# Taking Back "Electronic Storage": South Carolina's *Jennings* and Why the Stored Communications Act Should (and Does) Protect Opened Emails*

## INTRODUCTION

Despite such warnings as the recent buzz surrounding Google's policy of scanning email messages for verbal cues in order to target advertising,[1] Americans have increasingly come to rely on email and other online communication as a replacement for traditional mail.[2] And as with traditional mail, users tend to regard such correspondence as private.[3] Even General David Petraeus, former director of the United States Central Intelligence Agency, made the mistake of assuming that the contents of his Gmail account would be safe from prying eyes.[4] Many users accept, as the price of "free" online services, that information sent or stored can potentially be accessed by the providers of the online services.[5] Most users,

* © 2014 Rebecca A. Fiss.

1. *See, e.g.*, Jason Kincaid, *Gmail to Roll Out Ads That Learn from Your Inbox*, TECHCRUNCH (Mar. 29, 2011), http://techcrunch.com/2011/03/29/gmail-to-roll-out-ads-that-learn-from-your-inbox/.

2. *See* Brigid Schulte, *So Long, Snail Shells*, WASH. POST (July 25, 2009), http://www.washingtonpost.com/wp-dyn/content/story/2009/07/24/ST2009072403875.html?sid=ST2009072403875 (noting that "first-class mail is . . . migrating to the web").

3. This is evidenced by law firms' willingness to send "confidential" client messages via email and the general public's use of personal accounts to exchange private messages, pictures, and files. This is so despite numerous recent cautions to the contrary. *See, e.g.*, Nicole Perlroth, *Trying to Keep Your E-Mails Secret When the C.I.A. Chief Couldn't*, N.Y. TIMES (Nov. 16, 2012), http://www.nytimes.com/2012/11/17/technology/trying-to-keep-your-e-mails-secret-when-the-cia-chief-couldnt.html (" 'The reality is if you don't want something to show up on the front page of *The New York Times*, then don't say it [in your email account].' "); *Email Privacy Concerns*, FINDLAW, http://consumer.findlaw.com/online-scams/email-privacy-concerns.html (last visited Jan. 22, 2013) ("This should come as no surprise anymore, but your email isn't private.").

4. *See* Perlroth, *supra* note 3. General Petraeus and his paramour attempted to remain secret by limiting their online communications to a shared Gmail account, in which they saved messages to the draft folder rather than sending them, presumably hoping to avoid creating a digital trail. *See id.*

5. In fact, in a June 2013 motion to dismiss a class action suit regarding its privacy policy, Google argued that all users of email impliedly consent to the automated processing of their communications by their email service. *See* Defendant Google Inc.'s Motion to Dismiss Plaintiffs' Consol. Individual & Class Action Complaint at 13–14, *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK (N.D. Cal. June 13, 2013), *available at* http://www.consumerwatchdog.org/resources/googlemotion061313.pdf.

however, would probably assume that legal redress would be available if a third party hacked into their email account, made duplicates of private messages, and shared those messages with others. However, as a ruling by the South Carolina Supreme Court recently suggested, such relief may not be available in some jurisdictions.

In *Jennings v. Jennings*,[6] the plaintiff's soon-to-be-ex-wife illicitly accessed email messages that the plaintiff had read and left in his email account. The plaintiff responded by suing his wife and her accomplices under the federal Stored Communications Act ("SCA").[7] Unbeknownst to the plaintiff, the case would go all the way up to the South Carolina Supreme Court, where it would highlight the now-obvious shortcomings of the SCA.

Part I of this Recent Development provides a backdrop for analyzing *Jennings*, including a brief history of the SCA and an introduction to the interpretative challenges that have plagued courts attempting to apply this statute to modern technology. Part II explores the Ninth Circuit's seminal *Theofel v. Farey-Jones*[8] decision and *Jennings*, including the South Carolina Supreme Court's plurality opinion and the two opinions concurring in the result. Part III evaluates the *Jennings* court's principal holding that email messages that a user has already accessed and left on the internet service provider's ("ISP") system do not qualify as "electronic storage" as required for protection under the Stored Communications Act. This Recent Development argues that such an interpretation of the SCA's various ambiguities is contrary to both the Act's explicit legislative purpose and users' understandings of their private communications. Part IV joins the chorus of voices calling for Congress to amend the SCA and provides suggestions for doing so. Above all, it encourages Congress to discard the term "electronic storage" by replacing it with language that tracks the function, rather than the mechanisms, of private online communication, and suggests a relocation of the SCA provisions prohibiting certain conduct by private parties.

6. 736 S.E.2d 242 (S.C. 2012), *cert. denied*, 133 S. Ct. 1806 (2013).

7. The Stored Communications Act was enacted as Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in 18 U.S.C. §§ 2701–2712 (2012)).

8. 359 F.3d 1066 (9th Cir. 2004).

## I. BACKGROUND: THE HISTORY AND INTERPRETATIVE DIFFICULTIES OF THE STORED COMMUNICATIONS ACT

Congress passed the Stored Communications Act in 1986, a time when the Internet was in its infancy.[9] The mid-1980s marked a period of growth in business use of online resources. Although few individuals had Internet access at the time, new companies were entering the electronic mail market and the industry was expected to nearly triple in size within just a few years.[10] Businesses began to outsource data processing and storage to "remote computing services."[11] Concerns about privacy were high, especially since it appeared that information shared with third parties as it made its way through various routers would be unprotected by the Fourth Amendment.[12]

In response to these concerns, Congress passed the Stored Communications Act.[13] The law's primary purpose was to provide Fourth Amendment-like privacy protections to electronic communications.[14] The SCA limits voluntary disclosure by internet service providers of messages in "electronic storage"[15] and regulates the government's ability to compel those providers to turn over messages that are in "electronic storage."[16] The Act also prohibits any unauthorized government or private actor from intentionally accessing "a facility through which an electronic communication service is provided . . . and thereby obtain[], alter[], or prevent[]

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

10. *See id.* at 1557, 1559.

11. *Id.* at 1560.

12. *See* Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209–10 (2004); Mulligan, *supra* note 9, at 1562–63. A series of Supreme Court cases, known as the "business records cases," had found that personal information voluntarily disclosed to a business was no longer within the scope of Fourth Amendment protection, stirring concerns that electronic mail and other remotely stored information would meet the same fate. Mulligan, *supra* note 9, at 1562 (citing Smith v. Maryland, 442 U.S. 735, 744 (1979) (finding no protection for records conveyed to phone company); United States v. Miller, 425 U.S. 435, 442 (1976) (finding no protection for business records conveyed to bank); Couch v. United States, 409 U.S. 322, 335–36 (1972) (finding no protection for tax records conveyed to accountant)).

13. *See* Kerr, *supra* note 12, at 1208 & n.1.

14. *See* S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 ("Most importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment."); *see also* Kerr, *supra* note 12, at 1212 (discussing the primary purpose of the law).

15. *See* 18 U.S.C. § 2702 (2012).

16. *See id.* § 2703.

authorized access to a wire or electronic communication while it is in electronic storage in such system."[17] The reach of each of these provisions—and thus the privacy of online correspondence—depends on the meaning of "electronic storage," which the Act defines as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[18]

While the SCA may have been appropriate for the forms of digital communication that existed in 1986, the law preceded the emergence of the World Wide Web,[19] and its age is often evident as courts struggle to apply it—and particularly its definition of "electronic storage"—to modern technology.[20] Due to a combination of both technical variations between different types of electronic communications and disagreements over statutory interpretation, the application of the SCA to email messages can fluctuate depending on the court in which the litigation arises[21] and whether the email account is web-based (as with Yahoo! or Gmail) or software-based (as with Microsoft Outlook).[22]

Much of the debate among lower court decisions regarding "electronic storage" centers around two issues. First, courts have disagreed about the relationship between the two prongs of the Act's "electronic storage" definition. Some courts, following the Department of Justice's interpretation, have held that subsection (B) encompasses "backup protection" of only those communications that are themselves in "temporary, intermediate storage" under

17. *Id.* § 2701.

18. *Id.* § 2510(17).

19. *See* Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. TIMES (Jan. 9, 2011), http://www.nytimes.com/2011/01/10/technology/10privacy.html ?pagewanted=all&_r=0; *cf.* Petition for a Writ of Certiorari at 2, Garcia v. City of Laredo, Tex., 133 S. Ct. 2859 (2013) (No. 12-1264), 2013 WL 1751478, at *2 ("As quaint as it sounds, back then Congress contemplated that an e-mail provider might actually print an email to deliver it via the post office."); Kerr, *supra* note 12, at 1214 (noting that the SCA's distinction between "electronic communication service" providers and "remote computing service" providers "freez[es] into the law the understandings of computer network use as of 1986").

20. *See infra* Part III.

21. *Cf.* Kerr, *supra* note 12, at 1240 (arguing that "several of the major judicial interpretations of the SCA" misinterpret the Act).

22. *See, e.g.*, United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (arguing that "[t]he distinction between web-based email and other email systems makes *Theofel* largely inapplicable here").

subsection (A).[23] Under this view, " 'electronic storage' refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity."[24] Thus, unread email messages would be covered, but an already-read message would not, since messages in "post-transmission storage"[25] are no longer "incidental to . . . electronic transmission," nor are they backups of such intermediate communications.[26] Most other courts, by contrast, treat the definition's two prongs as creating two entirely independent categories: communications that are *either* in "temporary, intermediate storage" *or* stored "for purposes of backup protection" qualify as "in electronic storage" and thus are protected under the SCA.[27] Proponents of this approach disagree on whether already-read emails receive protection.[28]

Second, some courts have struggled with the meaning of "backup protection," which Congress neglected to define but is one of the key components of the SCA's definition of "electronic storage."[29] Specifically, courts and critics interpreting the SCA have disagreed over whether such "backup protection" must be created by the ISP

23. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) ("The phrase 'for purposes of backup protection of such communication' in the statutory definition makes clear that messages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of 'electronic storage.' "), *aff'd in part and vacated in part*, 352 F.3d 107 (3d Cir. 2003).

24. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 123 (3d ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

25. *Id.*

26. 18 U.S.C. § 2510(17) (2012).

27. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); Cornerstone Consultants, Inc. v. Prod. Input Solutions, LLC, 789 F. Supp. 2d 1029, 1055 (N.D. Iowa 2011); Crispin v. Christian Audigier, Inc., 717 F. Supp. 965, 983 (C.D. Cal. 2010), *summary judgment granted in part and denied in part*, 839 F. Supp. 2d 1086 (2011); Flagg v. City of Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008).

28. For example, the Ninth Circuit in *Theofel* adopted this position and held that already-read emails are protected. *See Theofel*, 359 F.3d at 1069–70. On the other hand, the majority of the South Carolina Supreme Court (namely Justices Hearn and Pleicones and those who joined their opinions) also adopted the either-or position and yet agreed that already-read emails are not "in electronic storage." *See generally* Jennings v. Jennings, 736 S.E.2d 242 (S.C. 2012)(holding that the plaintiff's emails were not "in electronic storage" under the SCA when the defendant accessed them, but disagreeing on a rationale), *cert. denied*, 133 S. Ct. 1806 (2013).

29. *See* § 2510(17)(B); *see also* 1 JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE § 4:76 (2d ed. Supp. 2013) (providing an overview of courts' concerns and decisions when addressing electronic communications and backup processes).

for its own purposes[30]—for example, backups of the ISP's servers in case of a server crash[31]—or whether it must be created by the ISP for the user's purposes.[32] In the *Jennings* case discussed below, one justice even settled on a third interpretation, concluding that another copy must have been created *by the user* in order for the SCA's definition to apply.[33]

Because courts' conclusions regarding the aforementioned sub-issues are not necessarily predictive of their final decisions on what constitutes "electronic storage," case law in this area remains somewhat erratic.[34] Though few courts have had occasion to wrestle with the definition as it applies to email, the federal district courts that have addressed the question have varied between including only unretrieved messages in the definition,[35] including both unread messages and messages which have been retrieved and left on the provider's system,[36] and leaving the question open to either possibility.[37]

The scope of "electronic storage" and the extent of the SCA protections afforded to email messages have also come under the microscope in at least two important appellate cases during the last decade. The first of those was *Theofel v. Farey-Jones*, decided by the Ninth Circuit in 2004.[38] In that case, the court concluded that any

30. A majority of the justices on the *Jennings* court (Chief Justice Toal, Justice Pleicones, and those who join them) seems to agree on this position. *See generally Jennings*, 736 S.E.2d 242 (addressing the roles of service providers and backup protection); *see also, e.g.*, Kerr, *supra* note 12, at 1217 n.61 ("[T]he most obvious statutory signal is the text of 18 U.S.C. § 2704, entitled 'Backup Preservation.' Section 2704 makes clear that the SCA uses the phrase 'backup copy' in a very technical way to mean a copy made by the service provider for administrative purposes." (citation omitted)).

31. *See* Kerr, *supra* note 12, at 1217 n.61.

32. *See, e.g.*, *Theofel*, 359 F.3d at 1075.

33. *See Jennings*, 736 S.E.2d at 245 (Hearn, J., plurality opinion). Justice Hearn suggested that the plaintiff must have downloaded the messages or saved a copy of them in a second location in order for there to have been a backup copy. *See id.*

34. For recommendations on how these issues should be resolved, see *infra* Part III.

35. *See, e.g.*, United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part and vacated in part*, 352 F.3d 107 (3d Cir. 2003).

36. *See, e.g.*, Shefts v. Petrakis, No. 10–cv–1104, 2011 WL 5930469, at *6 (C.D. Ill. Nov. 29, 2011); Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) ("The fact that Plaintiff may have already read the emails and messages copied by Defendant does not take them out of the purview of the Stored Communications Act. The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service.").

37. *See, e.g.*, Rene v. G.F. Fishers, Inc., 817 F. Supp. 2d 1090, 1096 (S.D. Ind. 2011) (declining to decide whether unopened emails are in "electronic storage").

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

email, whether read or unread, qualified as being "in electronic storage" and thus was protected under the SCA.[39] Eight years later, in October 2012, the South Carolina Supreme Court reviewed the same question. Despite being unable to agree on a rationale for its decision—the court issued three separate opinions, with none of them winning a majority—the court held unanimously that emails already viewed by the plaintiff before the defendant accessed them did *not* fall under the definition of "electronic storage" and that the plaintiff thus had no claim against the defendant.[40] This holding created a "clear split" with the Ninth Circuit's *Theofel* holding.[41]

Because of the frequent recurrence of the term "electronic storage" in key provisions of the SCA, the determination of the term's scope is of utmost importance in determining the reach of the Act. Given the large amount of confusion courts face in attempting technical applications of the definition of "electronic storage"—especially now, in light of the clear split between the Ninth Circuit and the South Carolina Supreme Court—legislative action is necessary to the continued utility of the SCA.[42] This Recent Development urges Congress to take substantial steps to clarify the language of the SCA and thus help courts avoid "absurd results" that are not "consistent with the legislative purpose."[43]

39. *See id.* at 1071 ("[W]e think that prior access is irrelevant to whether the messages at issue were in electronic storage.").

40. *See generally* Jennings v. Jennings, 736 S.E.2d 242 (S.C. 2012) (featuring three concurring opinions, all arriving at the same conclusion but relying on conflicting rationales), *cert. denied*, 133 S. Ct. 1806 (2013).

41. 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/.

42. *Cf id.* (urging review by the Supreme Court). The confusion is made even more intense by the fact that providers often have customers all over the country and that it is still unclear whether the legal standard should be based on the location of the litigation or the location of the ISP. Thus, "any disagreement among lower courts causes major headaches," as providers are unsure which rule will apply. *Id.* Furthermore, the fact that large proportions of the messages in users' email accounts have been read and then left there for safekeeping (and that oftentimes these messages are so stored because the subscriber considers them important) makes this issue a critical one to internet users. However, the Supreme Court declined to hear this case, and so the onus is on Congress to provide clarification.

43. Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 575 (1982).

## II. *THEOFEL* AND *JENNINGS*: THE DISAGREEMENT BETWEEN THE NINTH CIRCUIT AND SOUTH CAROLINA

### *A. Theofel v. Farey-Jones*

The Ninth Circuit's *Theofel v. Farey-Jones* was the first major case to explore SCA coverage of already-read email messages.[44] Farey-Jones, as defendant in another lawsuit, had issued a far-too-broad subpoena to the plaintiff's ISP, ordering " '[a]ll copies of e-mails sent or received by anyone' " in the plaintiff corporation regardless of whether the messages were related to the litigation.[45] In response, the ISP posted a "sample" of the emails online, where Farey-Jones read them.[46] Several employees of the plaintiff company whose emails were included in the excessive sample filed a separate lawsuit against Farey-Jones, alleging that Farey-Jones had violated section 2701 of the SCA by causing the ISP to access the plaintiffs' company's server without authorization.[47]

The main question before the Ninth Circuit—the only federal appeals court to confront the issue so far—was whether the emails, many of which had already been accessed by their recipients, fell under the statutory definition of "electronic storage."[48] The court rejected the government's "traditional"[49] interpretation of the relationship between the two prongs of the definition of "electronic storage" in favor of an interpretation that treated the subsections as creating two distinct categories of protected communications.[50] It contended both that the government misread the plain language of the definition[51] and that such an understanding would "drain[] subsection (B) of independent content," since "virtually any backup of a subsection (A) message will itself qualify as a message in

44. *See Theofel*, 359 F.3d 1066.

45. *Id.* at 1071 (alteration in original).

46. *Id.*

47. *Id.* at 1072.

48. *Id.* at 1075.

49. The "traditional" interpretation is the name given by Orin Kerr to the understanding of the "electronic storage" definition that the Department of Justice has historically advocated. *See* Kerr, *supra* note 12, at 1208–09.

50. *Theofel*, 359 F.3d at 1069.

51. *See id.* ("The phrase 'such communication' in subsection (B) does not, as a matter of grammar, reference attributes of the type of storage defined in subsection (A). The government's argument would be correct if subsection (B) referred to 'a communication in such storage,' or if subsection (A) referred to a communication in temporary, intermediate storage rather than temporary, intermediate storage of a communication. However, as the statute is written, 'such communication' is nothing more than shorthand for 'a wire or electronic communication.' ").

temporary, intermediate storage."[52] Next, after noting that "nothing in the Act requires that the backup protection be for the benefit of the ISP," the Ninth Circuit interpreted the "backup" language of subsection (B) as referring to backup copies created for the user's purposes in case the user needed to download the message again.[53] It then concluded that an already-read email can qualify as a backup copy under the statutory definition of "electronic storage," and thus held that whether or not an email message had been accessed by the user is immaterial to its coverage under the SCA.[54]

### *B. Jennings v. Jennings*

In *Jennings*, the plaintiff's wife, Gail Jennings, suspected that her husband was engaged in an extramarital affair and confronted him about it.[55] Jennings confessed that he had fallen in love with another woman and that he had been in contact with her via email for some time.[56] Gail approached her daughter-in-law, Holly Broome, who had previously worked for Jennings and knew that he had a personal Yahoo! email account.[57] After guessing the answers to his security questions, Broome was able to access Jennings's account and read the emails between Jennings and his mistress.[58] Broome then printed out copies, giving them to Gail, the attorney who was representing Gail in divorce proceedings against Jennings, and a private investigation firm.[59] After finding out that his email account had been compromised, Jennings filed suit against Broome, Gail, Gail's attorney, and the investigation company, alleging a violation of section 2701(a) of the SCA.[60]

52. *Id.* at 1069–70.

53. *Id.* at 1075.

54. *See id.* at 1071. Interestingly, despite the apparent bright line in *Theofel* classifying all emails (read or unread) as constituting "electronic storage," a district court in *United States v. Weaver*, 636 F. Supp. 2d 769 (C.D. Ill. 2009), relied on dicta from *Theofel* to conclude that the Ninth Circuit's holding applied only to email systems in which users downloaded messages from the ISP's server onto their computers and that email stored on the ISP's server should not be considered stored "for purposes of backup protection" under the definition of "electronic storage." *See Weaver*, 636 F. Supp. 2d at 771–73.

55. *See* Jennings v. Jennings, 736 S.E.2d 242, 243 (S.C. 2012) (Hearn, J., plurality opinion), *cert. denied*, 133 S. Ct. 1806 (2013).

56. *See id.*

57. *See id.*

58. *See id.*

59. *See* Jennings v. Jennings, 697 S.E.2d 671, 672 (S.C. Ct. App. 2010), *rev'd*, 736 S.E.2d 242 (S.C. 2012).

60. *See Jennings*, 736 S.E.2d at 243.

### 1. State Circuit Court

Following a hearing, the circuit court issued an order dismissing the plaintiff's section 2701 claim.[61] The circuit court held that Jennings had failed to allege the necessary elements for a cause of action because the emails at issue were not in "electronic storage" as required under section 2701.[62] The circuit court concluded the emails could be most accurately described "as in the personal long-term storage of the e-mail client" rather than maintained by the electronic communication service ("ECS") for backup protection as specified in the SCA.[63] Jennings filed a motion to reconsider, which the circuit court denied, and Jennings appealed.[64]

### 2. State Court of Appeals

After concluding that the only relevant defendant in the case was Broome,[65] the court of appeals focused the bulk of its analytical energy on determining whether the emails were in "electronic storage" as required under section 2701.[66] In considering the question, the court divided its analysis neatly into three smaller issues: (1) whether the emails were stored by an "electronic communication service" (pursuant to the definition of "electronic storage"); (2) whether they were being stored "for purposes of backup protection"; and (3) whether the SCA applies to "emails in a 'post-transmission' state."[67] Rather than delving into highly-nuanced distinctions of 1980s

61. *See id.*

62. *See id.*

63. Order Granting Defendants' Motion for Summary Judgment and Denying Plaintiff's Motion to Amend Complaint at 11, Jennings v. Jennings, No. 07-CP-40-1125, 2008 WL 8185934 (S.C. Com. Pl. Sept. 23, 2008).

64. *See Jennings*, 736 S.E.2d at 243.

65. The court of appeals first considered whether the circuit court had erred in dismissing Jennings's SCA claim on the basis of a supposed failure to allege the necessary elements for the cause of action. *See Jennings*, 697 S.E.2d at 674–75. The appellate court concluded that the circuit court had erred, given that it was in fact ruling on motions for summary judgment and thus should have credited Jennings's evidence that Broome had logged onto his email account without authorization and read and printed emails stored in the account. *See id.* at 675. The court of appeals also examined the denial of Jennings's suits against Gail, her attorney (whom Jennings had attempted to add to the complaint), and the private investigation firm, and determined that the circuit court had been correct in rejecting the claims. *See id.* at 680–81 ("[L]iability under the SCA extends only to those who actually engaged in a violation of that act."). The only relevant defendant, the court therefore concluded, was Broome, who had actually accessed the emails.

66. *See Jennings*, 697 S.E.2d at 675–81 (concluding that the emails which plaintiff had read and left in her inbox were in "electronic storage" and thus were protected under the SCA).

67. *Id.* at 675–79.

technology to answer these questions, the appellate court relied heavily on *Theofel*[68] and the legislative history of the SCA.[69] Like the Ninth Circuit, the South Carolina Court of Appeals reasoned that " '[a]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to [access] it again.' "[70] Thus, the ISP copy serves as a "backup" for the user, and nothing in the SCA specifies whether the "backup protection" must be for the benefit of the user or of the ISP.[71] The court noted that both the House and Senate Reports on the SCA state that section 2701 was intended to address the problem of unauthorized access to and tampering with private electronic communications.[72] The South Carolina Court of Appeals argued that, in order to effectuate such a purpose, backup protection would clearly be needed after the message had been transmitted.[73] In a unanimous opinion, the court of appeals held that Broome's infiltration of the plaintiff's email account may well have constituted a violation of section 2701[74]—a decision that comports with what a user might expect from a statute that purports to protect "stored communications."

3. State Supreme Court

By contrast, the South Carolina Supreme Court's decision was fragmented. The court issued three separate opinions that aligned only in result—that a user's emails which he has already read and left in his account are not "in electronic storage"—but could not agree on a rationale. Justice Hearn, writing for the plurality, and apparently adopting the view that "backup" storage must be created by the subscriber for his own purposes, argued that Jennings's emails were not in electronic storage since Jennings had not presented evidence that he himself had ever downloaded any other copies.[75] Relying on

68. *See, e.g.*, *id.* at 679 (quoting and adopting the Ninth Circuit's reasoning).

69. *See, e.g.*, *id.* at 676 (" '[E]lectonic mail companies are providers of electronic communication services.' " (quoting S. REP. NO. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568)); *id.* (" 'An "electronic mail" service . . . would be subject to Section 2701.' " (omission in original) (quoting H.R. REP. NO. 99-647, at 63 (1986))).

70. *Id.* at 677 (quoting Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004)).

71. *See id.* (citing Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004)).

72. *See id.* at 678 (citing H.R. REP. NO. 99-647, at 62 (1986); S. REP. NO. 99-541, at 35 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589).

73. *See id.* at 679.

74. *See id.* at 681.

75. *See* Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012) (Hearn, J., plurality opinion) ("After opening them, Jennings left the single copies of his e-mails on the Yahoo! server and apparently did not download them or save another copy of them in any

the *Merriam-Webster Dictionary*'s definition of "backup," Justice Hearn reasoned that the word presupposed the existence of another copy and emphasized that there were no such copies of the emails in question.[76]

Chief Justice Toal rejected Justice Hearn's interpretation of "backup."[77] Relying primarily on one law review article's technical analysis of the "structure of the SCA,"[78] she reasoned that whether copies were "for purposes of backup protection" under the second prong of the "electronic storage" definition should be determined from the viewpoint of the internet service provider[79]—in other words, whether the backups were created by the ISP for its own purposes. Above all, the chief justice objected to Justice Hearn's departure from the "traditional interpretation" of "electronic storage."[80] Supporting the interpretation championed by the Department of Justice,[81] Chief Justice Toal contended that Congress's choice of the conjunctive "and" to connect the two prongs of the "electronic storage" definition was no coincidence, and thus the two prongs must be read together.[82] According to a plain reading of the definition, therefore, only a message which was in "temporary, intermediate storage of a[n] . . . electronic communication incidental to . . . electronic transmission"[83] or a backup *of such a temporary copy* would be protected by the Act.[84] Under this interpretation, Jennings's emails fell outside of the statute's protection simply by virtue of already having been read by the time Broome illicitly accessed them, given that such communications are no longer in " 'temporary, intermediate storage . . . incidental to . . . electronic transmission' "[85] nor are they backups of temporary storage.

The second concurring opinion consisted of a single paragraph by Justice Pleicones. Although he largely agreed with Chief Justice Toal's opinion, Justice Pleicones interpreted the two prongs of the

other location. We decline to hold that retaining an opened email constitutes storing it for backup protection under the Act."), *cert. denied*, 133 S. Ct. 1806 (2013).

76. *See id.* ("We see no reason to deviate from the plain, everyday meaning of the word 'backup,' and conclude that as the single copy of the communication, Jennings's e-mails could not have been stored for backup protection.").

77. *See id.* at 246 (Toal, C.J., concurring in result).

78. *See id.* (quoting Kerr, *supra* note 12).

79. *See id.*

80. *See id.*

81. *See id.* at 247.

82. *See id.*

83. *Id.* (quoting 18 U.S.C. § 2510(17) (2012)).

84. *See id.*

85. *Id.* at 248 (omissions in original) (quoting 18 U.S.C. § 2510(17) (2006)).

definition of "electronic storage" as creating two distinct types of storage—one "temporary and incidental to transmission" and the other "a secondary copy created for backup purposes by the service provider."[86] Because Jennings's emails were neither in temporary storage incidental to transmission nor copies made by Jennings's internet provider for the purposes of backup, they were unprotected under the SCA.[87]

Despite its fragmentation, the court's decision created a clear split with the Ninth Circuit's *Theofel* ruling. According to the South Carolina Supreme Court, emails which a user has read and left in his account do not constitute "electronic storage" and thus are unprotected from unauthorized access by third parties under the SCA.

## III. AN EVALUATION OF THE SOUTH CAROLINA SUPREME COURT'S OPINION AND A GUIDE FOR FUTURE DECISIONS

Unlike the unanimous opinion of the state court of appeals, the opinions of the South Carolina Supreme Court find very little of their support in the statute's legislative history[88] (or even in case law[89]), relying instead on the justices' comprehension of the technology at issue and a single law review article.[90] Professor Orin Kerr, the article's author, though certainly among the nation's leading authorities on the Stored Communications Act, bases his reading of the statute on narrow, highly technical statutory interpretation and "the structure of the SCA" rather than on Congress's direct statements of the statute's purpose.[91]

86. *Id.* at 248–49 (Pleicones, J., concurring in result).

87. *See id.* at 249.

88. Altogether, the three opinions make only one direct reference to the 1986 congressional reports, and then only to support the proposition that the technology at that time was "strikingly different . . . compared to the present." *See id.* at 248 (Toal, C.J., concurring in result). All of the court's remaining dependence on legislative history and purpose seems to be through the lens of Professor Orin Kerr, discussed *infra* notes 91–92 and accompanying text.

89. Most of the justices' references to cases are either to reject other courts' approaches or support general propositions regarding statutory interpretation.

90. Chief Justice Toal cited Orin Kerr's *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, *supra* note 12, as substantial support for the main premises of his argument. *See Jennings*, 736 S.E.2d at 246 (Toal, C.J., concurring in result). Justice Pleicones, in his extremely brief opinion, cited the article in a footnote. *See id.* at 249 n.4 (Pleicones, J., concurring in result).

91. *See* Kerr, *supra* note 12, at 1208. Kerr arrives at many of his conclusions by comparing the wording of certain provisions of the SCA to the wordings and rules contained in other provisions. *See, e.g.*, *id.* at 1217 n.61 (interpreting the definition of "electronic storage" in 18 U.S.C. § 2510(17) by comparing it with 18 U.S.C. § 2704). While

However, "interpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available."[92] In this case, a strict, narrow reading of the Act is impractical, given that such disparate treatment of opened emails is in no way clearly mandated by the statutory language[93] and that the opposite approach seems to be more in keeping with congressional intent.[94] This Recent Development advocates instead that in addressing questions raised by the Act's various ambiguities, courts base their answers on both the SCA's recorded purposes and users' understandings of their private communications.

### *A. The Elusive Definition of "Electronic Storage"*

It is difficult to delineate the outer bounds of an act protecting electronically "stored communications" without first determining the meaning of "electronic storage." As each of the concurring justices of the South Carolina Supreme Court pointed out in their opinions, there is a longstanding debate about the relationship between the two prongs of the SCA's definition of "electronic storage."[95] According to the traditional interpretation advocated by the United States Department of Justice,[96] subsection (B) of the definition applies only to backup copies of communications that are themselves in temporary, intermediate storage pursuant to subsection (A),[97] the result being that an email message that a user has already accessed would no longer qualify.[98] Meanwhile, the opposing interpretation—

Kerr's attention to detail is impressive, he loses sight of the bigger picture of Congress's purpose in creating the SCA.

92. Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 575 (1982). Chief Justice Toal cited this language in support of her own position. *See Jennings*, 736 S.E.2d at 247 (Toal, C.J., concurring in result). This is rather ironic, however, given that neither Toal nor any of the other South Carolina justices supported their opinions with direct sources documenting the statute's purpose, relying instead on Professor Kerr's interpretation of them.

93. Professor Kerr admitted as much. *See* Kerr, *supra* note 12, at 1216 ("In particular, the proper treatment of opened e-mail is currently unclear."); *see also id.* at 1208 ("[T]he statute is dense and confusing . . . .").

94. *See infra* notes 105–06, 133–34 and accompanying text.

95. *See Jennings*, 736 S.E.2d at 244 (Hearn, J., plurality opinion); *id.* at 247–48 (Toal, C.J., concurring in result); *id.* at 248–49 (Pleicones, J., concurring in result).

96. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, *supra* note 24, at 123.

97. This is the approach supported by Professor Kerr. *See* Kerr, *supra* note 12, at 1214.

98. *See* 1 CARR & BELLIA, *supra* note 29, § 4:76. By contrast, an email that has been received but not yet accessed by the recipient is considered to be in "electronic storage."

the one adopted by a majority of courts that have considered the question—holds that a communication can receive protection if it falls under either subsection of the definition considered as a separate category.[99] Supporters of each interpretation defend their position through long-winded grammatical scrutiny[100] and accusations that the opposing view renders one or the other prong obsolete.[101]

Rather than continuing the squabble over grammatical nuances or adding to the speculation over the effect that each approach would

*See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, *supra* note 24, at 123.

99. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) (impliedly accepting this interpretation and finding no violation of the SCA through a different analytical path); Shefts v. Petrakis, No. 10-cv-1104, 2011 WL 5930469, at *5 (C.D. Ill. Nov. 29, 2011); Cornerstone Consultants, Inc. v. Prod. Input Solutions, LLC, 789 F. Supp. 2d 1029, 1055 (N.D. Iowa 2011); Strategic Wealth Grp., LLC v. Canno, No. 10-0321, 2011 WL 346592, at *3–4 (E.D. Pa. Feb. 4, 2011) (adopting the Ninth Circuit's position in *Theofel* regarding the distinct protections under subsections (A) and (B)); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 983 (C.D. Cal. 2010); United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009); Flagg v. City of Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008). Citing House Reports, another scholar took as a given that "Congress intended for the privacy protections established by the SCA to apply to two categories of communications: 'those associated with transmission and incident thereto' and those of a 'back-up variety.' " Jason Isaac Miller, Note, *"Don't Be Evil": Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-mail Privacy Rights*, 33 HOFSTRA L. REV. 1607, 1618 (2005) (quoting H.R. REP. NO. 99-647, at 68 (1986)).

100. *See, e.g.*, *Theofel*, 359 F.3d at 1069. The court explained:

> Subsection (A) identifies a type of communication ("a wire or electronic communication") and a type of storage ("temporary, intermediate storage . . . incidental to the electronic transmission thereof"). The phrase "such communication" in subsection (B) does not, as a matter of grammar, reference attributes of the type of storage defined in subsection (A). The government's argument would be correct if subsection (B) referred to "a communication in such storage," or if subsection (A) referred to a communication in temporary, intermediate storage rather than temporary, intermediate storage of a communication. However, as the statute is written, "such communication" is nothing more than shorthand for "a wire or electronic communication."

*Id.*

101. According to the Ninth Circuit in *Theofel*, the traditional interpretation "drains subsection (B) of independent content because virtually any backup of a subsection (A) message will itself qualify as a message in temporary, intermediate storage," and, moreover, "the lifespan of a backup is necessarily tied to that of the underlying message. Where the underlying message has expired in the normal course, any copy is no longer performing any backup function." *Id.* at 1069–70. On the other hand, Chief Justice Toal argued that "Justice Hearn's approach would delete a word [('and')] and insert a new one [('or')] into the statutory text, effectively writing out subsection A from the definition of electronic storage." Jennings v. Jennings, 736 S.E.2d 242, 247 (S.C. 2012) (Toal, C.J., concurring in result), *cert. denied*, 133 S. Ct. 1806 (2013). Chief Justice Toal did not elaborate on how this would occur. *See id.*

have on the layout of the legislature's definition, a more constructive approach would be to decide the issue based on what would best advance the statute's purposes. Assuming that the traditional interpretive approach would in fact place opened emails outside the scope of the SCA's protection,[102] then the relevant inquiry is whether Congress intended this result.[103] In fact, the legislative history of the SCA seems to precisely address the situation.[104] The Senate Report explains broadly that

> a computer mail facility authorizes a subscriber to access information in their portion of the facilities [sic] storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of this provision.[105]

The language makes no qualification that would seem to draw a line between particular types of stored messages. Moreover, there are other indications that the legislature intended to cover both read and unread email messages under the SCA. As the court of appeals in *Jennings* pointed out:

> both the House and Senate Reports state that section 2701 "addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic . . . communications that are not intended to be available to the public."[106]

The reports do not distinguish between read and unread communications, nor is any such distinction inherent in the

102. The Department of Justice believes that it would. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, *supra* note 24, at 124. This distinction could itself be complicated by modern email clients' option to allow users to mark their opened message as "unread."

103. Of course, looking to the legislative history is appropriate even if the plain language of the statute were to lend itself clearly to one interpretation or the other. *See* United States v. Am. Trucking Ass'ns, 310 U.S. 534, 543–44 (1940) ("When aid to the construction of the meaning of the words, as used in the statute, is available, there certainly can be no 'rule of law' which forbids its use, however clear the words may appear on 'superficial examination.' ").

104. In a case with facts similar to those in *Jennings*, the district court argued that "the legislative history shows that Congress intended the Stored Communications Act to cover the exact situation in this case." Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 925–26 (W.D. Wis. 2002). In the *Fischer* case, the defendant hired a computer expert to access plaintiff's Hotmail account using a password that the defendant had guessed. *See id.* at 920. The defendant and expert then read and printed emails they found in plaintiff's inbox. *See id.*

105. S. REP. NO. 99-541, at 36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3590.

106. Jennings v. Jennings, 697 S.E.2d 671, 678 (S.C. Ct. App. 2010) (citing H.R. REP. NO. 99-647, at 62 (1986); S. REP. NO. 99-541, at 35).

rationale—messages that a user has read and left in his account for safekeeping are no less private and no less vulnerable to intrusion than unread messages.

By contrast, those who contend that messages are no longer protected once they have been accessed find weak support in legislative history. In *Theofel*, the government focused on a line from a 1986 report indicating that messages stored by a remote computing service ("RCS") (as distinguished from an electronic communications service) "would 'continue to be covered by section 2702(a)(2)' if left on the server after user access."[107] The government's argument was apparently that if an email is covered by RCS provisions after it is read, it is impliedly no longer covered by the more protective ECS provisions.[108] The Ninth Circuit, however, found the statement to support its position rather than weaken it:

> If section 2702(a)(2) applies to e-mail even before access, the committee could not have been identifying an exclusive source of protection, since even the government concedes that unopened e-mail is protected by the electronic storage provisions.[109]

Furthermore, the discussion in the report dealt entirely with provisions regarding remote computing services and did not purport to address whether ECS provisions also applied.[110] Indeed, the snippets of legislative history relied upon by the government in *Theofel*[111] and the South Carolina justices in *Jennings*[112] are only tangentially related to the issue at hand; by contrast, the legislative history cited in support of the nontraditional view seems to address the situation precisely.[113]

The proposition that the SCA was meant to emulate Fourth Amendment protections for stored communications[114] also supports a reading of the definition of "electronic storage" that would provide protection for both read and unread messages. Despite an email message's complex commute between routers to reach its

107. Theofel v. Farey-Jones, 359 F.3d 1066, 1070 (9th Cir. 2004) (quoting H.R. REP. NO. 99-647, at 65 (1986)).
108. *See id.*
109. *Id.*
110. *See id.*
111. *See id.* at 1070–71.
112. *See supra* note 88 and accompanying text.
113. *See supra* notes 105–06 and accompanying text.
114. Kerr, *supra* note 12, at 1212.

destination,[115] from a user's perspective, an email serves the same function as a physical letter sent by first-class mail.[116] Such a traditional letter would receive just as much Fourth Amendment protection once opened, read, and left on the recipient's desk[117] as it did in transit.[118] Although section 2701 proscribes actions by nongovernmental third parties and thus does not overtly address a situation in which the Fourth Amendment would be applicable,[119] the same definition of "electronic storage" applies throughout the Act so that protection of opened emails would operate against invasion by both governmental actors and private parties.[120]

Thus, the question of how the two subsections of the definition of "electronic storage" interact should not be decided solely by reference to the rules of grammar or the supposed effect that each approach will have in rendering one or the other prong superfluous, given that neither of those factors clearly favors one interpretation. Instead, the issue should be decided based on congressional intent, which appears not to discriminate between read and unread messages in affording protection.[121] If only one interpretation—the so-called nontraditional interpretation—permits protection for messages that the user has already accessed, then this is the interpretation that should be followed. Indeed, the approach which would extend protection to communications *either* in "temporary, intermediate storage . . . incidental to . . . electronic transmission" *or* stored "for purposes of backup protection"[122] is the interpretation adopted by a majority of lower courts.[123] Accordingly, judicial decisions adopting this interpretation would be most in accord with the legislative history of the SCA.

115. *See* Mulligan, *supra* note 9, at 1562–63.

116. *See* Schulte, *supra* note 2.

117. *See* U.S. CONST. amend. IV (guaranteeing "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

118. *See* United States v. Van Leeuwen, 397 U.S. 249, 253 (1970) (noting that there is a "significant Fourth Amendment interest . . . in the privacy of . . . first-class mail").

119. The Fourth Amendment only applies to actions by government agencies. *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

120. *See, e.g.*, 18 U.S.C. § 2703 (2012) (limiting the government's ability to compel providers to disclose information "in electronic storage").

121. *Cf.* Wirtz v. Bottle Blowers Ass'n, 389 U.S. 463, 468 (1968) ("[P]roper construction frequently requires consideration of [a statute's] wording against the background of its legislative history and in the light of the general objectives Congress sought to achieve."); United States v. Universal C.I.T. Credit Corp., 344 U.S. 218, 222 (1952) (consideration of the "specific history of the legislative process that culminated in the [statute] affords . . . solid ground for giving it appropriate meaning").

122. § 2510(17).

123. *See supra* note 99.

### *B. The Debated Meaning of "Backup Protection"*

Courts have also disagreed over what constitutes storage "for purposes of backup protection."[124] The debate centers around whether the backup must be created by the ISP for its own purposes[125] or whether the backup must be for the user's purposes.[126] Chief Justice Toal and Justice Pleicones took the former view,[127] whereas the Ninth Circuit expressed its allegiance to the latter.[128]

Unlike the debate between the two interpretations of the "(A) and (B)" relationship, whether the storage "by an [ECS] for purposes of backup protection" is created for the ISP's own purposes or for the user's purposes is immaterial on a practical level. Internet service providers like Gmail, Yahoo!, and Hotmail are just that—service providers—whose popularity among consumers is largely dependent on those consumers' faith in the ISPs to protect and maintain the information entrusted to them.[129] In other words, since an ISP's practice of creating backups to protect users' information is

124. This discussion assumes that the court has adopted the "non-traditional" view of the relationship between subsections (A) and (B) discussed *supra* Part II.A. Otherwise, only messages in temporary storage incidental to transmission and backups of those transient messages would be covered, which appears to be contrary to congressional intent.

125. Jennings v. Jennings, 736 S.E.2d 242, 248–49 (S.C. 2012) (Pleicones, J., concurring in result), *cert. denied*, 133 S. Ct. 1806 (2013).

126. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004). Justice Hearn seems to suggest another alternative, whereby the user needs to have downloaded or saved a copy of the messages in another location in order for the messages left on the server to qualify as "backup protection." *See Jennings*, 736 S.E.2d at 245 (Hearn, J., plurality opinion); § 2510(17)(B). However, it is difficult to read the phrase "storage of such communication by an electronic communication service for purposes of backup protection" to require the user to affirmatively download a copy of each email, so that the ISP's copy spontaneously becomes "backup protection," in order for that message to receive protection under the SCA. § 2510(17)(B). Even Professor Kerr (with whom this Recent Development often respectfully disagrees) commented that he "[did not] know why e-mail on the server couldn't be a backup of that copy even if the user's perspective controls." *See* Kerr, *supra* note 41.

127. *See Jennings*, 736 S.E.2d at 247–48 (Toal, C.J., concurring in result); *id.* at 249 (Pleicones, J., concurring in result).

128. *See Theofel*, 359 F.3d at 1075 ("An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again . . . . The ISP copy of the message functions as a 'backup' for the user.").

129. *See* Don Miller, Comment to *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/.

inherently for the benefit of the user, the ISP's purposes and the user's purposes are more or less equivalent.

Attempts to protect only certain copies of a message according to whose interest it was created to serve or whether the copy is itself a "backup" are bound to create confusion and lead to arbitrary distinctions. First, where an ISP maintains multiple, identical copies of its servers and data[130] and a user accesses his email directly on the ISP's server (as is the case for many popular web email clients today), it can be difficult to determine precisely which copies of an email are backup copies and which are originals. Deeming some of these copies to be protected from tampering under the SCA and others not could only be done on arbitrary grounds. Second, the language of section 2701, which prohibits unauthorized access to an "electronic communication while it is in electronic storage in such system,"[131] does not specify that the violator must access a copy that itself serves as backup protection; under the language of section 2701, it is sufficient that the accessed message is being stored somewhere on the ISP's server for backup protection.[132] Just as it would be arbitrary to discriminate between identical copies of the same communications, it would be especially nonsensical to allow a plaintiff to sue where the intruder accessed one "backup" replica of a server but not where the intruder accessed the copy in the user's email account.

Likewise, there is little evidence that Congress intended to make such distinctions. The portions of the congressional reports that clarify the Act's purpose of "address[ing] the growing problem of unauthorized persons deliberately gaining access to . . . communications that are not intended to be available to the public" do not create categories of backup protection according to whose

130. *See* Kerr, *supra* note 12, at 1217 n.61. ISPs may use multiple mechanisms to reliably provide service to their users and to ensure that data integrity is maintained in the event of a server crash or other technical problem. For example, they may use server mirroring, clustering, and redundant disk drive systems, among other methods. *See Server Mirroring*, TECHOPEDIA, http://www.techopedia.com/definition/1156/server-mirroring (last accessed Dec. 28, 2013) (defining "server mirroring" as "a process in network management through which an exact replica of a server is continuously created on run time"); *Computer Cluster*, TECHOPEDIA, http://www.techopedia.com/definition/6581/computer-cluster (last accessed Dec. 28, 2013) (defining "computer cluster" as a single unit of multiple, linked computers that act as a single, more powerful machine); *Redundant Array of Independent Disks (RAID)*, TECHOPEDIA, http://www.techopedia.com/definition/24492/redundant-array-of-independent-disks--raid (last accessed Dec. 28, 2013) (defining RAID as "a method of storing duplicate data on two or more hard drives").

131. § 2701.

132. *See id.*

purposes it serves.[133] It would appear that, rather than creating an additional arbitrary element that the plaintiff must prove in order to receive protection, the backup provision exists so that those wishing to gain access to private messages "cannot make an end-run around the privacy-protecting ECS rules" by attempting to access the ISP's backup copies.[134]

The opinions of the justices of the South Carolina Supreme Court, though they vary widely, share a common thread: each of them gets enmeshed in a technical reading of the statutory language—an approach that will only become more complicated and fruitless as technology evolves further away from what it was in 1986—while paying little attention to the direct evidence of what Congress actually intended. Such a garbled approach cannot stand.

## IV. THE NEED FOR SUBSTANTIAL CHANGES IN THE SCA TO KEEP UP WITH MODERN TECHNOLOGY

While the state of SCA jurisprudence would have been well served by a Supreme Court decision aligning adjudication with congressional purpose,[135] an even better solution—and one that is still available to Congress—would be a legislative overhaul of the language of the SCA. Competing interests between consumers and law enforcement agencies create a "tug of war between security concerns and the need to protect privacy,"[136] and Congress is traditionally considered the umpire for such policy decisions.[137] Indeed, the national outcry for amendment is growing,[138] and Professor Kerr suggested his own substantial revisions in 2004.[139] In order to achieve the SCA's purpose of "address[ing] the growing

133. H.R. REP. NO. 99-647, at 62 (1986); S. REP. NO. 99-541, at 35 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589.

134. Kerr, *supra* note 12, at 1217 n.61.

135. The Supreme Court has already denied certiorari. Jennings v. Broome, 133 S. Ct. 1806 (2013).

136. Helft & Miller, *supra* note 19.

137. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 589 (1952) ("The Founders of this Nation entrusted the law making power to the Congress alone . . . .").

138. *See, e.g.*, Cyrus Farivar, *Reading Someone's Gmail Doesn't Violate Federal Statute, Court Finds*, ARS TECHNICA (Oct. 11, 2012, 11:10 PM), http://arstechnica.com/tech-policy/2012/10/reading-someones-gmail-doesnt-violate-federal-statute-court-finds/ (quoting Professor Woodrow Hartzog at the Cumberland School of Law at Samford University as saying that " 'Ultimately, this problem is . . . best resolved by the legislature . . .' "); Helft & Miller, *supra* note 19 ("Many Internet companies and consumer advocates say the [SCA] . . . is outdated, affording more protection to letters in a file cabinet than e-mail on a server.").

139. *See* Kerr, *supra* note 12, at 1233–42.

problem of unauthorized persons deliberately gaining access to, and sometimes tampering with,"[140] private stored communications, Congress needs to flush the SCA's language of overly technical distinctions and shift some of its efforts to protect electronic correspondence over to the Computer Fraud and Abuse Act ("CFAA").[141]

### *A. Simplifying the Stored Communications Act*

As one Internet privacy specialist pointed out, " '[a]ll of the discussions regarding backups, temporary copies, and the [read versus unread] distinction seem to have very little to do with the way that most people perceive their use of e-mail.' "[142] Many have expressed concerns that the SCA has been "outrun" by developments in technology,[143] and one scholar has suggested that the need for amendment is even more urgent given the growing popularity of cloud computing services, whose advertising-supported business models might not technically qualify for SCA protection.[144] In order to safeguard the SCA from becoming entirely obsolete with the evolution of technology, new language should track the function, rather than the mechanisms, of online private communication.

Congress can take its biggest step in this direction by eradicating the term "electronic storage" from the SCA. Indeed, in his 2004 suggested rewritings of sections 2702 and 2703, Professor Kerr eliminated the phrase without comment,[145] apparently regarding the amendment as a given. The term should instead be replaced with language that tracks the function—from the perspective of the *user*—of the technology. Instead of "communication . . . in electronic storage,"[146] the revised statute should use simple language like "private communication."[147] Only by doing this can the statute cope

140. H.R. REP. NO. 99-647, at 62 (1986); S. REP. NO. 99-541, at 35 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589.

141. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

142. Farivar, *supra* note 138 (quoting Professor Woodrow Hartzog).

143. *See, e.g.*, Helft & Miller, *supra* note 19.

144. *See* William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1196 (2010).

145. *See* Kerr, *supra* note 12, at 1235–38. For example, in his rewriting of § 2702(a), the phrase "the contents of a communication while in electronic storage by that service" was replaced with "the contents of that communication or any record or other noncontent information pertaining to a subscriber to or customer of such service." *See id.* at 1237.

146. 18 U.S.C. § 2701 (2012).

147. Because the decision regarding the exact language to be used implicates a great number of Fourth Amendment considerations, it is beyond the scope of this Recent

with fast-paced changes in communication technology, such as the increased integration of text messaging, "instant messaging," and email, as well as the development of replacements for electronic mail services.[148]

### *B. Moving Section 2701 to the CFAA*

Unlike the rest of the SCA, section 2701 does not lay out procedural rules for governmental entities to follow in gaining access to electronic communications; it instead regulates private actions that would not be covered by the Fourth Amendment protections that the statute purports to imitate.[149] Quite simply, if the statute's purpose was to "ensure the continued vitality of the Fourth Amendment,"[150] section 2701 does not fit. Though it disagrees with many points of his narrow interpretation of the SCA, this Recent Development supports Professor Kerr's rather bold proposal to repeal section 2701 from the SCA altogether.[151] However, this Recent Development goes a step further by advocating amendments to the Computer Fraud and Abuse Act to ensure that Congress's goals under section 2701 of the SCA are not lost.

Among Professor Kerr's major rationales for repealing section 2701 is that this part of the statute "is almost entirely redundant," echoing to a large degree prohibitions that already appear in the CFAA.[152] However, if interpreted in accordance with legislative intent, section 2701 has the potential to cover a great number of civil plaintiffs who would not have standing under the CFAA. Whereas the SCA provides relief to any ISP, subscriber, or other person aggrieved by a knowing and intentional violation of the statute,[153] the

Development to settle on finalized language for the statute. Nonetheless, whatever language Congress chooses should be as simple and function-oriented as possible.

148. Tracking in digital trends in recent years has shown a decrease in the use of email and a shift over to platforms like Facebook private messages. *See* Alexia Tsotsis, *ComScore Says You Don't Got Mail*, TECHCRUNCH (Feb. 7, 2011), http://techcrunch.com/2011/02/07/comscore-says-you-dont-got-mail-web-email-usage-declines-59-among-teens/.

149. *See* Kerr, *supra* note 12, at 1238–39.

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

151. *See* Kerr, *supra* note 12, at 1238.

152. *Id.* at 1239. According to Kerr, § 2701 does nothing but "provide[] federal jurisdiction for acts of hacking into and otherwise damaging providers of ECS in the rare circumstance that the conduct does not involve an interstate or foreign communication," as is a condition of the CFAA. *Id.* at 1240.

153. *See* 18 U.S.C. § 2707(a) (2012); ANDREW B. SERWIN, PETER F. MCLAUGHLIN & JOHN P. TOMASZEWSKI, PRIVACY, SECURITY, AND INFORMATION MANAGEMENT § 6:80 (2011). The damages provisions of the SCA provide that "in no case shall a person entitled

CFAA (which is primarily a criminal statute) allows civil actions only by victims who suffer specific types of loss or damage,[154] such as physical injury, modification of medical files, or at least $5,000 in economic loss.[155] For many individual plaintiffs, like Jennings, who wish to protect their private communications from "hackers," such showings would be difficult or impossible.[156] In order to continue to effectuate Congress's broad goal of protecting ISP subscribers from "unauthorized persons [who] deliberately gain[] access to . . . electronic . . . communications that are not intended to be available to the public,"[157] amendments to the CFAA should exempt civil plaintiffs from the statute's nuanced loss requirements and allow relief to those whose private communications have been accessed by intruders.[158]

The protection of private digital information from non-governmental third parties fits more closely into the CFAA, which was created to combat computer crimes and illegitimate access to information belonging to others,[159] than into the SCA, which focuses on creating Fourth Amendment-like protection from government intrusion. Relocating the provisions of section 2701 to the CFAA and broadening the civil remedies allowed to private parties under that statute will prevent the debate over the technical reach of the SCA from disorienting courts into denying relief to plaintiffs whose privacy has been compromised.

---

to recover receive less than the sum of $1,000" and allows for punitive damages if the violation is willful or intentional. *See* 18 U.S.C. § 2707(c).

154. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 3 (2d ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

155. § 1030(g); *id.* § 1030(c)(4)(A)(i).

156. The case does not reveal, for example, whether defendant Gail used the illicitly obtained emails to procure a hefty divorce settlement. If that were the case, then perhaps Jennings would have a cause of action under the CFAA. In a case with similar facts, the court granted summary judgment in favor of the defendants because the plaintiff, who had lost his job after the defendants accessed the contents of his email account, did not allege or prove economic damage. *See* Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914 (W.D. Wisc. 2002).

157. H.R. REP. NO. 99-647, at 62 (1986); S. REP. NO. 99-541, at 35 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589.

158. The CFAA already provides for criminal prosecution of anyone who engages in similar activity. *See* § 1030(a)(2)(C) (punishing anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer"). Allowing civil liability would thus be a small step.

159. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, *supra* note 154, at 1–2.

## CONCLUSION

The language of the Stored Communications Act is notoriously "dense and confusing."[160] The term "electronic storage" alone has especially created rifts among courts attempting to apply the statute to modern technology. That the *Jennings* decision is unsatisfactory is clear: simply failing "to settle on a rationale for a decision invites perpetual attack and reexamination."[161] Reexamination of this case immediately reveals a preoccupation with arbitrary technical distinctions and a failure to consider the only source of clear guidance for SCA decisions—congressional intent.

The need for legislative revision is urgent. The SCA should be simplified and the phrase "electronic storage" eliminated in order to encourage consistent application of the Act among courts and to ensure the SCA's continued relevance as technology develops. In order to support Congress's apparent original intent regarding civil causes of action, the need for amendment also pours over into the CFAA. In the meantime, rather than joining the fruitless struggle of overly-technical analysis of the meaning of "electronic storage," courts should interpret statutory language broadly to avoid arbitrary distinctions and to carry out the purpose which Congress made evident in its reports.

REBECCA A. FISS**

160. Kerr, *supra* note 12, at 1208.

161. Lewis F. Powell, Jr., *Stare Decisis and Judicial Restraint*, 47 WASH. & LEE L. REV. 133, 148 (1990).

** The author would like to thank Professor David Ardia, Professor Anne Klinefelter, and her primary editor, Adam Fleckenstein, for donating their technical knowledge to a student in need.