologies.[15] These differing interpretations have created uncertainty regarding the scope of the SCA. In *Jennings v. Jennings*,[16] for example, the Supreme Court of South Carolina unanimously held that unauthorized access by any person to emails stored on Yahoo!'s server did not create a cause of action under the SCA.[17] The Supreme Court of South Carolina's issuance of three opinions in *Jennings* is indicative of the "headaches" courts encounter when applying the SCA to new technologies.[18]

This Note argues that Congress needs to update the SCA to ensure adequate protection of electronic communications. Moreover, it advances that the ultimate outcome of *Jennings* was correct, but that the case's different opinions have increased the uncertainty of the SCA's application. To that extent, this Note proposes crucial legislative reforms and a simple and consistent approach for courts to follow and effectuate Congress's intent.

Part I of this Note provides background information on the evolution of email technologies, a general description of the SCA, and its relevant legislative history. Part II explores the unanswered questions from the statutory text and the inconsistent case law interpreting the SCA's scope. Part III sets forth the current legislative proposals to update the SCA. This Part also proposes much-needed legislative changes and suggests a simple, consistent scheme that courts should use to properly effectuate Congress's intent when applying the SCA to modern technologies. Finally, Part IV explains

---

14. *See infra* text accompanying note 36 (defining "webmail").

15. *Compare, e.g.*, United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (en banc) (concluding that the phrase "electronic communication" encompasses "transient electronic storage that is intrinsic to the communication process for such communications"), *and* Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2004) (broadening the definition of electronically transmitted communications to include messages stored on a web server that have already been received but remain in storage in case a user needs to download them again), *with* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–62 (5th Cir. 1994) (arguing that electronically stored communications are no longer in transmission once received).

16. Jennings v. Jennings, 736 S.E.2d 242 (S.C. 2012), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013).

17. *Id.* at 245.

18. *See* discussion *infra* Part II (outlining the trouble courts experience applying the SCA).

why the *Jennings* court was correct in concluding that unauthorized access to email stored on a remote server does not implicate the SCA.

I. BACKGROUND

A. Email and Its Emerging Technology

Early email systems allowed users to send, transmit, and receive messages between computer terminals via telephone lines.[19] Generally, users could send and receive emails in two ways. First, the transmission could be sent from computer to computer between subscribers of the same email company.[20] These communications remained in electronic form.[21] Once the sender composed and sent the email, the message would travel via telephone lines until it reached the recipient email provider's server.[22] There, the email would sit on the recipient email provider's server until requested via a dial-up modem to connect to the server and download the copy to the recipient's personal computer.[23] Once the message was downloaded, it would be deleted from both the sender and recipient email provider's servers.[24] The second way in which individuals could send or receive emails occurred when the recipient was not an email subscriber.[25] In this scenario, a composer would send the electronic message directly to the email company.[26] Once the company received the message, it converted the message to a hard copy and sent it via traditional mail or courier service.[27] In both cases, the email

19. OFFICE OF TECH. ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 47 (1985) [hereinafter OTA REPORT] (discussing the evolution of electronic written communications), *available at* http://www.justice.gov/jmd/ls/legislative_histories/pl99-508/fgit-1985.pdf.

20. *See Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, & the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 474 (1985) [hereinafter *House ECPA Hearing*] (memorandum from ACLU Project Staff) (detailing the various methods through which electronic mail can be transmitted); OTA REPORT, *supra* note 19, at 47–48 (describing the differences between electronic communication options).

21. OTA REPORT, *supra* note 19, at 47–48.

22. *See* S. REP. NO. 99-541, at 8 (1986).

23. *See id.* (stating that the message would be stored on the electronic mail company's computer "mail box" until the user called to retrieve it).

24. *See* S. REP. NO. 113-34, at 2 (2013) (noting that at the time the SCA was enacted, Congress assumed that most individuals would download emails to their personal computers and ISPs would subsequently delete any emails stored on their servers). *But see* S. REP. NO. 99-541, at 3 (stating that, "to ensure system integrity," service providers did retain copies of these communications for about three months).

25. OTA REPORT, *supra* note 19, at 46–47 (explaining the use of a courier service when an email was sent to a non-subscriber recipient).

26. *Id.* at 48.

27. *Id.*; *see also* Erik Sandberg-Diment, *When Technology Outpaces Needs: Expense*

company created copies of the message along the way "to ensure system integrity" and retained those copies for about three months.[28]

Until the late 1980s, users retrieved their emails under the systems described above using individual networks sanctioned by the government and provided by employers or academic institutions.[29] Due to the prohibitive cost of storage, service providers maintained at most a handful of servers to store data.[30] Accordingly, permanent storage of emails was not feasible. Thus, service providers generally offered two distinct services—email services or outsourced storage services.[31] Due to the expense and limitations of outsourced storage, use of that service was essentially limited to businesses.[32] Therefore, at least with regard to individual use, technology revolved around the personal computer. All information and communications were stored at the system level and could only be accessed through that point.[33]

What was prohibitively expensive at the time Congress enacted the SCA is now commonplace for email users. Today, Internet Service Providers (ISPs), such as Google and Yahoo!, operate data centers

---

and Lack of Standards Frustrate Users of Electronic Mail and Videotex, N.Y. TIMES, June 9, 1985, at F13 (detailing new email services that include "a two-hour delivery of letter-quality documents to many parts of the country").

28. S. REP. NO. 99-541, at 3.

29. *See* Sean Michael Kerner, *Why Cloud Is Like Email in the 1980's*, INTERNETNEWS.COM (May 10, 2011), http://www.internetnews.com/bus-news/article.php/3933111/Why+Cloud+is+Like+Email+in+the+1980s.htm (stating that until the late 1980s, email services functioned separately between service providers, were not connected to the Internet, and required permission from the federal government).

30. *See ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 84 (2010) [hereinafter *ECPA and Cloud Computing Hearing*] (statement of Kevin Werbach, Associate Professor, Legal Studies and Business Ethics, Wharton School, University of Pennsylvania). In 1988, two years *after* the SCA was enacted, the cost of a 1.2 gigabyte (GB) hard drive was $7,799.95. *Amiga Product Guide: Hardware Edition*, 3 AMAZING COMPUTING, no. 3, 1988, at 55, 62. This translates into $15,420.36 in 2013 dollars. *CPI Inflation Calculator*, BUREAU LAB. STAT., http://www.bls.gov/data/inflation_calculator.htm (last visited Sept. 28, 2013) (enter "7,799.95" and "1988," then select "2013" and the "Calculate" button). Today, a consumer can purchase a three terabyte hard drive, or 3,000 times more storage, for only $114.95. *WD My Book 3TB External Hard Drive Storage USB 3.0 File Backup and Storage*, AMAZON, http://www.amazon.com/Book-External-Drive-Storage-Backup/dp/B0041OSQBG/ref=sr_1_fkmr0_2?ie=UTF8&qid=1379464619&sr=8-2-fkmr0&keywords=Western+Digital+MyBook+WDBACW0020H (last visited Sept. 28, 2013).

31. *See* Kerr, *supra* note 13, at 1213–14 (detailing different electronic communications service options utilized at the time the SCA was legislated).

32. *See* William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1207 (2010) (noting that marketing was targeted at business organizations, not individual consumers).

33. *See* S. REP. NO. 99-541, at 8 ("If the intended addressee subscribes to the service, the message is stored by the company's computer 'mail box' until the subscriber calls the company to retrieve its mail . . . .").

spanning the size of several football fields, and provide an almost unlimited amount of storage at no cost to the consumer.[34] These expanded capabilities, combined with affordable mobile devices that provide Internet access, have led many users to use webmail—a cloud computing service[35] that provides a user with the ability to create, send, access, archive, and organize emails through the Internet.[36]

Webmail and other cloud computing services have changed the way most Americans approach email. The personal computer is no longer important as a means for storing or retrieving emails.[37] For webmail users, the computer or mobile device merely serves as a conduit to access the remote server—a situation far from the realm of possibility when Congress enacted the SCA. This stark change in the way Americans communicate has rendered the SCA obsolete in many ways. The task of adapting the SCA to the current—and more advanced—regime of web technology necessarily falls to the legislature.

B. Congress's Creation of the SCA

The 1980s represented the beginning of a "revolution" in the telecommunications infrastructure in the United States that radically changed the way people and entities communicate with one another.[38] While the sudden boom in technology brought advantages, it also became clear that the law did not adequately protect these new and emerging forms of communication.[39]

---

34. *See ECPA and Cloud Computing Hearing*, *supra* note 30, at 84 (acknowledging the rapid shift from personal computing to cloud based computing built upon "massive, multi-billion dollar data centers").

35. Cloud services are applications for media and data storage that are "hosted on or run on Internet servers," allowing the user to run the application and store data on an ISP's remote server rather than on a computer. Joanna Stern, *What Is the 'Cloud'?*, ABC NEWS (June 26, 2012), http://abcnews.go.com/Technology/cloud-computing-storage-explained/story?id=16647561#.UbN6uJW9064.

36. *See id.* (discussing the expansion of network and information storage since the ECPA was first legislated).

37. *See* Maeve Duggan & Lee Rainie, *Cell Phone Activities 2012*, PEW INTERNET & AM. LIFE PROJECT 2, 7 (Nov. 25, 2012), http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_CellActivities_11.25.pdf (showing that 50% of the 85% of adults with cell phones in the United States use their mobile devices to check email); Jay Garmon, *What Is My Gmail Account Really Worth?*, BACKUPIFY (July 25, 2012), http://blog.backupify.com/2012/07/25/what-is-my-gmail-account-really-worth (indicating that the average Gmail account contains 17,640 messages and the average Gmail user adds about 1.4 megabytes (MB) of storage a day, the same amount of data that fit on a floppy disk).

38. *House ECPA Hearing*, *supra* note 20, at 48 (statement of Fred W. Weingarten, Program Manager, Communication and Technologies Program, Office of Technology Assessment) (tracing the consumer shift in telecommunications towards a new paradigm of media, communication, and innovative use of concepts and data).

39. *See* H.R. REP. NO. 99-647, at 18 (1986) ("[T]he same technologies that hold

Congress realized that Title III of the Omnibus Crime Control and Safe Streets Act of 1968[40] (Wiretap Act) and the Fourth Amendment[41]—the two available sources of privacy protection for electronic communications—did not cover certain new forms of these communications.

The Wiretap Act only provided for protection for voice communications sent via common carriers.[42] Thus, non-aural communications such as video, text, digital, and other electronic communications did not warrant protection under the Wiretap Act.[43] Moreover, stored communications did not fall within the parameters of the Wiretap Act.[44]

Similarly, stored communications were left susceptible to discovery under the Fourth Amendment. An individual must have a "reasonable" or "legitimate" expectation of privacy in the information sought to qualify for Fourth Amendment protection.[45] Whether someone possesses a reasonable expectation of privacy is determined by the two-pronged analysis from Justice Harlan's concurrence in *Katz v. United States*.[46] This test, known as the *Katz* test, incorporates both subjective and objective elements by requiring that an individual's conduct reflect "an *actual* (subjective) expectation of privacy" and that the expectation be "one that *society* is prepared to recognize as '*reasonable*.'"[47] Due to the difficulty of proving or disproving an individual's subjective expectations, the objective prong of the *Katz* test—whether society recognizes the individual's subjective expectation as reasonable—is often outcome

such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government."); OTA REPORT, *supra* note 19, at 48 (revealing that "[t]he emergence of electronic mail has raised a number of policy issues," including questions about market structure and regulation, such as whether regulations for common courier systems and private systems should be the same).

40. 18 U.S.C. §§ 2510–2522 (2012).

41. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . but upon probable cause . . . .").

42. Courtney M. Bowman, *A Way Forward After* Warshak*: Fourth Amendment Protections for Email*, 27 BERKELEY TECH. L.J. 809, 814 (2012).

43. *Id.*; H.R. REP. NO. 99-647, at 17.

44. *See* H.R. REP. NO. 99-647, at 17 ("This statutory framework appears to leave unprotected an important sector of the new communications technologies.").

45. Oliver v. United States, 466 U.S. 170, 177, 180–81 (1984).

46. 389 U.S. 347 (1967).

47. *Id.* at 361 (Harlan, J., concurring) (emphasis added).

determinative.[48] Thus, Fourth Amendment protection changes as societal expectations evolve.[49]

Employing the *Katz* test, the Supreme Court has repeatedly held that individuals do not hold a reasonable expectation of privacy in information transmitted to a third party.[50] This third-party doctrine has grave implications for the privacy of any information transmitted electronically, as many courts have used it to hold that the contents of email communications are not protected under the Fourth Amendment.[51] Consistent with *Katz*'s context-based analysis, courts rely on a number of different factors to determine whether the contents of emails are entitled to Fourth Amendment protection. For example, some courts rely on the terms of service agreements or privacy policies associated with a user's account.[52] Additionally,

---

48. OFFICE OF LEGAL EDUC., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 116 (2009) [hereinafter DOJ MANUAL], *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

49. *Compare* Florida v. Riley, 488 U.S. 445, 451–52 (1989) (plurality opinion) (finding that helicopter surveillance of individual's property was not a search under the Fourth Amendment because "no intimate details" of the property were revealed and the officers were flying in public airspace), *and* Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that aerial photograph of a chemical company's industrial complex did not violate the Fourth Amendment in part because the photograph was taken using a conventional commercial camera widely available to the public, and because its "open areas" were comparable to an open field, which is generally not covered by the Fourth Amendment), *with* Kyllo v. United States, 533 U.S. 27, 34–35 & n.2 (2001) (finding a reasonable expectation of privacy in "the relative heat of various rooms in the home" revealed by a thermal imaging device in part because thermal imaging is not widely available to the public).

50. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that the petitioner had no expectation of privacy in the telephone number he dialed because, by using his phone, he "voluntarily conveyed numerical information to the telephone company and . . . [thereby] assumed the risk that the company would reveal to police the numbers he dialed"); United States v. Miller, 425 U.S. 435, 442 (1976) (no reasonable expectation of privacy in bank records); Couch v. United States, 409 U.S. 322, 335–36 (1973) (no reasonable expectation of privacy in records provided to an accountant).

51. *See, e.g.*, United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (suggesting that email is not protected by the Fourth Amendment because, "[w]hile it is clear to this court that Congress intended to create a statutory expectation of privacy in email files, it is less clear that an analogous expectation of privacy derives from the Constitution"); *In re* Search Warrant for Contents of Elec. Mail, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009) (finding no reasonable expectation of privacy in email contents because "defendants voluntarily conveyed to the ISPs and exposed to the ISP's employees in the ordinary course of business the contents of their emails").

52. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 895, 906 (9th Cir. 2008) (finding a reasonable expectation of privacy in a police sergeant's text messages based on the police department's "informal policy that the text messages would not be audited"), *rev'd on other grounds sub nom.* City of Ont. v. Quon, 130 S. Ct. 2619 (2010); Biby v. Bd. of Regents, 419 F.3d 845, 850–51 (8th Cir. 2005) (holding that a university employee had no reasonable expectation of privacy in email where university policy stated that computer files and emails may be searched in response to litigation discovery requests).

courts disagree on whether a reasonable expectation of privacy is relinquished once the intended recipient receives the email.[53] The uncertainty of this fact-based approach makes the status of email under Fourth Amendment jurisprudence impossible to predict.

Congress was concerned that the legal uncertainty created by the inadequacies of the Wiretap Act and the Fourth Amendment with respect to electronic communications would lead to the "erosion of a precious [Fourth Amendment] right" and severely inhibit the progress of telecommunications technology.[54] To address these concerns, Congress sought to fill the gap left open by the Wiretap Act and Fourth Amendment.[55] The result was the SCA, a narrowly tailored and complex statute providing Fourth Amendment-like protections to certain electronic communications modeled on early computer networks.[56] Congress proceeded cautiously and sought a careful balance between three important principles: (1) the public's right to privacy; (2) society's interest in expanding and benefitting from continued technological progress; and (3) the legitimate needs of law enforcement.[57] Consequently, the SCA protects certain electronic communications but also preserves avenues for law enforcement to effectively conduct criminal investigations.[58]

---

53. *Compare* United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (analogizing email to postal mail, which loses its reasonable expectation of privacy upon delivery of the letter, and holding that the Fourth Amendment does not afford protection to "transmissions over the Internet or email that have already arrived at the recipient"), *and* State v. Hinton, 280 P.3d 476, 484 (Wash. Ct. App.) (finding no reasonable expectation of privacy in text messages once the recipient received the messages), *review granted*, 291 P.3d 253 (Wash. 2012), *with* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP." (internal quotation marks omitted)), *and* United States v. Forrester, 512 F.3d 500, 509–11 (9th Cir. 2008) (holding that email metadata, such as the to and from address and the amount of data exchanged, is not protected by the Fourth Amendment, but stating that the contents of emails "may deserve Fourth Amendment protection").

54. H.R. REP. NO. 99-647, at 19 (1986); *see also House ECPA Hearing*, *supra* note 20, at 44 (statement of Fred W. Weingarten, Program Manager, Communication and Technologies Program, Office of Technology Assessment) (indicating that consumers will not use these services and companies will not develop and sell the services if they are not adequately protected).

55. *ECPA (Part I): Lawful Access to Stored Content: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 1–2 (2013) [hereinafter *ECPA Part I Hearing*] (statement of F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations) (observing the legal landscape in 1986 with regard to the inadequate protections for electronic communications that led to the passage of the SCA).

56. *See* discussion *infra* Part I.C (setting forth the structure of the SCA).

57. *ECPA Part I Hearing*, *supra* note 55, at 4 (statement of Bob Goodlatte, Chairman, H. Comm. on Judiciary).

58. *See* S. REP. NO. 99-541, at 5 (1986) ("[The ECPA] represents a fair balance between the privacy expectations of American citizens and the legitimate needs of

C. The Structure of the SCA

The SCA protects stored electronic communications in three ways. First, § 2701 provides a cause of action against anyone who intentionally "obtains, alters, or prevents authorized access" to certain stored communications.[59] Second, § 2702 governs when network providers may voluntarily disclose customer communications and records.[60] Finally, § 2703 regulates when state actors, such as federal and state law enforcement officers, may compel disclosure of stored communications from network service providers.[61]

The statute provides different levels of protection based on the drafters' "perceived importance of the privacy interest involved."[62] The level of protection afforded to any particular information sought turns on two factors: (1) the classification of the network provider and (2) whether the information being sought is in "electronic storage."[63] The SCA addresses the meaning of both of these important factors.

1. Definitions

Congress drafted the SCA with an eye toward the two predominant types of service providers at the time of its passage, which differed in how and why they stored users' data.[64] The SCA therefore distinguishes between "electronic communication service"[65] (ECS) and "remote computing service"[66] (RCS) providers.

An ECS is defined as any service that enables a user to send or receive a wire or electronic communication.[67] Essentially, ECS providers are analogous to the early electronic mail systems, in which messages would be stored until the user dialed-up and retrieved the message via telephone.[68] Congress also sought to protect information stored by third-party service providers, albeit to a lesser degree than ECS stored information, through the creation of RCS. An RCS is

---

law enforcement agencies."); Robison, *supra* note 32, at 1205 (finding that Congress intended to only provide privacy protection to specific areas of electronic data with the passage of the SCA).

59. 18 U.S.C. § 2701(a)(2) (2012).
60. *Id.* § 2702.
61. *Id.* § 2703.
62. DOJ MANUAL, *supra* note 48, at 116.
63. *See infra* Part I.C.2 (discussing privacy protections of the SCA).
64. *See supra* note 31 and accompanying text (reviewing the two types of service options predominantly utilized at the time the SCA was legislated).
65. 18 U.S.C. § 2510(15).
66. *Id.* § 2711(2).
67. *Id.* § 2510(15).
68. *See supra* notes 20–24 and accompanying text (discussing the legislative interpretations of ECS at the time the SCA was debated).

defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[69] Congress intended RCS provisions to regulate information stored by "an off-site computer that stores or processes data for a customer."[70] This category covers any long-term remotely stored communications. Examples of modern services that may qualify as an RCS provider include Dropbox[71] or email stored on Webmail after it has been opened.[72] However, today, nearly all modern technologies can serve multiple functions with regard to a specific communication—an important reason why courts find it so difficult to apply the SCA.[73]

Finally, the term "electronic storage"—quite possibly the most important term in the SCA because communications in electronic storage are afforded the greatest protections—"does *not* simply mean storage of information by electronic means."[74] Rather, the Act specifically defines electronic storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,"[75] as well as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[76] The electronic storage analysis definitively establishes the scope of the SCA.[77]

2. Privacy protections

The SCA tracks these two types of providers and sets forth a bifurcated approach, which generally provides greater protection to

---

69. 18 U.S.C. § 2711(2). An "electronic communications system" is broadly defined in 18 U.S.C. § 2510(14).

70. DOJ MANUAL, *supra* note 48, at 119.

71. Dropbox is an online storage provider that allows users to store photos, documents, videos and files on a remote server so that users can access this data from anywhere. *What's Dropbox?*, DROPBOX, https://www.dropbox.com/tour/1 (last visited Sept. 28, 2013).

72. *See* discussion *supra* Part IV.A (reasoning that post-transmission emails left in storage on webmail servers fall under the RCS provisions).

73. Eric R. Hinz, Note, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 515 (2012) (showing how Dropbox, while most clearly resembling an RCS, can arguably be categorized as an ECS when its sharing function is considered); *see supra* Part II.A (discussing the split of authority surrounding whether an opened email is protected by the act's ECS provisions or falls under the RCS category).

74. DOJ MANUAL, *supra* note 48, at 123.

75. 18 U.S.C. § 2510(17)(A). For clarity's sake, this Note refers to storage described in this subsection as "temporary, intermediate storage."

76. *Id.* § 2510(17)(B). This Note refers to storage described in this subsection as "backup."

77. *See* discussion *infra* Part II.B (debating how differing definitions of electronic storage can change the classification between ECS and RCS, which in turn affects the applicable scope of the SCA).

information stored by an ECS in "electronic storage."[78] A simple subpoena and prior notice of acquisition of electronic communications to the user can compel electronic communications that are not in electronic storage and held by an RCS.[79] Alternatively, the government must comply with the more stringent requirement of obtaining a warrant for electronic communications that are held by an ECS in electronic storage for less than 180 days.[80] More importantly, there is a private cause of action for unauthorized access only if the unlawfully obtained communications are held by an ECS provider in electronic storage.[81] Thus, the scope of the SCA depends on whether an electronic communication is held by an ECS or RCS provider and whether the communication is in electronic storage.

This specifically tailored and complicated approach indicates that the SCA is "not a catch-all statute."[82] Rather, it reflects Congress's careful attempt to fill the gap left open by Fourth Amendment jurisprudence and the Wiretap Act by protecting individuals when they have an actual, reasonable expectation of privacy.[83] Unfortunately, cases interpreting the scope of the SCA are in disarray, and some courts have extended the SCA into areas that Congress likely never intended.

II. QUESTIONS LEFT UNANSWERED BY THE SCA

A. Whether "Post-Transmission" Storage Qualifies as Electronic Storage

Courts across the country disagree on what constitutes "backup protection" under the SCA's definition of electronic storage.[84]

---

78. *Compare* 18 U.S.C. § 2701(a) (unauthorized access provision only available if communication is stored by ECS in "electronic storage"), *id.* § 2702(a) (prohibiting public ECS providers from voluntarily disclosing communications in electronic storage by that service), *and id.* § 2703(a) (requiring the government to obtain a warrant to compel communications held by ECS in "electronic storage" for less than 180 days), *with id.* § 2703(b)(1)(B) (providing that the government can compel communications held by RCS providers with only a subpoena or court order pursuant to 18 U.S.C. § 2703(d), which requires only "reasonable grounds to believe" that information sought is "relevant and material to an ongoing criminal investigation").

79. *Id.* § 2703(b)(1)(A).

80. *See id.* § 2703(a) ("A governmental entity may require the disclosure . . . of a wire or electronic communication, that is in electronic storage in an [ECS] for one hundred and eighty day or less, *only* pursuant to a warrant." (emphasis added)).

81. *See id.* § 2701(a) (providing a cause of action for intentional unauthorized access to a facility that provides electronic communications service).

82. Kerr, *supra* note 13, at 1214.

83. *See* Robison, *supra* note 32, at 1223–32 (discussing the legislative history of the SCA and Congress's intent to provide a limited set of privacy protections where users needed them most); *see also supra* notes 46–49 (discussing the *Katz* test).

84. *See generally* 18 U.S.C. § 2510(17)(B).

Notably, they agree that unopened communications stored by ECS providers are in electronic storage and therefore deserve the full protection of the SCA for 180 days.[85] The dispute lies in whether an already opened email that is stored by a user on the service provider's server qualifies for the Act's heightened "electronic storage" protections.[86]

Under the "traditional narrow interpretation," adopted by the U.S. Department of Justice (DOJ) and many courts, post-transmission emails do not qualify as "electronic storage."[87] Under this interpretation, the "such communication" language in the electronic storage backup provision refers to the temporary, intermediate storage provision.[88] Therefore, "electronic storage" is limited to temporary storage made during transmission of electronic communications and to backups of intermediate communications by the service provider to ensure system integrity.[89] Under this view, communications falling outside of the narrow definition are not protected by the SCA's electronic storage provisions but may still receive protection under the RCS provisions.[90]

In 2004, the U.S. Court of Appeals for the Ninth Circuit rejected the traditional narrow interpretation of electronic storage and created a split in authority that has caused considerable confusion among courts, service providers, and the government.[91] In *Theofel v.*

---

85. *See, e.g.*, Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994) (invoking the SCA's warrant requirement for documents in storage for less than 180 days).

86. These "post transmission emails" include webmail, where all of a user's emails are stored on the remote server. *See supra* Part I.A (arguing that the SCA is inadequate for modern storage systems).

87. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission."); United States v. Weaver, 636 F. Supp. 2d 769, 772–73 (C.D. Ill. 2009) ("If the [SCA] drafters intended emails a user leaves on an email service for re-access at a later date to be covered by section 2702(a)(2), they also must have intended them to be covered by the Government's trial subpoena power."); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (noting that the SCA "only protects electronic communications stored 'for a limited time in the middle of a transmission" (internal quotation marks omitted)); DOJ MANUAL, *supra* note 48, at 123–25 (detailing the types of electronic storage).

88. *See supra* text accompanying notes 75–76 (listing the definition of electronic storage).

89. DOJ MANUAL, *supra* note 48, at 123.

90. *See id.* at 125–26 (illustrating that an email falls under the RCS provisions once a user retrieves the email and decides to store it on the ISP's server).

91. *See* Petition for Writ of Certiorari at 15–21, Jennings v. Broome, 133 S. Ct. 1806 (2013) (No. 12-831), 2013 WL 75746, at *15–21 (noting that the Ninth Circuit decision has left some states with a rule at odds with the DOJ's interpretation of the SCA and has created confusion among district courts).

Farey-Jones,[92] the Ninth Circuit adopted the novel theory that post-transmission email messages qualify as electronic storage for purposes of the SCA because the messages fall within the backup provision.[93]

The *Theofel* court reasoned that interpreting "electronic storage" restrictively to only cover pre-transmission storage would render the backup provision superfluous.[94] According to the court, any backup storage pending transmission would already qualify as "temporary, intermediate storage" within the meaning of 18 U.S.C. § 2510(17)(A).[95] Therefore, whether the electronic messages at issue were in storage was not based on prior access.[96] Moreover, the court argued that the backup provision was not limited to "backup protection" for the ISP's purposes.[97] Rather, storage for the benefit of the user "literally [fell] within the statutory definition."[98]

According to the *Theofel* court, an opened email stored by an ECS provider continues to constitute electronic storage until "the underlying message has expired in the normal course."[99] The court did not provide any guidance as to when an underlying message "expire[s] in the normal course," but it did provide examples suggesting that the lifespan of a backup turns on whether the user or the ISP still need to store the email message.[100] Some courts have adopted *Theofel*'s departure from the traditional interpretation of

92. 359 F.3d 1066 (9th Cir. 2004).

93. *See id.* at 1075–77 (acknowledging that the court's position differs from the Government's and explaining that the analysis turns on whether messages are stored for backup-protection purposes).

94. *See id.* at 1075–76 (noting that, while a copy of an email serves as a backup to the user and the service, the fact that a copy may be a backup does not necessarily mean it is stored for that purpose).

95. *Id.*

96. *See id.* at 1077 (concluding that the government's reading of the SCA was erroneous because prior access is not determinative of whether emails were in storage).

97. *Id.* at 1075.

98. *Id.*

99. *Id.* at 1076.

100. *Id.* at 1070 (discussing the interrelation of messages a user flags for deletion and emails sent to or from the service provider's staff). If either the user or service provider needs the message, it probably has not expired under *Theofel*. *See* Kerr, *supra* note 13, at 1217–18 (describing the *Theofel* standard as a fact-sensitive test under which it is irrelevant whether an email has been accessed).

electronic storage,[101] but the decision continues to receive substantial judicial[102] and academic criticism.[103]

B. Whether the RCS/ECS Distinction is Context-Specific or Provider-Specific

A court addressing an SCA challenge must classify modern technology according to the SCA's 1986 technological constructs—a task seemingly akin to fitting a square peg in a round hole. Not surprisingly, courts across the country are in disarray with regard to what the proper approach should be. Generally, "a single provider can simultaneously provide ECS with regard to some communications and RCS with regard to others, or ECS with regard to some communications and neither ECS nor RCS with regard to others."[104] What determines their role is the type of communications sought.

The SCA and its legislative history embody the principle that a provider is categorized as an ECS or RCS based on an analysis of the provider's role with respect to the particular communication in question.[105] For example, a service provider that is holding intermediate temporary copies of a communication incident to transmission, or backups of those intermediate communications created by that service provider, is protected under the ECS provisions.[106] The same provider is protected by the RCS rules if it holds electronic communications in long-term storage.[107] The same

---

101. *See, e.g.*, Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (asserting that the *Theofel* court correctly reasoned that an email remains in electronic storage both before and after it is read; thus purposefully reading an unauthorized email would be a violation of the SCA); Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (adopting *Theofel* and stating that an email is not removed from the purview of the SCA solely because an individual read it).

102. *See, e.g.*, United States v. Weaver, 636 F. Supp. 2d 769, 772–73 (C.D. Ill. 2009) (determining that *Theofel*'s interpretation of electronic storage "cannot be squared with legislative history and other provisions of the [SCA]"); Flagg v. City of Detroit, 252 F.R.D. 346, 358–62 (E.D. Mich. 2008) (applying RCS provisions to post-transmission content); Jennings v. Jennings, 736 S.E.2d 242, 247 (S.C. 2012) (Toal, J., concurring) ("I advocate a rejection of *Theofel* entirely and the adoption of the 'traditional interpretation' of the SCA, which tracks the statutory language and comports with legislative history."), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013).

103. *See, e.g.*, Kerr, *supra* note 13, at 1217 & n.61 (providing several reasons why *Theofel*'s analysis "is quite implausible and hard to square with the statutory text"); Hinz, *supra* note 73, at 504 (noting that the court never explained what the "normal course" might be).

104. *See* DOJ MANUAL, *supra* note 48, at 127 (explaining the complexities within the ECS/RCS relationship).

105. H.R. REP. NO. 99-647, at 65 (1986) (suggesting that when a user chooses to store a copy of an email on the ISP's server after retrieving the email, the email is protected under the RCS and not the ECS provisions).

106. *See* Kerr, *supra* note 13, at 1215–16.

107. *Id.*

is true for copies of the communication.[108] The communication is protected under the ECS rules as long as it is held in temporary storage.[109] Once the communication is placed in long-term storage, it is protected by the RCS rules.[110]

This legislative intent, however, was arguably ignored by the Ninth Circuit in a case decided shortly after *Theofel*. The *Theofel* court hinted that a network provider cannot qualify as an ECS when it stores the only copy of an electronic communication.[111] However, in *Quon v. Arch Wireless Operating Co.*,[112] the court seemingly refuted the dicta in *Theofel* by focusing on the predominant "nature of services" offered by the provider. In doing so, *Quon* essentially expanded *Theofel*'s holding to network service providers that provide permanent post-transmission storage.[113]

The communications at issue in *Quon* were permanently archived text messages held by a cell phone service provider.[114] The court reasoned that although archived text messages could be considered a "virtual filing cabinet" and thereby resemble RCS, the provider qualified as an ECS because a cell phone service provider predominantly offers services more analogous to those of an ECS.[115] The provider's archival of text messages merely qualified as "backup" as characterized in *Theofel*.[116]

Together, *Theofel* and *Quon* suggest that providers are categorized as a whole, rather than looking to particular communications. Therefore, a service provider that predominately provides ECS-like services will remain an ECS—with its communications in "electronic storage"—indefinitely. Likewise, RCS providers will remain subject to the RCS provisions without regard to the role they play with respect to the communication sought.[117] Like *Theofel*, *Quon*'s "unitary approach" has received considerable criticism, prompting some

---

108. *Id.* at 1216.
109. *Id.*
110. *Id.*
111. Theofel v. Farey-Jones, 359 F.3d 1066, 1076–77 (9th Cir. 2004) ("A[n RCS] might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes.").
112. 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds sub nom.* City of Ont. v. Quon, 130 S. Ct. 2619 (2010).
113. *See id.* at 900; *see also* Flagg v. City of Detroit, 252 F.R.D. 346, 361–62 (E.D. Mich. 2008) (explaining the dicta in *Theofel* and its applicability to *Quon*).
114. *Quon*, 529 F.3d at 900.
115. *See id.* at 902 (explicating that the provider essentially "served as a conduit for the transmission of electronic communications").
116. *See id.* (classifying the service provided as ECS rather than RCS)
117. *See id.* at 900–01 (contrasting the characteristics of RCS with those of ECS).

courts to reject it.[118] This split in authority has left courts confused as to what standard to apply in SCA actions.

C. A State Supreme Court Weighs In

In *Jennings*, the Supreme Court of South Carolina attempted to make sense of the conflicting interpretations and determine the application of the SCA's unauthorized access provision in § 2701 to emails stored by Yahoo!'s webmail service.[119] The case arose from a civil action involving § 2701, but its holding has implications beyond such private actions due to its interpretation of "electronic storage."[120] Notably, the *Jennings* opinion and its lower court rulings are illustrative of the confusion that courts experience when interpreting the SCA's scope and the "headaches" that arise because of that ambiguity.

Jennings arose out of a marital feud. Lee Jennings confessed to his wife, Gail Jennings, that he had fallen in love with another woman, but refused to disclose that woman's identity.[121] He did, however, indicate that he corresponded with the woman via email.[122] Mrs. Jennings' daughter-in-law, Holly Broome, gained access to these emails by guessing the answers to Mr. Jennings's security questions on his Yahoo! email account.[123] During the course of the divorce proceeding, Mr. Jennings discovered that his emails had been hacked and sued Ms. Broome and his wife, along with his wife's divorce attorney and private investigator, for alleged violations of the SCA.[124] The suit resulted in a multi-year litigation, a flip-flop of three

---

118. *See, e.g.*, *Flagg*, 252 F.R.D. at 362–63 (rejecting *Quon* and holding that a cell phone service provider was acting as an RCS with respect to archived text messages because the provider should be classified "with regard to a particular communication, and [not based] upon the classification of the service provider or on broad notions of the service that [it] generally or predominantly provides").

119. *See* Jennings v. Jennings, 736 S.E.2d 242, 243 (S.C. 2012), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013). As previously mentioned, § 2701 requires that the electronic communication be held by the ECS in "electronic storage." 18 U.S.C. § 2701 (2012); *see supra* note 102 and accompanying text (discussing the SCA's unauthorized access language).

120. For a description of the importance of the term "electronic storage," see discussion *supra* Part I.C.2 and *infra* Part III. *See also* Orin Kerr, *South Carolina Supreme Court Creates Split with Ninth Circuit on Privacy in Stored E-mails—and Divides 2-2-1 on the Rationale*, VOLOKH CONSPIRACY (Oct. 10, 2012, 4:24 PM), http://www.volokh.com/2012/10/10/sourth-carolina-supreme-court-deepens-split-on-privacy-in-stored-e-mails-and-divides-2-2-1-on-the-rationale (postulating that *Jennings* "really calls out for U.S. Supreme Court review" because of its broad application and uncertainty relating to the definition of electronic storage).

121. *Jennings*, 736 S.E.2d at 243.

122. *Id.*

123. *Id.*

124. *Id.*

court opinions, and a denial of certiorari to the United States Supreme Court.[125]

The South Carolina trial court found that Mr. Jennings's emails did not meet the requisite element of being in "electronic storage" because his personal storage of emails, which could be deleted at any time, could "hardly be considered part of any 'backup protection' system operated by an [ECS]."[126] The Court of Appeals of South Carolina reversed the trial court and found that Yahoo! undoubtedly provided ECS for Mr. Jennings's emails and that the emails qualified as electronic storage under the backup provision.[127] The appellate court applied *Quon* and *Theofel* to find that Yahoo! "unquestionably" qualified as an ECS by virtue of its overall service in giving its users the ability to send or receive emails.[128] The stored emails qualified as backup because they "were stored on Yahoo's servers so that, if necessary, [Mr. Jennings] could access them again."[129]

The Supreme Court of South Carolina unanimously reversed the appellate court but could not agree on a rationale for doing so.[130] Consequently, the judges issued three separate opinions[131] In the majority opinion, Justice Hearn espoused a textual approach and suggested that the critical question a court must ask to determine whether an electronic communication lies within the backup provision is whether a second copy of the communication exists.[132] Copies of Mr. Jennings's emails stored on Yahoo!'s server could not qualify as "backup" because no evidence indicated that he downloaded or saved another copy of the emails after reading

125. *See* Jennings v. Jennings, No. 07-CP-40-1125, 2008 WL 8185934 (S.C.C.P. Sept. 23, 2008), *aff'd in part*, *rev'd in part*, 697 S.E.2d 671 (S.C. Ct. App. 2010), *rev'd*, 736 S.E.2d 242, *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013).
126. *Jennings*, 2008 WL 8185934.
127. *Jennings*, 697 S.E.2d at 676–78, 681.
128. *Id.* at 676.
129. *Id.* at 678.
130. *Jennings*, 736 S.E.2d at 243.
131. *See id.* at 243, 245.
132. *Id.* at 245. Notably, this approach was adopted by a federal district court in *United States v. Weaver*, 636 F. Supp. 2d 769 (C.D. Ill. 2009). The *Weaver* court invoked dicta from *Theofel* to argue that *Theofel*'s reasoning "relies on the assumption that users download[ed] emails from an ISP's server to their own computers." *Weaver*, 636 F. Supp. 2d at 771–72. The court distinguished "web-based" from "non-web-based" email and found that *Theofel* is inapplicable to "web-based" email because "[u]sers of web-based email systems . . . default to saving their messages only on the remote system." *Id.* at 772. However, the court argued, users can receive protection for "web-based" email under *Theofel* if they deviate from the "default method" and opt to connect to an email program that downloads messages to a personal computer, such as Microsoft Outlook. *Id.*

them.[133] In employing this technical interpretation, the majority was able to avoid the appellate court's reliance on *Theofel* without explicitly rejecting the Ninth Circuit's holding.[134]

In a separate concurring opinion, Chief Justice Toal advocated for a complete rejection of *Theofel*.[135] The Chief Justice reasoned that the conjunctive "and" in the electronic storage definition necessarily indicated Congress's intent that "electronic storage" encompass both temporary, intermediate storage and backups of those communications.[136] Relying on the text and legislative history of the SCA, Chief Justice Toal concluded that the DOJ's traditional narrow interpretation "provide[d] a sounder basis" for the court's holding.[137]

Lastly, Justice Pleicones's opinion incorporated both Justice Hearn and Chief Justice Toal's opinions but provided a different view on the relationship between the temporary, intermediate storage and backup provisions of the electronic storage definition.[138] He emphasized that determining whether an electronic communication is in "electronic storage" necessitates an inquiry into both whether the electronic communication is in temporary or intermediate storage, and whether it qualifies as backup.[139] Justice Pleicones argued that the two provisions describe two types of storage that are "necessarily distinct from one another."[140] Therefore, "an email is protected if it falls under the definition of either subsection (A) or (B)."[141] While technically providing a different view on the relationship between the two electronic storage provisions, Justice Pleicones's opinion is substantively identical to Chief Justice Toal's.[142]

---

133. *Jennings*, 736 S.E.2d at 245 (reasoning that "[t]he ordinary meaning of the word 'backup' is 'one that serves as a substitute or support'" (quoting *Backup Definition*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/backup (last visited Sept. 28, 2013))).

134. *Id.*

135. *Id.* at 247 (Toal, C.J., concurring).

136. *Id.* ("Justice Hearn's approach would delete [the] word ["and"] and insert ["or"] into the statutory text, effectively writing out subsection A from the definition of electronic storage.").

137. *Id.* at 245. Chief Justice's Toal's statement that the definition of electronic storage encompasses both intermediate storage and storage for backup protection does not mean that both subsections (A) and (B) must apply. Kerr, *supra* note 120. Instead, Chief Justice Toal's view is that the storage for purposes of "backup protection" in "(b) refers to back up copies of emails in (a)." *Id.* (explaining the difficulty in interpreting subsections (A) and (B) of 18 U.S.C. § 2510(17) (2012)).

138. *See Jennings*, 736 S.E.2d at 248–49 (Pleicones, J., concurring) (distinguishing that the second copy is created for backup purposes.

139. *Id.* at 249.

140. *Id.*

141. *Id.*

142. *Id.* at 249 n.4. Justice Pleicones wrote a separate opinion to emphasize the idea that analyzing whether an electronic communication is in "electronic storage" requires a court to determine not only whether the electronic communication is in

The SCA's outdated and complicated framework is exemplified in *Jennings*. The three differing opinions are perhaps the most illustrative example of the difficulties courts encounter when applying the SCA as a result of the conflicting jurisprudence interpreting the statute. These difficulties raise serious concerns about the privacy of electronic communications and the continued growth of technological progress.

III. THE FUTURE OF THE SCA

Despite its previous ability to adapt to vast changes in technology, the twenty-seven-year-old SCA has become hopelessly outdated. The Act's framework made sense in 1986 when service providers served two distinct functions, technology and computers were not widely accessible, and remote storage of electronic communications was prohibitively expensive. Today, email has become an integral and necessary part of Americans' professional and personal lives.[143] Most Americans use webmail services and many store these emails and other personal information on the cloud.[144] Individuals use the cloud to store information ranging from personal emails, photos, and videos as a complete back-up of their hard drive.[145] Businesses store emails and highly sensitive information, such as medical and financial data, trade secret information, and business plans on the cloud.[146] The legal uncertainty surrounding the protections afforded to these remotely stored communications leaves today's Congress with the

---

temporary, intermediate storage, but also whether it qualifies as backup. *Id.* at 249. Nevertheless, Chief Justice Toal's opinion does not advocate that only temporary, intermediate storage qualifies as electronic storage. Her opinion calls for two types of protected storage: (1) temporary, intermediate storage and (2) backups of those "intermediate communications." *Id.* at 248 (Toal, J., concurring). The inquiry does not stop at temporary, intermediate storage. Therefore, while theoretically different, Justice Pleicones's opinion does not practically differ from Chief Justice Toal's.

143 *See generally Trend Data (Adults)*, PEW INTERNET, http://www.pewinternet.org/Static-Pages/Trend-Data-%28Adults%29/Online-Activites-Total.aspx (last visited Sept. 28, 2013) (indicating that as of May 2013, 85% of adults in the United States use the Internet and 88% of those users send or receive email).

144. *See* John B. Horrigan, *Use of Cloud Computing Applications and Services*, PEW INTERNET, (Sept. 2008), http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (documenting that as of September 2008, 69% of Internet users use webmail services and other cloud services).

145. Om Malik, *Infographic: Cloud Computing by the Numbers*, GIGAOM (Dec. 7, 2010, 8:54 AM), http://gigaom.com/2010/12/07/infographic-cloud-computing-by-the-numbers.

146. *See* Reuven Cohen, *The Cloud Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing*, FORBES (Apr. 16, 2013, 9:23 AM), http://www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-us-businesses-now-use-cloud-computing.

same problem the 1986 Congress faced—an outdated statute that threatens to inhibit technological innovation.

The 1980s signaled the beginning of an "information age" that fundamentally transformed the lives of individuals throughout the world in ways in which the 1986 Congress could never have imagined.[147] Advertisements for state-of-the-art electronics of the 1980s reveal primitive technology compared to what is available to consumers today.[148] More exciting innovations lie ahead of us.[149] Twenty (and even ten) years from now, newer generations will likely come across advertisements for a $1,400 3D scanner[150] and other gadgets that we consider cutting edge and find the technology and price laughable.[151] However, a failure to update the SCA will

147. *See* John Tammy, *A Blast Back to Our 'Glorious' 1980s Past? Not on Your Life!*, FORBES (Apr. 21, 2013, 10:00 AM) http://www.forbes.com/sites/johntamny/2013/04/21/a-blast-back-to-our-glorious-1980s-past-not-on-your-life (illustrating how simple tasks, such as finding and booking travel reservations, accessing news and sports scores, and coordinating with others on plans, were quite difficult in the 1980s).

148. In fact, a number of websites and blogs have posted articles and videos meant to poke fun at the outdated technology. *See, e.g.*, Brie Hiramine, *15 Hilarious Technology Ads from the 1980s*, MASHABLE, http://mashable.com/2013/06/19/vintage-tech-ads (June 19, 2013) (framing older technology ads as "funny" compared to modern-day technology); Jason M. Vaughn, *Viral Video: Modern Kids Take on 1980's Technology*, FOX 4, http://fox4kc.com/2012/07/09/viral-video-modern-kids-take-on-1980s-technology (July 9, 2012, 9:37 AM) (showing modern children attempting to operate 1980s technology such as a cassette player, a Commodore 64 computer, and an Atari game).

149. *See* Mark P. Mills, *The Next Great Growth Cycle*, AMERICAN (Aug. 25, 2012), http://www.american.com/archive/2012/august/the-next-great-growth-cycle (arguing that a new technology revolution is approaching and will be spurred by three existing innovations: "Big Data, the Wireless Wired World, and Computational Manufacturing").

150. *See, e.g.*, Lucas Mearian, *Makerbot's Desktop Scanner for 3D Printers Will Cost You $1,400*, INFOWORLD, http://www.infoworld.com/d/computer-hardware/makerbots-desktop-scanner-3d-printers-will-cost-you-1400-225470.

151. *See supra* note 148 (describing various blogs and articles making fun of 1980s technologies). *See generally* Oliver Burkeman, *Forty Years of the Internet: How the World Changed Forever*, GUARDIAN (Oct. 22, 2009), http://www.theguardian.com/technology/2009/oct/23/internet-40-history-arpanet (stating that one day in the near future, all of the progress that we have seen in the past forty years will seem like "early throat-clearings—mere preparations for whatever the internet is destined to become"). The relatively recent advent of "smart phones," which are now pervasive, demonstrates how fast technologies—and prices—can change. For example, in 2002, only eleven years ago, Blackberry first added phone capabilities to its devices, which traditionally offered only push email systems and organizer capabilities for corporations. Bruce Brown & Marge Brown, *BlackBerry 5810: Not-So-Convenient Combo Communicator*, PC MAG. (May 13, 2002), http://www.pcmag.com/article2/0,2817,3563,00.asp. The Blackberry 5810 had a retail price of $499 in 2002. *Id.* Today, it is hard to imagine anything that cannot be done on a smartphone, such as Apple's iPhone or Samsung's Galaxy, at a fraction of the price. *See iPhone 5s Review: Same Look, Small Screen, Big Potential*, CNET (Sept. 20, 2013), http://reviews.cnet.com/iphone-5s (showing that the iPhone 5S is available for as low as $199.99); *Samsung Galaxy S4 Review: The Everything Phone for (Almost) Everyone*, CNET (Apr. 23, 2013),

inevitably stunt progress by not providing consumers and businesses the confidence to use new technologies.[152] This "chilling effect" will negatively impact consumer choice and the economy on both a national and global level.[153] Fortunately, legislators have introduced a number of proposals to address these concerns, and recent events have fueled a privacy debate, suggesting that SCA reform may be imminent.[154]

Until Congress acts, however, courts must construe the SCA according to its current terms. As the fragmented opinions in *Jennings* demonstrate, attempting to fit modern technology into the limited technological framework of 1986 has proven to be a daunting task. This difficulty has had impacts beyond courts' application of the SCA. The conflicting opinions make it impossible to predict the outcome of cases and leave individuals, service providers, and law enforcement agencies in the dark about their rights and responsibilities. Additionally, the confusion surrounding the SCA's applicability encourages forum shopping, as the outcome of a case is inextricably tied to where the case is litigated.[155] Therefore, it is

---

http://reviews.cnet.com/samsung-galaxy-s4 (demonstrating the Galaxy S4, with its "laundry list" of features, is available for as low as $99.99).

152. Jeff Jarvis, *I Fear the Chilling Effect of NSA Surveillance on the Open Internet*, GUARDIAN, (June 17, 2013, 2:00 PM), http://www.theguardian.com/commentisfree/2013/jun/17/chilling-effect-nsa-surveillance-internet (expressing concern that increased media coverage of the government's spy operations could cause consumers, businesses, and international users to distrust the Internet and deter people from electronically communicating, sharing, and storing information).

153. *See id.*; Elizabeth MacDonald, *NSA Leaks Slam Cloud Computing Industry*, FOX BUS. (Aug. 9, 2013), http://www.foxbusiness.com/government/2013/08/09/nsa-leaks-slam-cloud-computing-industry ("U.S. technology companies warn they could lose between $21.5 billion to $35 billion in global cloud computing contracts over the next three years due to negative fallout from the U.S. National Security Agency (NSA) spying programs on Internet users, including emails."); *see also Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity*, MCKINSEY GLOBAL INST. (May 2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters (documenting the Internet's contribution to the global economy and the United States' role as "the largest player in the global Internet supply ecosystem"); Robert Lemos, *U.S. Surveillance Fallout Costing Third-Party Providers*, DARK READING (Aug. 23, 2013), http://www.darkreading.com/monitoring/us-surveillance-fallout-costing-third-pa/240160404 (noting that two secure email service providers—Lavabit and Silent Circle—shut down email services in the United States due to concerns that privacy laws failed to protect their customer's stored email communications).

154. Increasing media coverage and public outrage illustrating the real privacy threat to remotely stored electronic communications has prompted members of Congress from both the Republican and Democrat parties to join together and support reforming the SCA. *See* Carl M. Cannon, *Digital Privacy, a Non-Partisan Issue*, REAL CLEAR POLITICS (July 23, 2013), http:// http://www.realclearpolitics.com/articles/2013/07/23/digital_privacy_a_non-partisan_issue_119332.html (stating that recent revelations that the NSA engaged in a domestic spying operation gaining access to a host of Americans' private electronic communications has "given [an] added impetus" to SCA reform legislation).

155. For example, in the Ninth Circuit, Mr. Jennings would have been able to

important to promote consistency by setting forth clear rules that courts must follow to determine whether a communication is protected by the SCA.

To provide this consistency, courts should seek to effectuate Congress's intent at the time the SCA was enacted in order to avoid "blur[ring] the distinctive functions of the legislative and judicial processes."[156] Courts are constricted by the SCA and cannot enlarge its scope without Congressional authority.[157] Doing so would severely undermine the Nation's carefully balanced system of government that delegates specific powers to three separate branches of government.[158] To avoid upsetting this balance, courts must attempt to classify new technology according to the distinctions embodied in the SCA.

Despite the seemingly complicated structure of the SCA, an analysis of the language and legislative history of the Act suggests that applying its provisions to new technologies, such as webmail, is not an impossible task. By focusing on the legislative history and intent of Congress in light of the technology available when it passed the SCA, a simple framework emerges.

A. Amending the SCA

1. On the right path: Current proposed reforms

Congress is attempting to tackle the privacy concerns that threaten to stifle progress. On March 19, 2013, Senator Patrick Leahy introduced the Electronic Communications Privacy Act Amendments Act of 2013[159] ("S. 607"). This bill would amend the SCA's voluntary

---

bring a cause of action under § 2701. Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2004). However, the South Carolina Supreme Court precluded that option. *See* Jennings v. Jennings, 736 S.E.2d 242, 244–45 (S.C. 2012), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013).

156. *See* Addison v. Holly Hill Fruit Prods., 322 U.S. 607, 618 (1944) (warning against creating judicial legislation by deleting a portion of a definitive statute and applying the resulting definition to the instant case).

157. *See* Life Receivables Trust v. Syndicate 102 at Lloyd's of London, 549 F.3d, 216 (2d Cir. 2008) (stating that courts "must interpret a statute as it is, not as it might be"); Belfield v. Coop, 134 N.E.2d 249, 256 (Ill. 1956) ("The only legitimate function of the courts is to declare and enforce the law as enacted by the legislature, to interpret the language used by the legislature where it requires interpretation, and not to annex new provisions or substitute different ones, or read into a statute exceptions, limitations, or conditions which depart from its plain meaning.").

158. *See, e.g.*, *Life Receivables Trust*, 549 F.3d at 216 (explaining that it is not the role of the courts to legislate); Schrock v. Shoemaker, 640 N.E.2d 937, 945 (Ill. 1994) (describing the courts' function within the separation of powers framework provided by the Constitution).

159. S. 607, 113th Cong. (as reported by S. Comm. on the Judiciary, Apr. 25, 2013). Two identical proposals have also been introduced in the U.S. House of

and compelled disclosure provisions in § 2702 and § 2703 to require the government to obtain a warrant to gain access to the contents of any electronic communications stored on the cloud.[160] First, the bill would generally prohibit an ECS or RCS from voluntarily disclosing the contents of its customer's electronic communications to the Government.[161] Second, the bill would retain the ECS and RCS distinction but adopt one standard—a search warrant supported by probable cause—for the disclosure of a customer's electronic communications held in "electronic storage with or otherwise stored, held, or maintained by the provider."[162] Under the new provision, the government would be required to notify the individual whose account was disclosed within a specified period of time.[163] Finally, S. 607 would eliminate the SCA's 180-day rule that allows the government to obtain emails in electronic storage after 180 days.[164]

The Senate Judiciary Committee approved S. 607 on April 25, 2013.[165] The House also held hearings in March and April of 2013 dedicated to ECPA reform, suggesting that Congress is committed to at least some change in legislation.[166]

Representatives: the Email Privacy Act, H.R. 1852 (2013), and the ECPA Amendments Act, H.R. 1847 (2013). Another similar proposal, introduced by Representatives Zoe Lofgren, Ted Poe, and Suzan DelBene called the Online Communications and Geolocation Protection Act, H.R. 983 (2013), is identical to S. 607 with regard to electronic communications but would also require a warrant for location information generated by mobile phones. As of September 29, 2013, H.R. 1852, H.R. 1847, and H.R. 983 have yet to be heard by their referred committees.

160. *See* S. 607 § 3(a) ("A governmental entity may require the disclosure by a provider of electronic communication service or remote computing service of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only if the governmental entity obtains a warrant . . . .").

161. *See id.* § 2. There are current exceptions to this prohibition already embodied in the law, such as the customer consent requirement. *See id.* § 3 (a).

162. *See id.* § 3(a) (requiring the government to obtain a warrant for the contents of remote computing services as well). The language after electronic storage clarifies that electronic storage included opened and unopened emails.

163. *Id.* (requiring government notification, along with a copy of the search warrant and other details about the information acquired, within ten businesses days for a law enforcement agency and three business days for other agencies). The bill also provides procedures and standards the government may use to delay this notice requirement. *Id.* § 4.

164. *See id.* § 4 ("A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order delaying the notification required under section 2703(b) for a period of not more than 180 days in the case of a law enforcement agency, or not more than 90 days in the case of any other governmental entity.").

165. David Kravets, *Law Requiring Warrants for E-mail Wins Senate Committee Approval*, WIRED (Apr. 25, 2013, 11:42 AM), http://www.wired.com/threatlevel/2013/04/email-warrants-bill.

166. *See ECPA Part I Hearing*, *supra* note 55, at 4 (statement of Bob Goodlatte, Chairman, H. Comm. on Judiciary) (stating the Judiciary Committee "will modernize the decades' old Electronic Communications Privacy Act to reflect our current digital

2. Suggested amendments to modernize the statute

The SCA's complicated structure has confused courts and created a myriad of different protections that are seemingly inconsistent.[167] For example, under the current language, the same email is subject to different protection depending on whether it is in transit, stored on a home computer, opened and stored in remote storage, unopened and stored in remote storage for 180 days or less, or unopened and stored in remote storage for more than 180 days.[168] It is therefore not surprising that courts have difficulty construing the statute. Any change to the SCA should focus on simplifying this structure to ensure consistent results and avoid the need for further legislative revisions soon after its enactment.

Such a proposal would include three key changes. First, Congress should focus on technological neutrality to ensure the vitality of the amendment for years to come.[169] The 1986 Congress achieved its goal of technological neutrality when it enacted the SCA in some respects[170] but failed in others.[171] Accordingly, the SCA is illustrative of the benefits of technological neutrality and the cautions of the lack thereof. The neutral aspect of the SCA allows it to be equally applicable to webmail and newer technologies such as Facebook

---

economy while preserving constitutional protections"); *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 63 (2013) (statement of Bob Goodlatte, Chairman, H. Comm. on the Judiciary) (identifying a future goal to "protect individual liberties by providing clear guidelines for when and how geolocation information can be accessed and used").

167. *See* discussion *supra* Part I.C.2. (outlining privacy protections of the SCA); *see also* discussion *supra* Part II.A. (noting the conflict between courts with regard to whether "post-transmission" storage qualifies as electronic storage).

168. *Electronic Communications Privacy Act (ECPA)* EPIC http://epic.org/privacy/ecpa/#background (last visited Sept. 28, 2013) (illustrating, in a table, the different levels of protection for email under the SCA).

169. *See* H. REP. No. 106-932, at 9 n.1 (2000) (noting that "[r]egulation tied to a particular technology may quickly become obsolete and require further amendment" (internal quotation marks omitted)); Kevin Bankston, *Today's Other ECPA Reform News: Location Privacy Hearing in the House*, CENTER FOR DEMOCRACY & TECH. (Apr. 25, 2013) https://www.cdt.org/blogs/kevin-bankston/2504today%E2%80%99s-other-ecpa-reform-news-location-privacy-hearing-house ("[L]egislation that isn't technology neutral . . . is doomed to become increasingly meaningless." (internal quotation marks omitted)).

170. John R. Kresse, Comment, *Privacy of Conversations over Cordless and Cellular Telephones: Federal Protection Under the Electronic Communications Privacy Act of 1986*, 9 GEO. MASON U. L. REV. 335, 342 (1987) (stating that the ECPA embodied a broad and general definition of wire, oral, and electronic communications to meet the drafters' goal of drafting a "technology neutral" statute).

171. *See supra* Part II.C (discussing the structure of the SCA and its framework based on the two predominant types of service providers at the time of its passage).

messages and private Twitter Direct Messages.[172] On the other hand, by virtue of the Act's structure being necessarily based on the types of service providers in 1986 and the ways users and service providers traditionally stored communications, the Act has become obsolete, and many forms of modern communications are left without protection.[173] Consequently, Congress should update the Act's framework by eliminating the outdated distinctions between ECS and RCS and instead providing rules based on the type of communication involved.[174] In so doing, the amendment will be technologically neutral and achieve the objective that Congress sought in 1986.[175]

Second, Congress should provide a clear definition of electronic storage that, at the very least, clarifies that the term "electronic storage" encompasses both opened and unopened emails.[176] Whether an email is in transit, opened, or unopened should not determine its level of protection. Expanding the electronic storage definition in this manner will ensure proper protection from unauthorized access by a private party or the government.

S. 607 attempts to settle the opened/unopened distinction by including language indicating that all communications in electronic storage "with or otherwise stored, held or maintained" by an ECS or RCS are subject to a warrant requirement.[177] However, the bill's failure to provide a clear definition of electronic storage, coupled

---

172. Chris Soghoian, *US Surveillance Law May Poorly Protect New Text Message Services*, ACLU (Jan. 8, 2013, 9:44 AM), https://www.aclu.org/blog/national-security-technology-and-liberty/us-surveillance-law-may-poorly-protect-new-text (observing that, while the privacy laws have a number of flaws, the fact that they are "largely neutral with respect to particular technologies" has allowed them to adapt to newer forms of communication, such as Facebook messages and Snapchat photos).

173. *See supra* Part II (discussing the problems courts experience in trying to categorize modern technology into technological constructs from 1986).

174. Hinz, *supra* note 73, at 514–18 (illustrating how new technologies, such as Dropbox, Webmail, and social networking websites, blur the ECS and RCS lines because they can be categorized as both).

175. *See supra* notes 169–171 and accompanying text.

176. The distinction between opened and unopened communications is the product of 1986 technologies, when few Americans had access to a computer, the Internet, or email, and the feasibility of remote storage was virtually nonexistent. *See* discussion *supra* Part I.A. This is likely the reason that the 1986 Congress decided remote storage was not entitled to the heightened ECS protections. *See supra* text accompanying note 62 (stating that the SCA provides different levels of protection based on the privacy interest involved). Because remote storage was not widely available, and most individuals and businesses downloaded private email communications to their computers, the need for protecting these communications in remote storage was not yet apparent. As access to email and remote storage has increased and become ubiquitous, the opened versus unopened differentiation no longer makes sense. *See supra* notes 143–144 and accompanying text (demonstrating that the majority of American adults now use email and cloud computing services).

177. S. 607, 113th Cong. § 3(a) (as reported by S. Comm. on the Judiciary, Apr. 25, 2013).

with its retention of the ECS and RCS distinctions raises questions as to the scope of electronic storage.[178] Moreover, challenges under § 2701 will remain subject to the ambiguous case law discussed in Part II, including *Jennings*.[179] This remaining uncertainty is unfortunate because courts continue to grapple with this very issue and would greatly benefit from a clear directive.[180]

With a clear definition of electronic storage, Congress should then provide for one disclosure standard: the government must obtain a warrant to gain access to emails that are held in electronic storage.[181] This rule would ensure consistent results and account for society's changing privacy expectations regarding electronic communications.[182]

Because Fourth Amendment jurisprudence regarding privacy protections focuses on necessity and expectations, Congress could evaluate the necessity of using electronic communications and

---

178. For example, the bill is ambiguous regarding whether Congress would be imposing a warrant requirement for all remotely stored communications or just emails. A court could arguably find support for either argument. Electronic storage necessarily requires either "temporary, intermediate storage" or storage of such communication by an ECS for backup protection. A court could interpret S. 607's new language as still requiring an analysis of "electronic storage" prior to applying the warrant requirement. A court could therefore reason that communications held by an RCS provider (whatever it determines that to be) still cannot be in electronic storage and, therefore, are not subject to the warrant requirement. This is because the only "stored" communications that can qualify as electronic storage are those held by an ECS. Alternatively, a court could find that all stored communications are subject to the warrant requirement by interpreting the "otherwise stored, held, or maintained" language as nullifying the electronic storage definition's "temporary, intermediate" storage. If Congress does intend that courts apply this second interpretation, then why would it retain the electronic storage, RCS, and ECS distinctions? In either case, Congress should provide clearer rules for courts to apply.

179. *See supra* note 81 and accompanying text (noting that the SCA provides a private cause of action only if the communication was in electronic storage when it was unlawfully acquired); s*ee also* discussion *supra* Part II (discussing case law interpreting the SCA).

180. *Compare* Ehling v. Monmouth-Ocean Hosp. Serv. Corp., No. 2:11-CV-03305 (WJM), 2013 WL 4436539, at *7 (D.N.J. Aug. 20, 2013) (invoking *Theofel* and *Quon* to find that Facebook wall posts were held in electronic storage under the SCA's backup provision even though they are stored indefinitely), *with* Lazette v. Kulmatycki, No. 12-02416, 2013 WL 2455937, at *7 & n.13 (N.D. Ohio June 5, 2013) (rejecting *Theofel* and *Quon* to hold that opened emails stored on a remote server did not qualify as "electronic storage" because they were not being kept for the purposes of backup protection).

181. S. REP. NO. 113-34, at 3 (2013) (indicating that one disclosure standard requiring a warrant for compelled disclosure is necessary to "keep pace with the advances in technology in order to ensure the continued vitality of the Fourth Amendment").

182. *Id.* at 2–3 (noting that most Americans regularly use email in their personal and professional capacities and often use it for confidential communications, and the constitutional uncertainty of SCA provisions allows for the acquisition of personal emails by the government without a search warrant).

remote computing servicers with users' expectation that their communications would not be exposed to a service provider when adapting the third-party doctrine.[183] In 1986, few people had access to remote storage, the Internet, or even a computer.[184] Today, these things are not only convenient, but, for many, are necessities of everyday life.[185] Few Americans make it through a day without accessing a computer or the Internet.[186] Without access to these forms of communications, modern businesses could not function and citizens' lives would be significantly impacted.[187] Individuals should not be forced to sacrifice privacy in order to effectively communicate. Therefore, the government should be required to obtain a warrant to gain access to these electronic communications.[188]

Finally, as S. 607 does, Congress should eliminate the 180-day distinction.[189] In 1986, there was no plausible reason why a service provider would keep an electronic communication over 180 days. Therefore, Congress adopted the 180-day rule because it analogized a stored email for over 180 days as abandoned property using Fourth Amendment jurisprudence and archaic property law principles.[190] According to Congress, individuals did not have a reasonable

---

183. *See supra* note 49 and accompanying text (discussing Supreme Court cases showing that Fourth Amendment protection changes as the expectations of society change).

184. *See* CENSUS BUREAU, U.S. DEP'T OF COMMERCE, COMPUTER AND INTERNET USE IN THE UNITED STATES: POPULATION CHARACTERISTICS, at 1–2 & fig.1, 9, 11 (2013), *available at* http://www.census.gov/prod/2013pubs/p20-569.pdf ("In 2011, 75.6 percent of households reported having a computer, compared with only 8.2 percent in 1984 . . . ."). *See generally* Angela Bartels, *[INFOGRAPHIC] Data Storage 101*, RACKSPACE (July 20, 2011), http://www.rackspace.com/blog/infographic-data-storage-101 (stating that only 1% of data was stored digitally in 1986 compared to 94% in 2007); *supra* note 30 and accompanying text (discussing the prohibitive cost of storage).

185. CISCO, 2011 CISCO CONNECTED WORLD TECHNOLOGY REPORT 10 (2011), *available at* http://www.cisco.com/en/US/netsol/ns1120/index.html#~2011 (reporting a survey of college students and young professionals around the world showing that nearly one-third of respondents believe "the Internet is as important to them as water, food, air, and shelter").

186. *See More Than 2 Billion People Use the Internet, Here's What They're Up To*, CULTURE-IST (May 9, 2013), http://www.thecultureist.com/2013/05/09/how-many-people-use-the-internet-more-than-2-billion-infographic (showing that 70% of the 2.4 billion Internet users worldwide use the Internet every day and that there are eight new Internet users every second).

187. NAT'L SMALL BUS. ASS'N, 2010 SMALL BUSINESS TECHNOLOGY SURVEY 3, 7 (2010), *available at* http://www.nsba.biz/docs/nsba_2010_technology_survey.pdf (noting that "[t]he average small-business owner uses 19 computers in his or her business" and that 84% of small businesses have a web site).

188. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299–30 (2004) (discussing justifications for implementing a universal search warrant requirement).

189. S. 607, 113th Cong. 3 (as reported by S. Comm. on the Judiciary, Apr. 25, 2013).

190. H.R. REP. NO. 113-34, at 2 (2013).

expectation of privacy in these messages.[191] The 180-day rule is largely irrelevant in today's society as email is saved for years on remote servers.[192] Many of these saved emails are password protected, and most individuals reasonably believe that service providers do not have access to them.[193]

B. Judicial Change: A Simple Approach to Applying the Current SCA

Until Congress provides the necessary reforms, courts must construe the statute and carry out Congress's intent from when the SCA was enacted. The legislative history and statutory text provide helpful guidance. As previously mentioned, privacy protections under the SCA hinge on whether a provider is an ECS or RCS and whether the information is in "electronic storage."[194] Most commentators and courts either treat these distinctions as two separate inquiries or muddle them without explanation.[195] However, close examination of the statute and legislative history indicate that the process of determining the scope of the SCA is more straightforward than these cases would suggest.

Rather than focusing on specific technologies, Congress phrased the protections throughout the SCA in terms of transmission in an effort to draft a forward-looking statute that would evolve to keep up with new technologies.[196] Thus, the Act focused on the function that

---

191. Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1422 (2004) (stating that the SCA's 180-day rule necessarily embodies the premise that users do not have a reasonable expectation of privacy in those communications).

192. *See* Garmon, *supra* note 37 (noting the vast amount of emails users save on Gmail servers).

193. *See* United States v. Warshak, 631 F.3d 266, 284–86 (6th Cir. 2010) (reasoning that society is prepared to recognize a reasonable expectation of privacy in email because email has, in many ways, replaced traditional forms of communication such as the telephone call and letter); *Get the Facts*, SCROOGLED, http://www.scroogled.com /mail/GetTheFacts (last visited Sept. 28, 2013) (showing results of a 2012 study indicating that 89% of Gmail users believe their email is private).

194. *See* discussion *supra* Part II.A–B (weighing the similarities and differences between ECS and RCS).

195. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902–03 (9th Cir. 2008) (finding archived text messages in backup of "electronic storage" definition because cell-service provider qualified as ECS), *rev'd on other grounds sub nom.* City of Ont. v. Quon, 130 S. Ct. 2619 (2010); Jennings v. Jennings, 736 S.E.2d 242, 249 (2012) (Toal, J., concurring) (reasoning that Mr. Jenning's emails were not in "electronic storage" by invoking legislative history indicating that Yahoo! was RCS), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013).

196. *See A Bill To Amend Title 18, United States Code, with Respect to the Interception of Certain Communications, Other Forms of Surveillance, and for Other Purposes: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights & Trademarks of the S. Comm. on the Judiciary*, 99th Cong. 37–39 (1985) (statement of Rep. Carlos J. Moorhead) (opining that legislation attempting to take into account the specifics of varying, evolving technology would be too complex and would require frequent revisions).

ISPs play for their customers rather than the medium used to provide the service.[197] The language and structure of the Act provide considerable insight into Congress's intent with regard to the function that must be analyzed to determine the SCA's applicability.

The Act impliedly distinguishes between two types of storage: electronic storage and regular computer storage.[198] It then links the type of storage to ECS providers or RCS providers.[199] The unauthorized access provision in § 2701 only provides a cause of action for communications held by ECS providers in electronic storage.[200] Similarly, the Act's ECS provisions in § 2702(a)(1) and § 2703(a) only protect information in electronic storage.[201] On the other hand, the RCS provisions in § 2702(a)(2) and § 2703(b), as well as the definition of RCS in § 2711(2), protect regular computer storage.[202] The term "electronic storage" only appears in conjunction with ECS providers,[203] and the term "computer storage" only appears in connection with RCS providers.[204] This link indicates that the type of storage service provided is the "function" that Congress described in the legislative history as dispositive in the SCA analysis.[205] This interpretation focuses on a service provider's actual function with regard to a particular communication rather than categorization of archaic technological frameworks—the exact solution Congress envisioned to combat the growing privacy implications of rapidly changing technology.[206]

With this understanding, a more straightforward framework emerges and provides three options for all electronic communications. First, if a communication lies within the "electronic storage" definition, it is protected under the ECS provisions as long as it is not older than 180 days and does not fall under an exception

197. *See id.* at 37 (explaining the significance of focusing the Act on a function rather than a technology).
198. *See* discussion *supra* Part II.B.
199. *See infra* notes 200–204.
200. *See* 18 U.S.C. § 2701(a) (2012).
201. *See id.* §§ 2702(a)(1), 2703(a).
202. *See id.* §§ 2702(a)(2), 2703(b), 2711(2).
203. *See id.* § 2701 (unauthorized access ECS provision); *id.* § 2702(a)(1) (ECS voluntary disclosure provision); *id.* § 2703(a) (ECS compelled disclosure provision).
204. *Id.* § 2702(a)(2) (RCS voluntary disclosure provision); *id.* § 2703(b) (RCS compelled disclosure provision); *id.* § 2711(2) (RCS definition).
205. *See supra* notes 196–197 and accompanying text (explaining that Congress focused the SCA on a function rather than on technology to avoid frequent revisions).
206. *See House ECPA Hearing*, *supra* note 20, at 474 (indicating that the SCA has been able to mold new technologies because it focuses on function rather than technology).

in the Act.[207] Second, if the communication is in regular "computer storage," it may be protected under the RCS provisions.[208] Third, those communications that do not lie within the preceding two categories fall outside of the SCA altogether.[209]

Moreover, this framework better comports with congressional intent. Unlike the providers in 1986, most modern providers supply ECS and RCS services interchangeably.[210] For this reason, courts have had trouble categorizing newer services such as social networking websites pursuant to the SCA's framework.[211] Adopting a "function" approach, as envisioned by Congress, eliminates this confusion by creating a simple process: analyze the communication involved and determine whether the communication is in "electronic storage" or "computer storage," irrespective of the type of provider. Once this is determined, the communication necessarily falls into either the ECS or RCS category or outside the SCA altogether.

Finally, by focusing on the information sought and the function of the communication, this interpretation answers the uncertainties left by *Quon*. Adopting *Quon*'s "all or nothing" approach would undermine the statutory scheme and fail to take into account the entire statute by focusing solely on the class of provider without accounting for the fact that ISPs provide *both* ECS and RCS services.[212] This "all or nothing" approach also creates holes in the electronic storage definition. Applying *Quon*'s reasoning, a court could

---

207. 18 U.S.C. §§ 2702(a)(1), 2703(a) (2012).

208. *Id.* §§ 2702(a)(2), 2703(b); *see supra* notes 105–110 and accompanying text (noting legislative history suggesting that an ECS provider becomes an RCS provider once an email is stored on a remote server indefinitely). Apart from qualifying as an RCS provider pursuant to the RCS definition, an RCS provider must further satisfy two requirements to enjoy the RCS privacy protections. The communications must be "carried or maintained" by the RCS "solely for the purpose of providing storage or computer processing services." *Id.* §§ 2702(a)(2), 2703(b)(2)(B). Moreover, the RCS cannot be "authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." *Id.* §§ 2702(a)(2)(B), 2703(b)(2)(B).

209. This third category encompasses both communications in electronic storage stored for more than 180 days and communications stored by RCS providers that do not meet requirements imposed on RCS providers. *See* Robison, *supra* note 32, at 1212–23 (discussing reasons why "cloud computing" services may not qualify as RCS).

210. DOJ MANUAL, *supra* note 48, at 120 (asserting that the either RCS or ECS approach contravenes the SCA's language and legislative history and noting that nothing prevents service providers from offering customers both ECS and RCS).

211. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (holding that subpoenas on Facebook and MySpace seeking private messaging were quashed under the SCA). The court could not determine whether the subpoenas seeking Facebook wall posting and MySpace comments could be quashed under the SCA because of insufficient evidence. *Id.*

212. *See supra* note 118 and accompanying text (noting that *Quon*'s approach has received considerable criticism from courts).

conclude that a modern-day provider such as Facebook predominately provides RCS services via storage of its wall posts, despite Facebook's "messaging" feature, which highly resembles an ECS service.[213] This rigid "provider-specific" interpretation would unnecessarily restrict the SCA's scope and deprive Facebook communications of the protections afforded to communications held by the ECS provider in electronic storage. On the other hand, the function-specific approach would focus on the particular communication—wall post or message—rather than categorize Facebook as RCS or ECS for all communications based on its predominant use. Consequently, it allows a court to analyze providers' services separately with respect to the particular communication, thereby removing the importance on the type of technology or provider used.

IV. APPLYING THE SCA TO MODERN TECHNOLOGY

A. An Email Stored on a Server After It Has Been Opened Is Not in "Electronic Storage"

Equipped with the simpler analysis identified in Part III.B, courts can apply the current formulation of the SCA to modern technology. Notably, even if Congress enacts S. 607 in its current form, this analysis would remain unchanged with regard to a § 2701 inquiry.[214] The only questions become: what is electronic storage, and how does it differ from regular computer storage? According to a House Report, email is in electronic storage while it is awaiting retrieval by its intended recipient (Phase I).[215] Once the user opens the email and decides to store that information indefinitely on the provider's

213. *Compare Crispin*, 717 F. Supp. 2d at 987 (holding that Facebook messages that were analogous to email communications qualified as ECS services, but also finding that the same service provider was an RCS with respect to wall postings that were stored on the server and available to the public), *with* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008) (holding that a cell phone provider was an ECS with regard to archived text messages because it predominately provided the ability to send and receive electronic communications), *rev'd on other grounds sub nom.* City of Ont. v. Quon, 130 S. Ct. 2619 (2010).

214. *See supra* note 177–180 and accompanying text (showing the implications of S. 607's failure to address the electronic storage definition). Congress's failure to amend the electronic storage definition could lend even more credence to the argument that post-transmission emails are not in electronic storage for purposes of § 2701. *See infra* notes 242–247 and accompanying text.

215. *See* H.R. REP. NO. 99-647, at 63 (1986) (stating that an electronic mail service that allows a user to send a message to the recipient's server "where it is held in storage until the [recipient] requests it" is subject to § 2701).

server (Phase II), the email falls out of the "electronic storage" provision and the provider becomes an RCS provider.[216]

Congress's intent to kick the ECS provider outside of the ECS protections once Phase II begins evidences the "electronic storage" versus "computer storage" distinction.[217] During Phase I, the email provider is providing services similar to early email systems. On the other hand, Phase II more closely resembles regular "computer storage" analogous to hospital and physician records and, for this reason, falls outside of the ECS category.[218]

This phased analysis comports with the narrow concept of "electronic storage" adopted under the SCA in light of the technology and electronic mail system of 1986 and Congress's policy objectives in enacting the statute.[219] The distinction between opened and unopened email, which seem arbitrary to modern-day users, starts to make sense when analyzed under this lens.[220] The "electronic storage" definition addresses the two primary privacy concerns from 1986; those of unauthorized access (1) of a message on the ISP's servers, awaiting retrieval by its recipient,[221] and (2) to copies of messages that service providers often stored for approximately three months to ensure "system integrity."[222] In light of this understanding, whether a communication falls under the backup provision is determined through the perspective of the ISP, rather than the user.[223] By stating that the backup must be stored *by* an ECS for purposes of backup protection, the statutory language in the backup provision itself suggests that it requires a more affirmative act on behalf of the service provider than simply providing a service allowing users to store their emails online.[224]

---

216. *Cf. id.* (noting that once the voicemail user requests and receives the message and decides to store it, it is protected under the voluntary disclosure provisions and not § 2701, which requires the communication to be in electronic storage).

217. *See* H.R. REP. NO. 99-647, at 62, 65.

218. S. REP. NO. 99-541, at 3 (1986) (explaining that services that create electronic copies for later reference and are subject to the control of a third party computer operator, such as hospital medical files and providers of electronic mail, are not entitled to ECS protection).

219. *See supra* note 57 and accompanying text (noting three important principles guiding legislative intent in drafting the SCA).

220. *See* discussion *supra* Part I.A (discussing early email networks that automatically deleted messages from remote servers once a user downloaded the message, but noting that service providers often kept a copy for administrative purposes).

221. *See* 132 CONG. REC. 27,635 (1986) (declaring that the SCA provides protections for unauthorized access to messages "stored for later forwarding" by the electronic mail company).

222. S. REP. NO. 99-541, at 3.

223. *See* 18 U.S.C. § 2510(17)(B) (2012).

224. *See id.*; *see also* Jennings v. Jennings, No. 07-CP-40-1125, 2008 WL 8185934

Moreover, this interpretation complies with Congress's intent to provide tiered levels of protection based on when it deemed a user had a reasonable expectation of privacy.[225] The SCA accords the highest protection to an email that is on the electronic mail server waiting for the recipient to retrieve it because the user reasonably expects that the email has similar protections to postal mail.[226] Similarly, while the email is in transit, the user does not reasonably expect the service provider to access the email or create any copies.[227] Therefore, backup copies that the service provider creates for administrative purposes are also afforded the Act's highest protections for 180 days[228]—the longest amount of time Congress thought that ISPs would possibly store these copies.[229] On the other hand, once the email reaches its recipient, the user's reasonable expectation of privacy diminishes in accordance with 1986 technology. In 1986, users did not have an option to store email on the web; rather, emails were either downloaded onto a personal computer or discarded.[230] For this reason, Congress did not believe that post-transmission emails stored on a server qualified as "electronic storage."

(S.C.C.P. Sept. 23, 2008), *aff'd in part*, *rev'd in part*, 697 S.E.2d 671 (S.C. Ct. App. 2010), *rev'd*, 736 S.E.2d 242 (S.C. 2012), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013); OTA REPORT, *supra* note 19, at 45–46 (indicating that electronic communications were vulnerable "when retained in the files of the electronic mail company for administrative purposes").

225. *See* 132 CONG. REC. 27,635 (statement of Sen. Mathias) (stating that the Act extends protections to certain electronic communications but exempts media that does not carry with it an expectation of privacy); *see also supra* text accompanying notes 45–53 (discussing Fourth Amendment jurisprudence).

226. *See House ECPA Hearing*, *supra* note 20, at 2 (statement of Rep. Robert Kastenmeier, Chairman, Subcomm. on Courts, Civil Liberties, & the Admin. of Justice) (stating that electronic mail messages were the "new technological equivalents of telephone calls, telegrams, and mail"); 131 CONG. REC. 24,366 (1985) (statement of Sen. Leahy) (asserting that Americans should feel just as confident in sending electronic messages as they are in putting mail in a mailbox).

227. *See* H.R. REP. NO. 99-647, at 22 & n.34 (1986) (stating that, while the service provider had access to the message in case of system failure, the service provider did not normally access the messages and analogizing a user's expectation in sending an email with that of someone sending postal mail).

228. *See* 18 U.S.C. § 2703(a) (requiring a warrant for communications in electronic storage held by an ECS for 180 days or less). Just as the U.S. Postal Service may not divulge an individual's mail, neither could an electronic mail company. *See* S. REP. NO. 99-541, at 5 (1986).

229. S. REP. NO. 113-34, at 2 (2013) ("[In 1986,] Congress believed that the most extended period of time that a service provider might store an email would be for six months.").

230. S. REP. NO. 112-258, at 4 (2012) ("At the time that Congress enacted the ECPA, Congress assumed that most Americans would periodically access their email accounts and download any emails that they wished to read, and that third-party service providers would subsequently delete any email stored on their servers.").

Moreover, the statutory text mandates that a court take into account the temporary, intermediate provision and the backup provision in determining whether an electronic communication is sought. As Chief Justice Toal noted in *Jennings*, by using the conjunction "and," Congress intended that the communications referred to in the backup provision be copies of those communications in the temporary, intermediate storage provision.[231] The *Theofel* court found that this interpretation would render the temporary, intermediate storage provision meaningless because every backup of a message in intermediate storage would be temporary.[232] However, the Ninth Circuit failed to properly analyze the legislative history of the Act.[233] Therefore, *Theofel* incorrectly rejected the government's interpretation of electronic storage.

In passing the SCA, Congress was concerned with closing a loophole created by the temporary, intermediate storage provision that left service providers' backup copies vulnerable to unauthorized access. Under the temporary, intermediate storage provision, the government could compel a service provider to provide backup copies that it generated because the backup copy itself would not accompany the transmission of the email.[234] Therefore, contrary to *Theofel*'s reasoning, properly construing "and" to encompass both provisions of the electronic storage definition does not render the temporary, intermediate provision superfluous. In fact, the opposite is true. Adopting *Theofel's* broad holding, which suggests that indefinitely stored communications fall within the electronic storage definition, renders the temporary, intermediate storage provision of the definition unnecessary.[235] Accordingly, the proper interpretation of the electronic storage definition is that it encompasses both temporary, intermediate communications incidental to transmission *and* backups of those communications created by the service provider.[236]

---

231. *See* Jennings v. Jennings, 736 S.E.2d 242, 244 (S.C. 2012), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013). In other words, the "backup" copies must be copies of the "temporary, intermediate storage" referred to in 18 U.S.C. § 2510(17)(A).

232. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2004).

233. *See id.* at 1070–71 (noting that the legislative history provided by the government had little probative value to the case at hand).

234. *See* Kerr, *supra* note 13, at 1217 n.61 (explaining that the backup provision ensures that backup copies created by service providers "of unopened e-mails are protected by the ECS rules even though they are not themselves incident to transmission").

235. Bellia, *supra* note 191, at 1422.

236. *See e.g.*, TRW Inc. v. Andrews, 534 U.S. 19, 31 (2001) (invoking the "cardinal principle of statutory construction" that a statute should be "so construed that, if it

B. Why the Jennings *Court's Conclusion Was Right*

Applying the simplified process espoused in Part III.B and the conclusion in Part IV.A. to *Jennings* indicates that Mr. Jennings's stored emails did not qualify as "backup" storage under the SCA's "electronic storage" definition. His emails had already reached their intended recipient and were stored on Yahoo!'s server indefinitely.[237] There is no indication that they were stored by or for the provider. Rather, Mr. Jennings had complete authority over whether the emails remained on the server.[238] Therefore, the *Jennings* court reached the correct conclusion. Unfortunately, the court's fragmented reasoning undermined the opinion by providing little guidance to courts attempting to apply its precedent or adopt its reasoning.

Applying the simplified analysis in Part III.B. to *Jennings* illustrates how the approach remedies many of the problems faced by courts currently interpreting the SCA. First, the information sought—Mr. Jennings's stored emails after they reached their intended recipient—should be analyzed without regard to the type of provider to determine whether the information is in electronic storage or computer storage. Because, as previously determined, Mr. Jennings's emails were not in electronic storage, they must have been in regular computer storage. Thus, his emails fell into the RCS category.[239] On the other hand, if a court had concluded that Mr. Jennings's emails were in electronic storage, they would have fallen within the ECS provisions, providing protection as long as they were stored for less than 180 days. In that case, Mr. Jennings would have had a cause of action under § 2701. However, since his emails were not in electronic storage when Ms. Broome accessed them, he could not avail himself of § 2701 protection.

Interestingly, the application of the SCA to *Jennings* under this proposed, simplified approach could remain unchanged even if

---

can be prevented, no clause, sentence, or word shall be superfluous, void or insignificant" (quoting Duncan v. Walker, 533 U.S. 167, 174 (2001))).

237. *See* Jennings v. Jennings, 736 S.E.2d 242, 248 (S.C. 2012) (Toal, C.J., concurring), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806 (2013).

238. *See id.* at 245 (majority opinion). Because Mr. Jennings had not downloaded or saved another copy of his emails in another location, the court held that he did not create a "backup" copy and was therefore in full control of whether the email remained on another server. *Id.*

239. The RCS provisions have a number of other requirements for service providers. *See supra* note 208 (discussing additional requirements for RCS providers to qualify for protection). These restrictions could make modern webmail services that employ targeted advertising fall outside the RCS provisions. *See* Robison, *supra* note 32, at 1212–23 (explaining the prerequisites an RCS must satisfy and the implications of targeted advertising on customer data protection). However, that topic is beyond the scope of this Note.

Congress enacts an amendment to the SCA. All current legislative proposals, including S. 607, which some suggest is likely to pass this legislative session,[240] fail to address § 2701 or any of the definitions that affect it.[241] In fact, Congress's approach in S. 607 may lend even more support to the conclusion that post-transmission emails do not qualify as electronic storage.

Congress's attempt to require a uniform warrant requirement by adding language to the compelled disclosure requirement, but not changing the electronic storage definition, creates a statute that uses the term electronic storage by itself in § 2701[242] and then expands the application of electronic storage to § 2703(a)'s compelled disclosure provision.[243] Invoking the well-established canons of construction that "courts should disfavor interpretations of statutes that render language superfluous"[244] and that Congress is presumed to be "aware of existing law when it passes legislation,"[245] courts will likely find that "post-transmission" electronic communications are not protected under § 2701. Finding otherwise would render the language following electronic storage in the "new" § 2703(a) meaningless, since that language specifically states that the compelled disclosure provision extends to post-transmission content.[246] Moreover, Congress affirmatively chose not to amend the electronic storage definition and declined to include language extending the scope of § 2701, despite the well-known controversy surrounding electronic storage and post-transmission emails.[247] For these reasons, it is very

240. Cannon, *supra* note 154 (quoting Representative Joe Barton as stating that S. 607 has "a really good chance" of passing).

241. *See supra* notes 176–182 and accompanying text (discussing suggested reforms of § 2701).

242. 18 U.S.C. § 2701 (2012) (delineating the offense and punishment for unlawful access only to communications in electronic storage held by an ECS provider).

243. S. 607, 113th Cong. § 3(a) (as reported by S. Comm. on the Judiciary, Apr. 25, 2013) (including electronic communications in "electronic storage with or otherwise stored, held, or maintained by" an ECS or RCS provider).

244. Conn. Nat'l Bank v. Germain, 503 U.S. 249, 253 (1992).

245. Miles v. Apex Marine Corp., 498 U.S. 19, 32 (1990).

246. *See e.g.*, United States v. Koh, 199 F.3d 632, 637 (2d Cir. 1999) (declining to adopt the appellee's interpretation of a statute because doing so would make the addition of certain language referring to specific branches and agencies superfluous if Congress had intended the statute to be limited to institutions already covered by the statute).

247. *See e.g.*, Keene Corp. v. United States, 508 U.S. 200, 208 (1993) (reasoning that a section of the statute that included a longer phrase "jurisdiction to render judgment" did not apply to a nearby section which spoke only of "jurisdiction" because courts generally assume that Congress acted intentionally "where Congress includes particular language in one section of a statute but omits it in another" (quoting Russello v. United States, 464 U.S. 16, 23 (1983))); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 621 & n.4 (5th Cir. 2013) (looking at

likely that if S. 607 is passed in its current version, individuals like Mr. Jennings would not be entitled to an action under § 2701 for unauthorized acquisition of post-transmission emails.

CONCLUSION

Congress's foresight in enacting the SCA has allowed the Act to adapt to a number of new technologies surprisingly well in the twenty-seven years since its enactment. However, many now argue that technology has outpaced the Act's structure and underlying assumptions. Currently, the success of an action under the SCA is necessarily tied to geography due to courts around the country ruling in different ways. Moreover, individuals, service providers, and the government are uncertain of their rights and responsibilities. For this reason, a clear and consistent framework is necessary. An amendment that updates the SCA by creating a technologically neutral statute that simplifies the current structure of the SCA, and its basis on archaic technology, is critical to ensure the continued progress of technology.

However, until Congress updates the SCA, courts must effectuate Congress's intent by categorizing modern technology within the language of the current statute. Courts must carefully avoid injecting their own language. By focusing on the function of ISPs with regard to the particular communication in question, a simple framework emerges that allows courts to apply the SCA to modern technologies and addresses the concerns that prompted Congress to adopt the SCA. Only then can courts be sure that Congress's intent is properly carried out.

---

the language of a related section of a statute that provided for mandatory issuance of surveillance orders to determine whether the other part of the statute that contained different language mandated an order).