Florida Law Review

Volume 73 | Issue 3 Article 4

November 2021

"You've Got [Open] [E]mail"—The Unknown Email Privacy Issue and the Need for the Stored Communications Act to Reflect the Modern Utility of the Inbox

James Palanica

"YOU'VE GOT [OPEN] [E]MAIL"—THE UNKNOWN EMAIL PRIVACY ISSUE AND THE NEED FOR THE STORED COMMUNICATIONS ACT TO REFLECT THE MODERN UTILITY OF THE INBOX

James Palanica[†] [*]

Abstract

This Note identifies the divided jurisprudence surrounding the protection of opened emails from unauthorized access under the Stored Communications Act and advocates for the interpretation espoused by the Fourth Circuit's 2019 decision in *Hately v. Watts*. The traditional view of the Stored Communications Act, as employed by the Department of Justice, neither sufficiently protects opened emails nor reflects the modern usage of email inboxes. While the Eighth and Ninth Circuits have previously attempted to expand protection to opened emails by prioritizing user intent, such a standard has proved difficult to manage and has resulted in disparate outcomes depending on whether one uses a desktop-based or web-based email provider. The Fourth Circuit's decision in *Hately* protects opened emails regardless of email platform, but it accomplishes this task by stretching legislative intent to its limit. As a result, the unauthorized access provisions of the Stored Communications Act have been fractured into at least three different interpretations and require a resolution by the Supreme Court or revision by Congress to uniformly protect emails nationwide.

† *Editor's Note*: This Note won the Gertrude Brick Prize for the best Note in Spring 2020.

* J.D./LL.M. in Taxation Candidate 2021, University of Florida Levin College of Law; B.A. 2014, Wofford College. The Author sincerely thanks the editors of the *Florida Law Review* for their insightful feedback and precision. The Author also extends gratitude to Professor Sabrina Little, who provided him with the foundational legal writing skills needed to succeed at UF Law and beyond. Lastly, the Author thanks his family and friends for their constant love and support.

INTRODUCTION

There are an estimated 254.7 million email users in the United States alone,[1] and 95% of them say they check their email either "as often as they should" or "way too often."[2] Despite the frequency with which a vast majority of Americans check their email, it seems unlikely that many email users are aware that the privacy of their emails might depend on whether they have opened their emails or the type of email provider they use.

From the memorable "Try America Online (AOL)" disks and the emergence of free providers such as Hotmail[3] to the much more recent rise of the smartphone and wireless high-speed internet, both the ease and speed of electronic communication have improved. But concerns surrounding privacy have also increased, especially as to the government's ability to acquire emails or other electronic data in the course of an investigation.[4] The recent decisions in *Carpenter v. United States*[5] and *United States v. Dorsey*[6] were quite noteworthy in that they berated and declared unconstitutional portions of the Stored Communications Act[7] (SCA), which had previously allowed the

1. eMarketer & Squarespace, *Number of E-mail Users in the United States from 2013 to 2020*, STATISTA, https://www.statista.com/statistics/253790/number-of-e-mail-users-in-the-united-states/ [https://perma.cc/SGJ2-4L9K].

2. J. Clement, *Frequency of Checking E-mail in General According to Workers in the United States as of June 2018*, STATISTA (July 3, 2020), https://www.statista.com/statistics/911623/frequency-workers-checking-emails-in-general/ [https://perma.cc/ZWG2-AA2E].

3. Kate Hoy, Opinion, *This Month in Tech History: Hotmail Launched*, IDG CONNECT (July 1, 2017, 11:30 AM), https://www.idgconnect.com/article/3581120/this-month-in-tech-history-hotmail-launched.html [https://perma.cc/5J5T-W6LV] (stating that Hotmail was "[p]roclaimed the world's first web-based email when it launched on 4th July 1996. The Independence Day launch aimed to symbolise the 'freedom' Hotmail offered—from ISP-based email as well as the ability to access your inbox from anywhere in the world").

4. *See* 18 U.S.C. § 2703.

5. 138 S. Ct. 2206 (2018).

6. 781 F. App'x 590 (2019).

7. Pub. L. No. 99-508, § 201, 100 Stat. 1860, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2711).

government to obtain electronic data without a warrant or probable cause.[8]

However, despite the importance of *Carpenter* and *Dorsey* in the United States' battle with modern technology, this Note is not another epic of the U.S. Supreme Court heroically lowering the Fourth Amendment's shield to protect individuals from government overreach. Rather, this Note presents the other side of the coin. It is a story of everyday wrongdoing by private parties against one another. Specifically, this Note identifies the splintered authority surrounding a commonplace issue that likely does not cross the mind of either the tech-savvy millennial or the baby boomer user of Outlook Express: the privacy of opened emails under the Stored Communications Act and the right to a civil cause of action for the violation of that privacy in addition to criminal penalties.[9] While courts have recognized that emails intercepted in transit or sitting *unopened* in one's inbox are protected under the SCA,[10] the judicial landscape surrounding the status of opened emails continues to be inconsistent, allowing, for example, the exposure of a mistress's emails to go unpunished in one jurisdiction[11] and reprimanding the search for alleged proof of infidelity in another.[12]

I. THE ESTABLISHMENT OF THE STORED COMMUNICATIONS ACT IN THE CONTEXT OF THE FOURTH AMENDMENT

Prior to examining the differing interpretations regarding one's privacy in open emails, it is important to understand the general reasoning behind Congress's enactment of the SCA.[13] Why would one's personal emails (or other electronic messages) not be inherently protected from

8. *See Carpenter*, 138 S. Ct. at 2221 (concluding "that the Government must generally obtain a warrant supported by *probable cause* before acquiring such records" (emphasis added)); *Dorsey*, 781 F. App'x at 591. In *Dorsey*, the Ninth Circuit acknowledged the unconstitutionality of portions of the Stored Communications Act (SCA), specifically § 2703(d). *Dorsey*, 781 F. App'x at 591. The government had obtained cell tower data under a court order, which does not require a warrant or probable cause. *Id.* "Under the SCA, the government needed to demonstrate only a reasonable belief that the data was relevant and material to an ongoing investigation. *Id.* In light of the recent decision in *Carpenter*, the court held that a warrant supported by probable cause was required to obtain this data.

9. 18 U.S.C. § 2701 (providing criminal penalties for unauthorized access to stored communications); *id.* § 2707 (providing for a civil cause of action).

10. Vista Marketing, LLC v. Burkett, 812 F.3d 954, 963–64 (11th Cir. 2016).

11. Jennings v. Jennings, 736 S.E.2d 242, 243, 245 (S.C. 2012).

12. Hately v. Watts, 917 F.3d 770, 773–74 (4th Cir. 2019).

13. The "Stored Communications Act" is the common vernacular to reference U.S.C. §§ 2701–2711. These sections were initially passed under Title II of the Electronic Communications Privacy Act, but nowhere does the phrase "Stored Communications Act" appear in the language of the statute. COMPUT. CRIME & INTELL. PROP. SECTION, U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 115, n.1 (3d ed. 2009) [hereinafter DOJ ELECTRONIC EVIDENCE].

unauthorized access? Why are electronic communications from one person to another not inherently private?

The average American's innate sense of "privacy" likely stems from the Fourth Amendment's language regarding search and seizure.[14] However, while the Fourth Amendment sets forth foundational individual liberties[15] and shields individuals from arbitrary surveillance,[16] *Katz v. United States*[17] recognized that the Fourth Amendment "cannot be translated into a *general constitutional 'right to privacy*.'"[18] Rather, the Fourth Amendment protects against "certain kinds of government intrusion"[19] and seeks to avoid the development of a police state.[20] *Katz* further refined the Fourth Amendment as "protect[ing] people, not places"[21] and provided the "reasonable expectation of privacy" test.[22] Also, Fourth Amendment protections only exist between the government and citizens, not between private parties.[23] As a result, the evolution of "privacy" in the United States appears to be bifurcated into (1) the judicial application of the Fourth Amendment and (2) any statutorily supplemented privacy rights.

Acknowledging that technology and the ability for arbitrary oversight have both changed since the Founding,[24] Professor Orin Kerr[25] provides an excellent overview of why the Fourth Amendment alone does not provide adequate protection for electronic mail. First, it is unclear

14. *See* 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, and no Warrants shall issue, but upon *probable cause* . . . ." (emphasis added)).

15. *See* Byrd v. United States, 138 S. Ct. 1518, 1526 (2018) ("Few protections are as essential to individual liberty as the right to be free from unreasonable searches and seizures.").

16. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) ("[T]he Amendment seeks to secure 'the privacies of life' against 'arbitrary power.'" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))).

17. 389 U.S. 347 (1967).

18. *Id*. at 350 (emphasis added).

19. *Id.*

20. *Carpenter*, 138 S. Ct. at 2213–14.

21. *Katz*, 389 U.S. at 351.

22. *Id.* at 360–61 (Harlan, J., concurring) (defining the test as "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'").

23. *See id.* at 350–51 (majority opinion) ("[A] person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States." (emphasis omitted) (footnote omitted)).

24. *See* S. REP. NO. 99-541, at 1–2 (1986) (noting that technological advancements over the past centuries have expanded the possibility of arbitrary government oversight beyond physically entering houses and seizing personal effects).

25. Professor Kerr's work and recent Volokh blog post, *see* Orin S. Kerr, *Fourth Circuit Deepens the Split on Accessing Opened E-Mails*, VOLOKH CONSPIRACY (Mar. 21, 2019, 6:05 AM), https://reason.com/2019/03/21/fourth-circuit-deepens-the-split-on-civi/ [https://perma.cc/2NUD-V3MR], shed light on this gap in the Stored Communications Act—and inspired this Note.

whether email users have a "reasonable expectation of privacy" due to the way that email functions as a technology.[26] Generally speaking, an email is first sent to an Internet Service Provider (ISP), which acts as a third party in processing and sending the message onward to the designated recipient.[27] But in theory, when one discloses information to a third party—in this case, an ISP—the individual cannot be considered to have a reasonable expectation of privacy and such information loses Fourth Amendment protections.[28] Second, Professor Kerr emphasizes that rules governing grand jury subpoenas leave emails exposed. Because grand jury subpoenas—unlike warrants—do not require probable cause, emails are much more easily accessible from third-party ISPs.[29] Finally, ISPs are usually *private* third parties and not government entities.[30] Because the Fourth Amendment only restrains the government's behavior, a third-party ISP can disclose information to the government or other third parties.[31] Absent any supplemental form of statutory regulation, the Fourth Amendment alone seems to afford limited protections to email or electronic communications.[32]

Aware of the limitations of the Fourth Amendment, Congress had already expressed sensitivity toward technological developments earlier in the twentieth century.[33] Yet by the mid-1980s, Congress became concerned about the applicability of existing federal law[34] to new forms of electronic communication, such as wireless phones, electronic mail,

26. 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, 1210 (2004).

27. *Id.*

28. *Id.* at 1210 & n.11 (citing several Supreme Court cases in support of this proposition).

29. *See id.* at 1211–12. Because government officials are not often physically raiding an ISP's premises, absent more stringent regulation, officials would request subpoenas over warrants. *See id.*

30. *Id.* at 1212.

31. *Id.* at 1212 & n.22 (citing circuit court cases holding that third-party actors, even when acting maliciously, do not violate the Fourth Amendment so long as they are not acting at the behest of the government).

32. *See id.* at 1212. Professor Kerr notes that the internet appears to be "'custom designed' to frustrate" Fourth Amendment protections. *Id.* (internal quotation marks omitted).

33. S. REP. NO. 99-541, at 1–2 (1986). In 1928, the Supreme Court held in *Olmstead v. United States*, 277 U.S. 438 (1928), that wiretapping did not violate the Fourth Amendment because no item was physically seized by the government nor did a trespass occur. S. REP. NO. 99-541, at 2. However, in 1967, the Court reversed its logic in *Katz v. United States*, 389 U.S. 347 (1967), holding that the Fourth Amendment did apply to government interception of telephone calls, and in the same year released a decision in *Berger v. New York*, 388 U.S. 41 (1967), providing that Fourth Amendment protected citizens from electronic eavesdropping of oral correspondence. S. REP. NO. 99-541, at 2.

34. *See* S. REP. NO. 99-541, at 2 (referencing Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which was enacted in response to the *Katz* and *Berger* decisions).

and pagers.[35] In response, the Office of Technology Assessment (OTA) concluded, in an extensive report published in 1985, that the "existing statutory framework" was not readily applicable to these new technologies and, specifically, that protections for electronic mail were "weak, ambiguous, or nonexistent."[36] The OTA report further clarified that while first-class mail had extensive statutory protections from unauthorized access both during delivery and when inside mail receptacles,[37] electronic mail did not possess any of these safeguards during its transit or storage.[38] Such a dichotomy presented a significant issue because the parties that used first-class mail and electronic mail were (and are still today) identical.[39] Consequently, Congress sought to advance the law with technology in mind to avoid the erosion of Fourth Amendment protections and to secure privacy for electronic mail.[40] As such, the SCA established "a set of Fourth Amendment–like privacy protections by statute" to protect electronic mail.[41] In accomplishing this goal, the SCA not only regulates the government's ability to *force* ISPs to reveal information but also limits the circumstances in which ISPs can *voluntarily* disclose information to the government.[42] To further regulate private parties, the SCA provides for both criminal and civil penalties for persons who unlawfully access, alter, or obstruct lawful access to stored electronic communications.[43] Overall, the SCA seeks to strike a fair balance between citizens' privacy expectations and the legitimate needs of law enforcement.[44]

---

35. *Id.* at 2–4. After Senator Patrick Leahy presented the question to the DOJ, the then-Attorney General concluded in 1984 that reasonable expectations of privacy were "not always clear or obvious" in the context of new forms of wireless electronic communication. *Id.* at 4.

36. OFF. OF TECH. ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 3, 45 (1985) [hereinafter OTA ELECTRONIC SURVEILLANCE].

37. *Id.* at 45; *see, e.g.*, 18 U.S.C. §§ 1701, 1702, 1708 (providing protections against unauthorized access of physical mail).

38. *See* OTA ELECTRONIC SURVEILLANCE, *supra* note 36, at 48–50.

39. *Id.* at 48 ("Government officials might be interested in accessing or maintaining surveillance of electronic mail messages for investigative purposes. Private parties might be interested in electronic mail surveillance for various competitive, personal, and/or criminal purposes.").

40. S. REP. NO. 99-541, at 5.

41. Kerr, *supra* note 26, at 1212.

42. *See id.* at 1212–13 (emphasis added) (citing 18 U.S.C. §§ 2702, 2703); *see also* § 2703(a)–(d) (providing the procedure by which the government can obtain a search warrant, administrative subpoena, or § 2703(d) court order (the latter being held unconstitutional per *Carpenter*) to compel disclosure from an ISP); § 2702(a)–(c) (prohibiting the voluntary disclosure of email contents or customer records, except in the process of disclosing such information to the intended recipients of the emails and certain other enumerated situations, such as in suspected child trafficking cases).

43. 18 U.S.C. §§ 2701, 2707.

44. *See* S. REP. NO. 99-541, at 5.

It appears that the SCA was well-intentioned in filling the gaps presented by the digital age. One would wager that most are happy with the general goal of protecting email in the same manner as first-class mail,[45] setting rules of engagements for third-party ISPs,[46] and sanctioning the unauthorized access of emails.[47] However, the devil is always in the details, or, in this case, in the definitions and conjunctions.[48] This Note focuses on the divisions caused by the SCA's definitions of "electronic storage" and "backup protection."[49] Such divisions highlight the courts' differing views on the SCA's treatment of "opened emails"—a focal point over the modern use of traditional or web-based email inboxes. Further, while the historical development of the SCA has an emphasis on establishing Fourth Amendment-like protections from government oversight, recent disputes seem focused on SCA breaches by private citizens against each other.

II. THE THREE EXISTING INTERPRETATIONS OF "ELECTRONIC STORAGE" AND "BACKUP PROTECTION"—ARE ANY OF THEM ACCEPTABLE?

This Part seeks to clarify the roughly three differing interpretations of the definition of "electronic storage" and "backup protection"[50] as applied to opened emails and, in turn, determine whether opened emails are statutorily protected from unauthorized access under the SCA.[51] To begin, Section II.A discusses the conservative yet splintered opinions in *Jennings v. Jennings*,[52] all of which held that opened emails are not protected by the SCA.[53] Section II.B then analyzes the holdings of *Theofel v. Farey-Jones*[54] and *Anzaldua v. Northeast Ambulance & Fire Protection District*,[55] which struck a middle ground, prizing the user's intent regarding "backup protection." Finally, Section II.C discusses the recent opinion in *Hately v. Watts*,[56] which attempted to embrace the

45. *See* OTA ELECTRONIC SURVEILLANCE, *supra* note 36, at 45.

46. *See* Kerr, *supra* note 26, at 1212–13.

47. *See* §§ 2701, 2707.

48. *See* Jennings v. Jennings, 736 S.E.2d 242, 244 (S.C. 2012); *id.* at 247–48 (Toal, C.J., concurring in the judgment) (debating the significance of the word "and"); Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2004) (applying the rule against surplusage to find certain subsections of the SCA disjunctive rather than conjunctive).

49. *See infra* Sections II.A–C; *see also* 18 U.S.C. § 2510(17) (defining "electronic storage").

50. *See* § 2510(17).

51. *See* § 2701.

52. 736 S.E.2d 242 (S.C. 2012).

53. *Id.* at 245; *id.* at 248 (Toal, C.J., concurring in the judgment); *id.* at 249 (Pleicones, J., concurring in the judgment).

54. 359 F.3d 1066 (9th Cir. 2004).

55. 793 F.3d 822 (8th Cir. 2015).

56. 917 F.3d 770 (4th Cir. 2019).

modern use of email inboxes by extending the SCA's protection to opened emails, regardless of the email technology used.

A. *The Importance of Conjunctions—The Fractured Opinion of* Jennings *and Three Different Ways of Saying "No"*

The background of *Jennings* reveals the importance of the legal distinction between opened and unopened emails. The case invoked a common scenario, the breakdown of an intimate personal relationship.[57] Lee Jennings (Lee) had been having an affair with a woman with whom he had corresponded with over email.[58] After finding a card from another woman in her husband's car and receiving subsequent verbal confirmation from Lee that he had a mistress, Gail Jennings (Gail) informed her daughter-in-law, Holly Broome (Broome), of the situation.[59] Broome knew that Lee had a Yahoo! email account and correctly guessed the answers to his security questions.[60] Broome found opened emails between Lee and his paramour, and Broome gave the emails to Gail's divorce attorneys.[61] When Lee realized that Broome had accessed these emails, Lee sued Gail, Broome, and a private investigator, *inter alia*, for violating § 2701 of the SCA, asserting that his opened emails qualified as being in electronic storage.[62]

After reading the facts of *Jennings*, one might guess that most individuals would recognize some form of wrongdoing on Broome's behalf. Does society's penchant for drama and reality television have one screaming at the television to investigate Lee's alleged mistress? Presumably, yes. But taking a step back, Broome clearly violated her father-in-law's privacy by breaking into his Yahoo! account and reading his emails, right? Wrong: Broome was not held liable under the SCA.[63] Although the five justices of the Supreme Court of South Carolina admonished Broome's behavior and emphasized possible relief on alternative theories, the court issued three different opinions detailing distinct rationales; however, all of the justices ultimately agreed with the result that Lee's emails were not protected under the SCA.[64] This Section explores all three opinions.

---

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

58. *Id.*

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.* Lee Jennings also sued for invasion of privacy, conspiracy, and violations of the South Carolina Homeland Security Act. *Id.*; *see also* S.C. CODE ANN. § 17-30-135 (2020) (providing a civil penalty similar to § 2707 of the SCA). Notably, the South Carolina Code uses the same definition for "electronic storage" as the SCA. § 17-30-15(18).

63. *Jennings*, 736 S.E.2d at 245.

64. *Id.* at 245 (Toal, C.J., concurring in the judgment); *id.* at 248 (Pleicones, J., concurring in the judgment).

First, it is important to identify the contested portion of the SCA. The SCA punishes unauthorized access to "electronic communication while it is in *electronic storage*."[65] The SCA defines "electronic storage" 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[.][66]

The words "and" as well as "backup protection" are key considerations in Justice Kaye Hearn's analysis and the additional concurring opinions.

With regard to the above-emphasized "*and*," Justice Hearn acknowledged that the "traditional interpretation" of the statute espoused by the Department of Justice (DOJ) is that emails must meet both subsection (A) and (B) to qualify for protection.[67] In this scenario, the only emails that would be protected under the statute are those that have been received by the intended recipient's email provider but that have not yet been accessed by the recipient.[68] Such an interpretation of electronic storage seems to focus on the technology of email submission rather than the express intent of the user.[69] Justice Hearn noted that a majority of courts have departed from this interpretation and now accept that an email can be in electronic storage if it meets either (A) *or* (B),[70] citing *Theofel* as the key proponent of the reasoning that opened emails left in an inbox could be considered "in electronic storage."[71] However, because Lee only argued that his emails were in electronic storage pursuant to paragraph (B), Justice Hearn did not commit the court to deciding its preferred interpretation of the "and" language.[72] Additionally, Lee had simply left these emails in his Yahoo! email inbox and did not copy or retain them elsewhere.[73] In reasoning that "passive inaction" in leaving opened emails in an inbox did not comport with the plain meaning of "backup,"

---

65. 18 U.S.C. § 2701(a) (emphasis added).

66. *Id.* § 2510(17) (emphasis added).

67. *Jennings*, 736 S.E.2d at 244; *see* DOJ ELECTRONIC EVIDENCE, *supra* note 13, at 123–24.

68. *See* DOJ ELECTRONIC EVIDENCE, *supra* note 13, at 123–24; Kerr, *supra* note 25.

69. *See* Kerr, *supra* note 25. In order to provide uninterrupted services or prevent loss of data, email/internet service providers often make backups of unopened emails on multiple servers. *See* OTA ELECTRONIC SURVEILLANCE, *supra* note 36, at 50 (mentioning that email providers often make copies of emails for administrative purposes).

70. § 2510(17); *see Jennings*, 736 S.E.2d at 244.

71. *Jennings*, 736 S.E.2d at 244 (citing Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004)).

72. *Id.*

73. *Id.* at 245.

Justice Hearn could not classify the emails as being in electronic storage and therefore held Broome not liable under the SCA.[74]

Furthermore, Chief Justice Jean Hoefer Toal's concurrence advocated that the adoption of the "traditional interpretation of the statute"[75] provides a more equitable application of the law and is most consistent with Congress's legislative intent.[76] In criticizing Justice Hearn's rationale, Chief Justice Toal reasoned that the privacy of opened emails should not depend on the technology the service provider uses.[77] Further, her reasoning turned on the unambiguous use of "and" in the statute, which, barring other context, should retain its plain meaning.[78] As a result, Chief Justice Toal reasoned that "electronic storage refers only to temporary storage [of emails], made in the course of transmission, . . . *and* to backups of such intermediate communications."[79] Thus, the only emails that would be protected under the SCA would be those that are unread. While Chief Justice Toal noted that this interpretation of the law may be "ill-fitted" to govern problems of the modern day, she asserted that this view is most consistent with the legislative history[80] and, in turn, she resisted legislating from the bench.

Justice Costa Pleicones provided the third opinion, with yet a different rationale. While Justice Pleicones agreed that the SCA applied to temporary storage during communications and backups of those communications, he argued that they were distinct from one another and thus must be equally and separately considered.[81] The former applies to unopened emails in transit to the final user, and the latter applies to

74. *Id.*

75. *See* DOJ ELECTRONIC EVIDENCE, *supra* note 13, at 125 (acknowledging both the traditional understanding of "electronic storage" and the new precedent in the Ninth Circuit under *Theofel*).

76. *Jennings*, 736 S.E.2d at 247 (Toal, C.J., concurring in the judgment).

77. *Id.* at 246–47 ("[I]f one uses Microsoft Outlook for e-mail, one will be protected, but if one uses Yahoo! Mail for e-mail, there is no protection."). Chief Justice Toal emphasized the difference between desktop email clients and webmail clients. A desktop email client is a piece of software that pulls emails from a server, such as Microsoft Exchange. In comparison, webmail products, such as Yahoo!, operate entirely in web browsers. Therefore, one would have to download an email from a webmail account to a desktop to save an email copy, but no action would be required with a desktop email client.

78. *Id.* at 247.

79. *See id.* at 248.

80. *Id.*; *see also* S. REP. NO. 99-541, at 8 (1986) ("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, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the *electronic mail company can put the message onto paper and then deposit it in the normal postal system*." (emphasis added)). One can only imagine a millennial's reaction to this suggestion.

81. *Jennings*, 736 S.E.2d at 248–49 (Pleicones, J., concurring in the judgment).

backup copies the service provider makes.[82] Because Lee's emails were not also copies his service provider made for backup, Justice Pleicones concurred that the emails were not protected under the SCA.[83]

Overall, each of the court's opinions sheds some light on the evident inconsistencies when interpreting the SCA. Beginning with the most conservative interpretation, Chief Justice Toal's argument makes sense from a strict textualist perspective. "And" is a coordinating conjunction, which would require the satisfaction of both paragraphs (A) and (B); to modify this meaning would constitute legislating from the bench.[84] In keeping with the traditional view of the SCA,[85] Chief Justice Toal highlighted that the *Theofel* rationale has produced inconsistent results depending on email technology.[86] It seems highly unlikely that the legislators wanted SCA protections to differ between desktop and web-based emails services, given that the intent of the SCA was to bring the security of electronic correspondence to parity with first-class mail.[87] Although Chief Justice Toal desired to avoid "interpretations of a statute which would produce absurd results" in light of legislative history,[88] it is equally frustrating that the SCA does not adequately protect the modern use of email inboxes, which could be accomplished via judicial action or, at least, by a suggestion to legislators.

Justice Pleicones did not add much to the landscape in his short concurrence. In viewing paragraphs (A) and (B) as necessarily distinct, perhaps because temporary intermediate storage and a service provider's decision to back up an email could occur independently from one another, Justice Pleicones's interpretation did not vary much in substance from Chief Justice Toal's.

Justice Hearn's plurality opinion proved to be more open yet somewhat arbitrary. Despite his indication that no decision would be made in adopting either the traditional DOJ interpretation or the *Theofel* interpretation of the SCA, Justice Hearn, perhaps unintentionally, endorsed user intent as a compelling factor relating to "backup protection" in the same vein as *Theofel*. In analyzing "backup protection,"

---

82. *See id.* at 249. This interpretation suggests that Justice Pleicones advocates for an "or" as opposed to an "and" interpretation.

83. *Id.*

84. *See id.* at 248 (Toal, C.J., concurring in the judgment).

85. *See* DOJ ELECTRONIC EVIDENCE, *supra* note 13, at 123.

86. *See Jennings*, 736 S.E.2d at 247–48 (Toal, C.J., concurring in the judgment); *see also* United States v. Weaver, 636 F. Supp. 2d 769, 771–72 (C.D. Ill. 2009) (highlighting that users of web-based email systems, such as Hotmail, are not protected under *Theofel* by Hotmail's default interface, in contrast to users of desktop email systems, such as Microsoft Outlook, who are protected).

87. S. REP. NO. 99-541, at 5 (1986).

88. *See Jennings*, 736 S.E.2d at 247 (Toal, C.J., concurring in the judgment) (quoting Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 575 (1982)).

Justice Hearn concluded that Lee's emails could not be considered backed up specifically because Lee did not take positive action to move the emails from his Yahoo! inbox to another location.[89] If Justice Hearn did not consider user intent relevant, it would not have mattered even if Lee *had* taken the positive action to move his emails because the traditional view of the SCA only considers "backup protection" as relevant to the ISP's needs, not the email user's. It also seems questionable that Justice Hearn's view of user intent could not also include "doing nothing" because Lee's emails were arguably "backed up" and accessible just as easily by leaving them in his Yahoo! inbox as by downloading them to his desktop or paying for separate storage. At any rate, Justice Hearn showed sympathy to the *Theofel* interpretation without formally endorsing it.

B. *Expanding the Protection of Opened Emails—The Ninth Circuit's Focus on User Intent and the Eighth Circuit's Subsequent Temperance*

Consistent with its reputation for having a more expansive jurisprudence,[90] the U.S. Court of Appeals for the Ninth Circuit broke away from the traditional interpretation of "electronic storage" and protections provided to opened emails in *Theofel*. Ironically, the *Theofel* and *Jennings* courts justified their conclusions using the same rationale: the plain meaning of the statutory language.[91] *Theofel* is arguably the seminal case in distinguishing itself from the "traditional" interpretation of the SCA,[92] supporting perhaps a more modern conception of email in effectuating the email user's intent over the ISP's intent. Further, while the U.S. Court of Appeals for the Eighth Circuit acknowledged the importance of user intent emphasized in *Theofel*, the court in *Anzaldua* placed constraints on the subject without clear-cut rules, narrowing the concept but making results less predictable for the public.

---

89. *Id.* at 245.

90. *Hearing on: Oversight of the Structure of the Federal Courts Before the Subcomm. on Oversight, Agency Action, Federal Rights and Federal Courts of the H. Comm. on the Judiciary*, 115th Cong. 12–13 (2018) (written testimony of Brian T. Fitzpatrick, Professor of Law, Vanderbilt Law School). From 1994 to 2015, the Ninth Circuit was reversed more than 2.5 times as often as the least reversed circuits and 44% more often than the next closest circuit, the Sixth Circuit. *Id. See also* Rush Limbaugh, *Keeping an Eye on the Ninth Circus,* RUSH LIMBAUGH SHOW (Feb. 9, 2017), https://www.rushlimbaugh.com/daily/2017/02/09/keeping-a-sharp-eye-on-the-9th-circus/ [https://perma.cc/U8E6-GQXF] (applying the nickname "Ninth Circus" and stereotyping the court as uniquely progressive).

91. *See Jennings*, 736 S.E.2d at 245 (referencing Merriam-Webster Dictionary); *id.* at 246 (Toal, C.J., concurring in the judgment) (citing Webster's Dictionary). Chief Justice Toal's concurrence stressed the plain meaning of the conjunction "and." *Id.* at 247.

92. *See* DOJ ELECTRONIC EVIDENCE, *supra* note 13, at 123. The traditional interpretation, as set forth by the Department of Justice, requires that an item satisfy *both* § 2510(17)(A) and (B) in order to qualify as being in "electronic storage." *See id.* at 123–24.

To continue illustrating the recurring friction of the SCA between private parties, a discussion of the facts of *Theofel* and *Anzaldua* is useful. In *Theofel*, officers of Integrated Capital Associates (ICA) had pending litigation against the defendant, Farey-Jones.[93] During discovery, the attorney for Farey-Jones issued an overly broad subpoena to ICA's ISP, Netgate, for production of emails.[94] Believing the subpoena was a legitimate order, Netgate did not challenge the subpoena and decided to provide garden variety emails to Farey-Jones without notifying ICA's officers.[95] The emails were post-delivery copies that were left on Netgate's servers.[96] Most of the emails provided did not relate to the ongoing litigation, and many were privileged.[97] Needless to say, the magistrate judge berated Farey-Jones's attorney for the egregious subpoena, which resulted in fines.[98] ICA's officers filed a separate civil suit alleging, *inter alia*, that Farey-Jones's actions regarding the subpoena violated the SCA, but the district court held that the SCA did not apply because Netgate had granted Farey-Jones access to the emails.[99]

As a baseline, the Ninth Circuit clarified that the quashed subpoena was consistent with the "unauthorized access" element of § 2701 of the SCA.[100] The court's comparison of the scenario to the common law tort of trespass is illustrative. Just as it would be trespass under common law to physically access, under false pretenses, a storage facility holding sensitive documents, so would it be a violation of the SCA to access electronic storage without permission.[101] Such a rationale seems parallel with Congress's intent to bring the protection of electronic correspondence to parity with older methods of communication.[102]

The Ninth Circuit's rationale regarding "electronic storage" made *Theofel* the seminal case on the issue, departing from the DOJ's traditional interpretation of the SCA.[103] Holding that the "electronic storage" element could be satisfied by meeting § 2510(17)(A) *or* (B),[104]

93. Theofel v. Farey-Jones, 359 F.3d 1066, 1071 (9th Cir. 2004).

94. *Id.* The subpoena should have only been for emails related to the litigation, but was rather for "all emails sent or received by anyone," without regard to date. *Id.* The magistrate judge found the subpoena "patently unlawful." *Id.* at 1071–72.

95. *Id.* at 1071. "Garden variety" is this Note's term—Circuit Judge Kozinski described Netgate's provision of 339 emails as a "free sample" in a "Baskin-Robbins" approach of complying with the subpoena. *Id.* at 1071.

96. *Id.* at 1075.

97. *Id.* at 1071.

98. *Id.* at 1071–72.

99. *Id.* at 1072.

100. *Id.* at 1072, 1074–75.

101. *Id.* at 1072–73 (citing PROSSER AND KEETON ON TORTS § 13, at 78 (W. Page Keeton et al. eds., 5th ed. 1984)).

102. *See* OTA ELECTRONIC SURVEILLANCE, *supra* note 36, at 48, 50.

103. *See* DOJ ELECTRONIC EVIDENCE, *supra* note 13, at 123.

104. 18 U.S.C. § 2510(17).

Theofel drastically increased the categories of emails (or other electronic communications) that are protected under the SCA.[105] As Justice Hearn recognized in *Jennings*, *Theofel*'s broader interpretation has become the majority view in a little over half a decade,[106] with numerous courts following suit.[107] By further recognizing that ICA's emails were undisputedly stored "by an electronic communication service," the *Theofel* court identified that the only issue at hand was whether the emails on Netgate's servers were stored "for purposes of *backup protection*."[108]

From the Ninth Circuit's perspective, the emails located on Netgate's servers were indeed stored for purposes of "backup protection" by the plain meaning of the statutory language.[109] Rather than disapprove of the "passive inaction" in leaving opened emails on Netgate's server, which Justice Hearn later did in *Jennings*,[110] the Ninth Circuit held that an "obvious purpose" of leaving the emails on the server was to recall them again, and that Netgate's copy functioned as a "backup" for the user.[111] Emphasizing the importance of user intent, the Ninth Circuit reasoned that ICA's previously opened emails on Netgate's server were indeed protected under the SCA, and thus reversed the district court's decision.[112]

By focusing on user intent, the *Theofel* court's interpretation of the SCA made the statute more "user-friendly," placing the decision-making regarding storage in the hands of the user. Should the users not ultimately decide how they go about managing their own emails? In a world of cheap (or often free) electronic storage, why should an email user feel compelled to take immediate action on emails, such as downloading,

105. *See Theofel*, 359 F.3d at 1075–76 (indicating that the government's interpretation of the SCA makes subsection (B) superfluous because, if the law only applies to unopened emails in one's inbox, then the emails are already protected under subsection (A)). *But see* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633–34, 636 (E.D. Pa. 2001) (holding that "back-up protection" under subsection (B) does not extend protection to post-transmission storage), *aff'd in part and vacated in part*, 352 F.3d 107 (3d Cir. 2003). The Ninth Circuit critiqued *Fraser*'s interpretation as also rendering subsection (B) substantially without effect by stipulating that "backup protection" only applies to temporary backup storage pending delivery and not to any "post-transmission" activities. *Theofel*, 359 F.3d at 1075–76.

106. Jennings v. Jennings, 736 S.E.2d 242, 244 (S.C. 2012).

107. *See, e.g.*, Strategic Wealth Grp., LLC v. Canno, No. 10-0321, 2011 WL 346592, at *3–4 (E.D. Pa. Feb. 4, 2011); Cornerstone Consultants, Inc. v. Prod. Input Sols., LLC, 789 F. Supp. 2d 1029, 1055 (N.D. Iowa 2011); Shefts v. Petrakis, No. 10-cv-1104, 2011 WL 5930469, at *5 (C.D. Ill. Nov. 29, 2011); 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).

108. *Theofel*, 359 F.3d at 1075 (emphasis added).

109. *Id.*

110. *Jennings*, 736 S.E.2d at 245. Justice Hearn disagreed with the reasoning in *Theofel*, holding that backup protection required some form of affirmative act rather than simply leaving the emails on the server. *Id.*

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

112. *See id.* at 1077.

categorizing, or deleting them? While the *Theofel* opinion is in some ways satisfying because of its emphasis on user intent, its reasoning raises other problems. In countering the government's argument that the SCA only required that the original message be temporary rather than the backup, the Ninth Circuit introduced the concept of an email's "lifespan":

> But 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. An ISP that kept permanent copies of temporary messages could not fairly be described as "backing up" those messages.[113]

As a result, the *Theofel* court prized the concept of user intent, but, perhaps inadvertently, placed a potentially arbitrary limit on the use of inboxes as a permanent repository for open emails. When or how does an underlying email "expire in normal course"? Is it a specific number of days, or when a certain action occurs? The *Theofel* court's reasoning on this issue leaves itself open to attack—particularly given the evidence regarding the SCA's legislative history[114]—and has led to a narrowing and speculation of user intent, rather than a general acceptance of the concept.[115]

Further, the *Theofel* opinion both produces different results depending on email technology and creates certain public policy concerns. To clarify, the plaintiffs in *Theofel* received emails via a traditional desktop client, which received the emails on a server before downloading copies to the plaintiffs' hard drives.[116] It was a two-step process. In contrast, emails delivered to web-based email accounts remain solely in the cloud

---

113. *Id.* at 1076.

114. *See Jennings*, 736 S.E.2d at 246 (Toal, C.J., concurring in the judgment) (reasoning that the legislative history supported that § 2510(17)(B) of the SCA valued the administrative purposes of the service provider, rather than the user's intent or preferences) ("An understanding of the structure of the SCA indicates that the backup provision of the definition of electronic storage exists only to ensure that the government cannot make an end-run around the privacy-protecting ECS rules by attempting to access backup copies of unopened e-mails made by the ISP for its administrative purposes. ISPs regularly generate backup copies of their servers in the event of a server crash or other problem, and they often store these copies for the long term. . . . The statutory focus on backup copies in the SCA was likely inspired by the 1985 Office of Technology Assessment report that had helped inspire the passage of the SCA. The report highlighted the special privacy threats raised by backup copies, which the report referred to as copies '[r]etained by the [e]lectronic [m]ail [c]ompany for [a]dministrative [p]urposes.'" (alterations in original) (citations omitted) (quoting Kerr, *supra* note 26, at 1217 n.61)).

115. *See* Kerr, *supra* note 25; *see also* Kerr, *supra* note 26, at 1218 (noting the ambiguous standard of "whether the user or employees of the service provider have reason to believe that they may need to access an additional copy of the file in the future").

116. *See Theofel*, 359 F.3d at 1075. Arguably, this is the traditional or original form of email, which still is common with employers seeking enhanced security for electronic communication.

on the provider's server. Despite the prioritization of user intent, *Theofel* maintained that in scenarios in which a "remote computing service" was the *only* repository of a user's emails, the emails would not be considered backups.[117] Web-based email inboxes have traditionally been considered "remote computing services" in their capacity of holding opened emails on their servers and therefore have not been protected under the SCA in the same fashion.[118]

In relying on *Theofel*'s logic, other cases have produced results in which web-based email users, which constituted the highest percentage of email users by far in 2020, were not protected under the statute. For example, in *United States v. Weaver*,[119] the district court held as follows:

> Users of web-based email systems, such as Hotmail, default to saving their messages only on the remote system. A Hotmail user can opt to connect an email program, such as Microsoft Outlook, to his or her Hotmail account and through it download messages onto a personal computer, but that is not the default method of using Hotmail. Thus, unless a Hotmail user varies from default use, the remote computing service is the only place he or she stores messages, and Microsoft is not storing that user's opened messages for backup purposes.
>
> . . . .
>
> Previously opened emails stored by Microsoft for Hotmail users *are not* in electronic storage . . . .[120]

Such unequal results under *Theofel*'s logic motivated Chief Justice Toal's concurrence in *Jennings*.[121]

While *Theofel* solidified a competing minority view among some district courts of the SCA's definition of electronic storage and prized the importance of user intent in backing up emails,[122] the Eighth Circuit, in *Anzaldua*, acknowledged the idea of user intent but restricted the scope of backup protection.[123] The circumstances behind *Anzaldua* are also indicative of continued issues with the unauthorized access of email by private parties rather than government interference. In *Anzaldua*, a paramedic (Anzaldua) worked for the local fire district and received a

117. *Id.* at 1076–77.

118. Kerr, *supra* note 26, at 1216.

119. 636 F. Supp. 2d 769 (C.D. Ill. 2009).

120. *Id.* at 772–73 (emphasis added) (footnote omitted).

121. *See* Jennings v. Jennings, 736 S.E.2d 242, 246–47 (Toal, C.J., concurring in the judgment).

122. *See Theofel*, 359 F.3d at 1075–76.

123. *See* Kerr, *supra* note 25.

reprimand from the fire chief for neglect of property.[124] After a further incident involving inflammatory correspondence, which resulted in his temporary suspension,[125] Anzaldua sent an email to a reporter for a large regional newspaper, which discussed alleged safety concerns and misappropriation of department funds.[126] Anzaldua specifically requested to remain anonymous.[127] Despite this attempt at a whistleblower complaint, a copy of the email was mysteriously forwarded from Anzaldua's own Gmail account to the fire chief.[128] As a result, Anzaldua was terminated from his position at the fire district.[129]

In bringing his lawsuit to the district court, Anzaldua claimed, *inter alia*, that his ex-girlfriend and the fire chief had accessed his Gmail account to forward his whistleblower email to the fire district.[130] In support of his theory, Anzaldua indicated that he had traced the account activity to an IP address at or near a restaurant the fire chief owned and where Anzaldua's ex-girlfriend worked.[131] Similar to the *Hately* case discussed below,[132] Anzaldua had provided his ex-girlfriend with his Gmail password for a limited purpose—in this case, to only send resumes to potential employers—but their romantic relationship had ended over a year prior.[133] Although the SCA complaint contained other errors, the district court saw a leave to amend the complaint as futile because Anzaldua had provided his ex-girlfriend with access to his account.[134]

On appeal, the Eighth Circuit held that Anzaldua had sufficiently pleaded the unauthorized access claim[135] but affirmed the denial to amend

124. Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 827 (8th Cir. 2015).

125. *Id.* at 827–28. After the incident regarding neglect of equipment, Anzaldua alleged that he drafted an email to a university professor on his personal computer but never sent it. *Id.* at 827. Despite this testimony, the email was sent from his Gmail account to the professor and made it back into the hands of the fire district chief. *Id.* While Anzaldua included this email to support his SCA claims, it seemed clear (and the court agreed) that a draft email was not included in the SCA because it had not yet been transmitted. *Id.* at 827, 840.

126. *Id.* at 828–29.

127. *Id.*

128. *Id.* at 829.

129. *Id.* at 830.

130. *Id.* at 831, 837–38.

131. *Id.* at 838. Specifically, Anzaldua alleged the forwarding of the whistleblower email from Anzaldua's "sent" box and subsequent deletion of this activity occurred at or near the fire chief's restaurant. *Id.*

132. Hately v. Watts, 917 F.3d 770, 774 (4th Cir. 2019). Given that Hately and his girlfriend had separated, it was presumed that she no longer had permission to utilize Hately's email account. *See id.*

133. *Anzaldua*, 793 F.3d at 838.

134. *Id.* (noting that the complaint was already deficient because it did not appropriately state an SCA claim).

135. *Id.* It seemed apparent to the Eighth Circuit that, taking Anzaldua's story as true, the ex-girlfriend exceeded the scope of permission granted to her. Such a rationale would be

because the email would not have qualified as being in electronic storage "for purposes of backup protection."[136] Anzaldua relied on *Theofel*'s logic, stating that the whistleblower email left in his sent folder served as a backup in case he ever needed to download it again.[137] Recognizing that *Theofel* had been controversial, the Eighth Circuit reasoned that even if it adopted *Theofel*'s user-friendly "lifespan of a backup" approach, the email would still not be considered an intended backup.[138] While user intent is a flexible doctrine and can account for "passive inaction,"[139] the Eighth Circuit was not as receptive to this idea as the *Theofel* court. Anzaldua claimed that the sent email remained on Gmail's servers "as a matter of course," which prompted the Eighth Circuit to reason that Anzaldua did not *intend* to use the copy as a backup.[140] Rather, *Theofel*'s logic would only apply to protect an email stored on the reporter's email system and not Anzaldua's Gmail account.[141]

Anzaldua's argument proves intriguing if one subscribes to the concept that the "SCA is not a catch-all statute designed to protect the privacy of stored Internet communications,"[142] but the Eighth Circuit, in drawing its conclusions, also misconstrued *Theofel*'s reasoning. Much of *Theofel*'s logic prized the idea of user intent and the concept of a "lifespan" or "normal course" of a message (and its corresponding backups).[143] *Anzaldua* quoted *Theofel* in stating that just because "a copy *could* serve as a backup does not mean it is stored for that purpose"; however, *Anzaldua* failed to mention further context.[144] The examples *Theofel* used to identify copies "not in electronic storage" were ones that were in direct correspondence with the ISP's staff or messages that a user had flagged for the ISP's deletion.[145] Both of these examples seem uncommon, however. Neither of these examples suggests that using email as normal, such as keeping emails in one's inbox during correspondence, would inherently disqualify emails as being in storage. Further, the plaintiffs in *Theofel* left their opened emails on Netgate's servers[146] and presumably knew that their "inaction" would leave these

consistent with *Theofel*'s reasoning regarding the common law tort of trespass—one can only use another's land within the scope of permission.

136. *Id.* at 838–39 (quoting 18 U.S.C. § 2510(17)).

137. *Id.* at 840 (citing Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2004)).

138. *Id.* at 842.

139. *See* Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012) (noting Justice Hearn's criticism of simply leaving an opened email in one's inbox).

140. *Anzaldua*, 793 F.3d at 842.

141. *Id.*

142. Kerr, *supra* note 26, at 1214.

143. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004).

144. *Anzaldua*, 793 F.3d at 842 (emphasis added) (quoting *Theofel*, 359 F.3d at 1076).

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

146. *Id.* at 1075–76.

emails in storage, making them available for future reference. Thus, it does not seem to follow that the Eighth Circuit did not allow Anzaldua to rely on the functionality of his email account—as the Ninth Circuit allowed the plaintiffs in *Theofel* to do—to keep his "sent" email in storage because he knew that "sent" emails remained in storage.[147] While *Theofel*'s "normal course" and "lifespan" doctrines are not friendly toward permanent or automatic storage,[148] it would hardly seem reasonable that Anzaldua's recent email correspondence with a reporter could not be considered within the "lifespan" of a sent message retained as a backup given the short period of time that elapsed from him sending the message and awaiting a response from the reporter.[149]

C. Hately v. Watts—*The Fourth Circuit's Focus on Modern Email Services: Satisfying Common Sense*

Hately further reiterates the role of email in the daily lives and relationships of everyday people—in a way not too dissimilar to *Jennings*, but with the opposite result. Again, the background and facts of the case set a relevant stage. From August 2011 to February 2015, Hately and his girlfriend, Torrenzano, had an intimate relationship resulting in two children.[150] During their relationship, they shared their log-in information for their email accounts, which were web-based email accounts provided through Blue Ridge (their community college) and hosted by Google.[151] In March 2015, Torrenzano informed Hately that she was having another intimate relationship with her co-worker, Watts; Hately and Torrenzano separated.[152] Hately's email password remained unchanged.[153] In an effort to help Watts with his still-ongoing divorce, Torrenzano alleged that Watts's wife and Hately were having an affair.[154] Torrenzano provided Watts with Hately's email password to locate emails that corroborated the alleged affair.[155] Once Hately found out that Watts accessed his opened emails, Hately filed a lawsuit, accusing Watts of unlawfully accessing Hately's emails under the SCA.[156]

In analyzing Hately's claim that the district court erred in granting summary judgment for Watts, the U.S. Court of Appeals for the Fourth

147. *Anzaldua*, 793 F.3d at 842.

148. *See Theofel*, 359 F.3d at 1076 ("An ISP that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages.").

149. *See Anzaldua*, 793 F.3d at 842.

150. Hately v. Watts, 917 F.3d 770, 774 (4th Cir. 2019).

151. *Id.* at 773–74.

152. *Id.* at 774.

153. *Id.*

154. *Id.* While the case facts are not crystal clear on this issue, it seems possible that Torrenzano may have contrived Hately's alleged affair.

155. *Id.*

156. *Id.*

Circuit emphasized the congressional intent and legislative history behind the SCA.[157] Making reference to the OTA's 1985 Electronic Surveillance and Civil Liberties study, the Fourth Circuit noted that prior to the SCA's enactment, the "legal protections for electronic mail [were] 'weak, ambiguous, or non-existent'" and further expressed that "electronic mail remain[ed] legally as well as technically vulnerable to unauthorized surveillance."[158] The Fourth Circuit further provided supplementary information from the Senate Report (and corresponding House Report) that this legal vulnerability (1) "discourage[d] potential customers from using innovative communications systems," such as email, (2) "encourage[d] unauthorized users to obtain access to communications" without regard to consequences, and (3) "ero[ded] th[e] . . . right [to privacy]."[159] By providing this background, the Fourth Circuit presented the SCA as a much-needed deterrent to those who might infringe on the privacy of another's electronic data.

Turning to whether Hately's emails were protected under the SCA, the Fourth Circuit began by accepting the basic framework of *Theofel*. First, the court agreed with *Theofel* that the "'prior access [was] irrelevant' [as] to whether emails [were] in 'storage.'"[160] Because Hately's emails were "reserved for future use" by being accessible on Blue Ridge's servers, irrespective of being opened, the court considered these emails "in 'storage'" per the SCA.[161] Second, the court mirrored *Theofel* again by holding that § 2510 could be satisfied by either (A) *or* (B) because holding otherwise would render (B) superfluous.[162]

In addressing the issue of Hately's emails being in "electronic storage" by an "*electronic communication service*," the Fourth Circuit pushed past *Theofel's* framework. Specifically, the SCA distinguishes between "electronic communication services" and "remote computing services." An electronic communication service allows users to send and receive electronic communications, whereas a remote computing service provides computer storage or processing services to the public.[163] Further, the SCA's elevated protections only apply to electronic communication services.[164] The Fourth Circuit rejected the argument that

157. *Id.* at 782.

158. *Id.* at 783 (quoting S. REP. NO. 99-541, at 4 (1986) (quoting OTA ELECTRONIC SURVEILLANCE, *supra* note 36, at 44)).

159. *Id.* (quoting S. REP. NO. 99-641, at 5) (alteration in original); *see* H.R. REP. NO. 99-647, at 19 (1986).

160. *Hately*, 917 F.3d at 786 (quoting Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004)).

161. *Id.*

162. *Id.* at 787.

163. 18 U.S.C. § 2510(15) (defining "electronic communication service"); *id.* § 2711(2) (defining "remote computing service").

164. *See id.* §§ 2701, 2703.

Hately's email account only functioned as a remote computing service with respect to his opened emails, holding that email providers were by definition electronic communication services and could function simultaneously as both types of services.[165]

With regard to "electronic storage" for purposes of "backup protection," the Fourth Circuit discarded *Theofel*'s user intent argument and sought coverage for web-based email services. Hately's opened emails were hosted by Google, a web-based provider, and such technology uses redundant systems in multiple locations around the world.[166] Redundant systems generate numerous copies of emails on different servers to prevent the destruction of email and ensure accessibility.[167] The Fourth Circuit reasoned that a web-based provider used these copies to its own benefit and administrative ease, as well as for the protection of the user.[168] In this same vein, while the court acknowledged and arguably expanded user intent to include permanent storage, the court focused on web-based email as a product and highlighted that:

> [T]he meaning of "backup protection" does not turn on whether a *user* subjectively chose not to delete the email after reading the message because the *user* wanted to keep the message for backup protection. That is because the purpose of the *web-based email service* in providing storage for the message—storage that is a feature of the product the web-based email service offers—is to afford the user a place to store messages the user does not want destroyed. The *web-based email service* does not need to know why the user has elected not to delete [a] particular message. Rather, the *web-based email service* recognizes that users who choose to use a web-based email platform desire storage for read and unread messages and therefore the *web-based email service* provides such storage to meet user demand."[169]

The Fourth Circuit also justified that web-based email technology conformed to the SCA's legislative history in how one accessed email. The House Report stated that an electronic mail service, which held a message in storage until the addressee "requested" it, was subject to

165. *Hately*, 917 F.3d at 789 ("[B]ecause an entity can simultaneously function as an electronic communication service and a remote computing service, an entity's status as a remote computing service in no way precludes a determination that the entity also was acting as an electronic communication service.").

166. *Id.* at 791.

167. *Id.* at 791–92.

168. *Id.* at 793.

169. *Id.*

§ 2701.[170] The court noted that Hately's email service held copies of his messages in this capacity, Hately could "request" them as many times as he wanted online, and nothing in the House report indicated that § 2701's protections were limited to the *first* time a message was "request[ed]."[171] As a result, the court held that Hately's opened emails stored by a web-based email were in electronic storage and protected under the SCA.[172]

While the Fourth Circuit's decision to fill the gap and protect the status of opened web-based emails was appreciated, practical, and needed, its reasoning was at times a stretch; the court reasoned that certain enumerated statements in the SCA and its legislative history did not expressly exclude other alternatives. The questionable nature of this reasoning can be seen in the court's allowance for remote computing services to overlap with electronic communication services, thereby extending the protections afforded to the electronic communication services under the SCA.[173] The lower court's interpretation that an email provider could only be acting as one type of service or the other, depending on the status of the email, also seemed plausible because they were separately enumerated. Despite bending specific SCA provisions, the *Hately* court seemed to run true to Congress's *overarching* intent, specifically to "fill in a 'gap' in the then-existing law as to 'the protect[ion of] the privacy and security of communications transmitted by . . . new forms of telecommunications and computer technology,' including email."[174] Web-based email platforms, such as Gmail, seem to fall in these "gaps" in the twenty-first century, just as the protections for email in general were "weak, ambiguous, or nonexistent" compared to first-class mail in the 1980s.[175] Much like Chief Justice Toal's opinion in *Jennings* criticized *Theofel*'s conceptions of user intent and differing email technologies as producing absurd results,[176] the Fourth Circuit's rationale also sought to avoid "arbitrary and untenable 'gap[s]' in the legal protection of electronic communications."[177] Indeed, the Fourth

170. H.R. REP. NO. 99-647, at 63 (1986).

171. *Hately*, 917 F.3d at 794.

172. *Id.* at 794–98.

173. *Id.* at 788 ("But nothing in the plain language of the definitions of electronic communication service and remote computing service precludes an entity from simultaneously functioning as both.").

174. *Id.* at 797 (alteration in original) (quoting S. REP. NO. 99-541, at 5 (1986)).

175. *See* OTA ELECTRONIC SURVEILLANCE, *supra* note 36, at 45.

176. Jennings v. Jennings, 736 S.E.2d. 242, 246–47 (Toal, C.J., concurring in the judgment) (citing Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 575 (1982)).

177. *Hately*, 917 F.3d at 798 (quoting S. REP. NO. 99-541, at 5) ("It defies logic that the unopened junk and spam email messages that a user leaves in his or her inbox or designated folder without opening would be entitled to *more* protection than those messages the user chooses to open *and* retain. We do not believe Congress intended such an absurd result when it enacted a statute intended to fill in the gaps in the then-existing privacy protections for electronic communications and therefore spur adoption of new communication technologies, like email.").

Circuit did so rather successfully by bringing opened emails on web-based email servers into the fold.

CONCLUSION

Overall, the importance of the SCA cannot be understated. Providing both civil and criminal penalties for unauthorized access to electronic communications services,[178] among other protections that restrict an ISP's disclosure of information to the government or other parties,[179] the SCA serves as an important deterrent in maintaining a civil society. Just as first-class mail is protected from unauthorized access while in transit or storage, so should electronic mail be protected from unauthorized access—whether the email is opened or not.

However, considering protections were unclear for electronic mail in the 1980s prior to the enactment of the SCA, "[i]t is not always easy to square the decades-old SCA with the current state of email technology."[180] Much about email use and technology has changed (and continues to change) since 1986, but the protection of emails should not depend on whether one uses a desktop-based email provider or web-based provider. Further, emails should be protected from unauthorized access whether they are unopened or opened. Unlike first-class mail, which requires physical storage space, email services provide an easy and compact way to store correspondence in a virtually unlimited capacity—and the privacy of these documents should not be absolved in an arbitrary manner.

Ensuring comprehensive email protections under the existing SCA has proved tedious. By maintaining a strict textual reading of the SCA and resisting the urge to legislate from the bench, a plurality of the *Jennings* court declined to expand coverage of opened emails yet acknowledged gaps in protection existed.[181] While the *Theofel* and *Anzaldua* courts sought to expand protection by emphasizing user intent, their interpretations were also flawed in that user intent could be difficult to prove regarding a user's inaction and the protection differed in result based on email technology. Only as recently as 2019 did the *Hately* court succeed in expanding coverage to opened emails irrespective of whether one uses a desktop or web-based email service, but it did so only by skillfully maneuvering around statutory language and construing nearly thirty-five-year-old legislative intent in its favor.

178. 18 U.S.C. § 2701 (criminal penalties); *id.* § 2707 (civil penalties).

179. *Id.* §§ 2702–2703.

180. Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 839 n.5 (8th Cir. 2015).

181. *See Jennings*, 736 S.E.2d at 248 (Toal, C.J., concurring in the judgment) ("The SCA is ill-fitted to address many modern-day issues, but it is this Court's duty to interpret, not legislate."); *id.* at 245 ("We emphasize that although we reject the contention that Broome's actions give rise to a claim under the SCA, this should in no way be read as condoning her behavior.").

Comprehensive email protection remains irregular outside of the Fourth Circuit. Although the Supreme Court denied certiorari in *Theofel* in 2004 and in *Jennings* in 2013, the recent decision in *Hately* brings hope that other circuits and the Supreme Court will adopt the Fourth Circuit's interpretation of the SCA to expand protection to all opened and unopened emails, regardless of email technology—or that Congress will revise the SCA accordingly.