The Stored Communications Act and the Fourth Circuit: Resolving the Section 2510(17)(B) Circuit Split in *Hately v. Watts*

James Elustondo*

TABLE OF CONTENTS

* James C. Elustondo, J.D., May 2022, The George Washington University Law School. I want to thank my parents, Patricia and Don, and my brother, Tom, for their unwavering support. I would also like to thank Professor Ethan Lucarelli for his assistance during drafting, as well as the Editorial Board and associates at FCLJ for their work during the editorial process.

I. INTRODUCTION

A person accesses your Gmail account by gaining your password or by hacking in. By viewing only your *opened* emails, those that have been read or opened previously, that person learns you will be away from your home or apartment for some period of time, and they rob you of all your belongings. When the perpetrator is caught, evidence of the robbery is thrown out in court, while evidence of the unauthorized access of your Gmail account remains admitted. Under this set of facts, the Eighth Circuit would likely hold that this perpetrator is not subject to any criminal or civil liability for accessing your inbox under section 2510(17)(B) of the Stored Communication Act (SCA) because he looked exclusively at *opened* emails, rather than viewing *unopened* emails that have not been read or opened previously.[1] If this comes across as an arbitrary, counter-intuitive interpretation of a law meant to protect electronic communications, you are not alone in that opinion.

The Eighth Circuit's narrow interpretation of the SCA, which excludes protections for opened emails, can discourage opening emails in order to protect their contents. Because people tend to open most emails that contain sensitive personal information, this reading of the SCA leaves a major gap in the already minimal protections Americans have against cyber-crime, identity theft, and other forms of fraud. Fortunately, the law regarding this issue is not settled and a substantial circuit split has formed between the Eighth Circuit and two other circuit courts. The other circuits, the Ninth and now the Fourth, have rejected the narrow reading of section 2510(17)(B) which fails to protect opened emails under the SCA's definition of 'electronic storage.'[2] This Note addresses this split and interprets the statutory language broadly to include and protect opened emails under this provision. In its holding in *Hately*, the Fourth Circuit adopted some of the Ninth Circuit's grammatical and superfluity reasoning from the Ninth Circuit's earlier *Theofel v. Farey-Jones* opinion, but the Fourth Circuit's opinion provides far more comprehensive arguments in favor of reading section 2510(17)(B) broadly, as well as addresses counterarguments at length, differs in crucial respects, and accounts for modern technology in its analysis. Courts across the country should adopt the Fourth Circuit's interpretation of section 2510(17)(B) of the SCA protecting opened emails because of the strength of the court's arguments regarding the statute's plain meaning, the superfluity doctrine, the legislative history, the absurdity doctrine, and the substantial, intervening technological developments, in addition to independent policy considerations and common sense.

This Note will first discuss the importance of providing adequate protections for email communications and explore the threats posed by a failure to do so. The Note will then discuss the rationale for passing the

1. *See* Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-42 (8th Cir. 2015).

2. *See* Hately v. Watts, 917 F.3d 770, 786, 796 (4th Cir. 2019); Theofel v. Farey-Jones, 359 F.3d 1066, 1071, 1075-76 (9th Cir. 2004).

Electronic Privacy Act, which included the Stored Communications Act, a provision specifically providing adequate protection for electronic communications from government overreach and cybercriminals. Next, this Note will cover section 2701, which outlines what is an offense under the SCA and explains the definitions of electronic storage, electronic communication, and electronic communication service for the purposes of interpreting section 2510(17)(B). Next, this Note will discuss the facts and holdings from key cases, including the primary arguments animating the circuit split and inconsistent treatment by the courts. The analysis section will then begin with the assertion that the Fourth Circuit's plain meaning and superfluity arguments for the broad interpretation should prevail over those arguments made by other courts. A discussion of the absurd results created by reading subsection B narrowly and a discussion of the evidence in the legislative history for a broad interpretation will follow. The Note will then analyze the Fourth Circuit's key interpretive innovations in *Hately* compared to the Ninth Circuit's ruling in *Theofel*. The Note will then cover policy considerations independent from the Fourth Circuit's arguments favoring the broad reading of section 2510(17)(B). The final section will discuss some alternative solutions to the circuit split other than adoption of the Fourth Circuit's interpretation.

II. BACKGROUND

A. Widespread Email Usage and Growing Threats Posed to Data Contained in Email Inboxes

Email has become one of the most pervasive forms of communication in the world. In 2020, roughly 306.4 billion emails were sent each day, and, as of 2020, there were 4 billion global email users with that number only set to grow.[3] Among Americans aged 15-64 in 2019, the percentage of Internet users utilizing email did not drop below 90%, and even 84% of Americans aged 65+ used email.[4] Despite the growing use of social media and other messaging platforms, email usage rates continue to increase steadily.[5] As Americans rely on their email accounts more and more during the Covid-19

3. Joseph Johnson, *Number of Sent and Received E-mails per Day Worldwide from 2017 to* 2025, STATISTA (Oct. 19, 2021), https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/ [https://perma.cc/2HUY-6T6E]; Statista Research Department, *Number of E-Mail Users Worldwide 2017-2025*, STATISTA (Mar. 19, 2021), https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/ [https://perma.cc/KX3R-H4R9].

4. Joseph Johnson, *Share of U.S. E-Mail Users 2019 by Age Group*, STATISTA (Jan. 27, 2021), https://www.statista.com/statistics/271501/us-email-usage-reach-by-age/ [https://perma.cc/C95B-VHNE].

5. THE RADICATI GROUP INC., EMAIL STATISTICS REPORT, 2015-2019, http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf [https://perma.cc/J39H-YBKS].

pandemic, the amount of personal data that can be gleaned from their inboxes grows alongside this reliance.[6]

Email usage in the U.S. is clearly widespread, and the threats posed to the security of these email accounts become more serious every day. For example, in 2016, Yahoo reported that 500 million accounts had been breached, and the company later confirmed the actual number was closer to three billion accounts worldwide.[7] The data stolen included names, email addresses, phone numbers, birthdays, passwords, as well as security questions and their answers; this essentially gave hackers (or those to whom they sell data) the ability to completely control Yahoo webmail accounts.[8] Personal and business email accounts are targeted by cyber-criminals for the treasure trove of personal or business data they hold for identity thieves and data brokers.[9] Most online services also require a user to enter an email address, and if someone else can access your inbox, they can reset the passwords of your accounts to take control of them.[10] In 2021, 3.2 billion emails and their associated passwords were leaked onto a hacker website from a number of different data breaches.[11] Additionally, the threat of identity theft and other types of fraud have grown in recent years. In 2019, the FTC received 3.3 million identity theft and fraud reports; while in 2020, the FTC reported 4.7 million.[12] From January 2021 to August 2021 alone, $519.43 million were lost to identity theft or other fraud often involving the use of personal data.[13] Furthermore, 70% of American adults believe that their personal data is less

6. Geoffrey Fowler, *The Three Worst Things about Email, and How to Fix Them*, WASH. POST (July 21, 2020), https://www.washingtonpost.com/technology/2020/07/21/gmail-alternative-hey/ [https://perma.cc/8SSJ-56MG].

7. Robert McMillan & Ryan Knuston, *Yahoo Triples Estimate of Breached Accounts to 3 Billion*, WALL ST. J. (Oct. 3, 2017, 9:23 PM), https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804.

8. Lily Hay Newman, *Hack Brief: Hackers Breach a Billion Yahoo Accounts.* WIRED (Dec. 14, 2016, 7:27 PM), https://www.wired.com/2016/12/yahoo-hack-billion-users/ [https://perma.cc/29AC-QRYZ].

9. Microsoft 365 Team, *Why a Billion Hacked E-Mail Accounts Are Just the* Start, MICROSOFT (Apr. 2, 2019), https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/why-a-billion-hacked-email-accounts-are-just-the-start [https://perma.cc/PJG2-8EAC].

10. *Id.*

11. Bernard Meyer, *COMB: The Largest Breach of All Time Leaked Online with 3.2 Billion Records*, CYBERNEWS (Feb. 12, 2021), https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free [https://perma.cc/B9PV-46YD].

12. *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Feb. 4, 2021) [https://perma.cc/SVL5-AH4B]; *New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020*, FTC (Feb. 4, 2021), https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers [https://perma.cc/UZ8G-DVGG].

13. Federal Trade Commission, *FTC Covid-19 and Stimulus Reports*, TABLEU PUBLIC, (Oct. 19, 2021), https://public.tableau.com/app/profile/federal.trade.commission/viz/COVID-19andStimulusReports/AgeFraud [https://perma.cc/XMX5-PYLB].

secure than it was five years ago.[14] Simply put, email inboxes contain vital personal information and business data which requires adequate protection.

B. The Electronic Communications Privacy Act of 1986 and Title II of The Stored Communications Act: An Effort to Protect Electronic Communications in Section 2701(a) and the Meaning of "Facility"

Even in the 1980s, before the massive growth in email usage, Congress saw the need for strengthened protections of electronic communications, both from government investigators and criminals.[15] The Electronic Communications Privacy Act of 1986 (ECPA) was the result, passed as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[16] ECPA has three titles under the general ECPA umbrella.[17] The first title is the Wiretap Act, or Title I, which raised the standards for government search warrants seeking aural communications, or those involving the human voice, while they are in transit.[18] The second title is the Stored Communications Act (SCA), or Title II, which is the key title in the broader law for the protection of email communications.[19] The third title is the Pen Register Act, or Title III, which prohibits the use of pen registers or other devices that capture dialing, routing, addressing, and signaling information absent a court order.[20] Whereas communications in transit are primarily protected by the Wiretap Act, communications within storage fall under the SCA.[21]

The opening section of the SCA, section 2701, lays out the protections afforded to email inboxes. Section 2701(a) makes it an offense to "(1) intentionally access without authorization a facility through which an electronic communication service is provided or (2) intentionally exceed an authorization to access that facility and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage."[22]

---

14. Brooke Auxier et. al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/K4B5-NDJ8].

15. *See* Justice Information Sharing, *Electronic Communications Privacy Act of 1986 (ECPA)*, U.S. DEP'T OF JUST., https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last accessed Feb.7, 2022) [https://perma.cc/N82G-GZMZ].

16. *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 350 (6th ed. 2018).

22. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701(a).

For the purposes of this Note, the pertinent "facility" is the inbox or web-based server on which email services store a user's communications, rather than a specific computer or cell phone. The violations discussed throughout involve accessing another person's email inbox from a device other than the victim's personal device. The question of whether computers, cell phones, and other physical devices qualify as facilities under the SCA, when someone intentionally accesses a victim's device without authorization rather than using a different device to access a web-based server without authorization, is outside the scope of this argument. First offenses are punishable by a fine per violation, and can be punished by up to a year in prison.[23] Offenses committed for purposes of commercial advantage, malicious destruction, or private commercial gain are subject to a fine and up to five years in prison.[24] The SCA also provides a private right of action for services, subscribers, or any other person aggrieved by a violation of the statute.[25] The court assesses the sum of actual damages suffered by the plaintiff and any resulting profits made by the violator, but in no case "will a person entitled to recover receive less than the sum of $1,000."[26] If the violation is intentional or willful, the court may also assess punitive damages, and, if the civil action is successful, reasonable attorney's fees.[27] While a few courts have held that actual damages are a prerequisite for awarding statutory damages,[28] a substantial number of district courts, as well as the Ninth Circuit, have held that proving actual damages is not required for an award of statutory damages per violation.[29] To fully understand the scope of the SCA's protections, the terms (1) electronic storage, (2) wire or electronic communication, and (3) electronic communication service must be fully defined and explained.

---

23. *Id.* § 2701(b)(2)(A).
24. *Id.* § 2701(b)(1)(A).
25. *Id.* § 2707(a).
26. *Id.* § 2707(c).
27. *Id.*
28. *See* Vista Mktg., LLC v. Burkett, 812 F.3d 954, 971 (11th Cir. 2016); Cornerstone Consultants, Inc. v. Prod. Input Solutions, L.L.C., 789 F. Supp. 2d 1029, 1055-56 (N.D. Iowa 2011).
29. *See* Cline v. Reetz-Laiolo, 329 F. Supp. 3d 1000, 1045-46 (N.D. Cal. 2018) ("I will follow the seemingly unanimous view of my fellow district courts in this circuit to conclude that actual damages are not necessary for a plaintiff to recover statutory damages under the SCA."); Aguiar v. MySpace LLC, No. CV1405520SJOPJWX, 2017 WL 1856229, at *9 (C.D. Cal. May 5, 2017) ("[A] party 'aggrieved by a violation of the Act could obtain the minimum statutory award without proving actual damages.'"); Chavan v. Cohen, No. C13-01823 RSM, 2015 WL 4077323, at *4 (W.D. Wash. July 6, 2015) ("The Court … finds that a plaintiff need not prove actual damages or profits and that multiple violations of the SCA may warrant multiplying the $1,000 minimum statutory award by the number of each discrete violation."); Joseph v. Carnes, 108 F. Supp. 3d 613, 618 (N.D. Ill. 2015); Maremont v. Susan Fredman Design Grp., Ltd., No. 10 C 7811, 2014 WL 812401, at *7 (N.D. Ill. Mar. 3, 2014); Brooks Grp. & Assoc.'s, Inc. v. LeVigne, No. CIV.A. 12-2922, 2014 WL 1490529, at *9-10 (E.D. Pa. Apr. 15, 2014); Shefts v. Petrakis, 931 F. Supp. 2d 916, 917-19 (C.D. Ill. 2013); Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 759 F. Supp. 2d 417, 427-428 (S.D.N.Y. 2010); Wyatt Technology Corp. v. Smithson, 345 Fed. App'x. 236, 239 (9th Cir. 2009) (remanding for determination of statutory damages even in the absence of actual damages).

1. Definition of "Electronic Storage"

The SCA defines electronic storage in section 2510(17) 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 the purposes of backup protection of such communication."[30] The definition focuses on how and why the communication was stored, whether temporarily, intermediately, or purposefully for backup purposes. Many courts have held, supported by legislative history, that the two subsections recognize two discrete types of protected electronic storage: (1) storage "incidental to transmission" and (2) "backup" storage.[31] However, the focus of the circuit split and the discussion in this Note is the meaning of 'for the purposes of backup protection,' and, specifically, whether opened emails fall under this section 2510(17)(B) definition of electronic storage. Congress did not define 'backup protection' in the law and courts have not been able to settle on one interpretation of this specific language, let alone how the language fits into the broader statutory scheme.[32]

2. Definition of "Electronic Communication"

The SCA defines electronic communication broadly, with a few exceptions irrelevant to this discussion, as "any transfer of signs, signals, writing, images, sounds, data, or intelligence for foreign commerce transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce."[33] The plain language of the definition and the SCA's legislative history both confirm that this definition includes email communications.[34] Although section 2510(17)(B) does not explicitly mention "wire or electronic communication," the words "such communication" clearly references this

30. 18 U.S.C. § 2510(17).

31. *See* Hately v. Watts, 917 F.3d 770, 783 (4th Cir. 2019); Theofel v. Farey-Jones, 359 F.3d 1066, 1069 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003), *aff'g in part, vacating in part, and remanding* 135 F.Supp.2d 623 (E.D. Pa. 2001); H.R. REP. NO. 99-647, at 68 (1986); S. REP. 99-451, at 35 (1986).

32. *See Hately*, 917 F.3d at 770; *Vista Mktg.*, 812 F.3d at 976 ("considerable disagreement exists over whether, and if so, under what conditions, opened email transmissions may qualify as being held in 'electronic storage'"); Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-42 (8th Cir. 2015); *Theofel*, 359 F.3d at 1066; Orin S. Kerr, *Fourth Circuit Deepens the Split on Accessing Opened E-Mails*, REASON: VOLOKH CONSPIRACY (Mar. 21, 2019; 6:05 AM), https://reason.com/volokh/2019/03/21/fourth-circuit-deepens-the-split-on-civi/ [https://perma.cc/2SAB-QAE5].

33. Stored Communications Act, 18 U.S.C. § 2510(12).

34. *See Hately*, 917 F.3d at 785; *Vista Mktg.*, 812 F.3d at 964 (recognizing that emails are "subject to the protections of 18 U.S.C. § 2701(a)"); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002); In Matter of Application of U.S., 416 F.Supp.2d 13, 16 (D.D.C. 2006) ("[T]here can be no doubt that the definition is broad enough to encompass e-mail communications."); H.R. REP. NO. 99-647, at 34 (recognizing that the definition of "electronic communications" provides "electronic mail" with protection); S. REP. NO. 99-541, at 14.

language in section 2510(17)(A).[35] Proponents of the narrow interpretation, however, disagree that "such communication" references "wire or electronic communication" exclusively, arguing instead that "such communication" references the entirety of "wire or electronic communication incidental to the electronic transmission thereof" from section 2510(17)(A).[36] Under this alternative reading, a stored, previously opened email would no longer be "incidental to the electronic transmission thereof" because the email is no longer in transit to the end viewer, and thereby falls outside the statutory definition.

3. Definition of "Electronic Communication Service"

Electronic communication service (ECS) is also defined broadly as any service which provides users with the ability to send or receive these wire or electronic communications.[37] When the law was originally passed in 1986, only email clients such as Eudora were used primarily by businesses, whereas widely accessible webmail services you can now access using a browser, such as Gmail, did not exist yet.[38] For traditional email clients, a user's email was stored on an Internet service provider's (ISP) server and the email was downloaded to permanent storage on a local computer to be read via a dedicated application.[39] By using webmail instead, anyone with access to a browser and an Internet connection can view their emails after they are pulled from an ECS server.[40] The browser downloads the emails and the messages are loaded to the user's device for temporary storage, remaining on the ECS server until expressly deleted but not permanently on any one device.[41] This ECS definition is broad enough to encompass both types of electronic mail

35. *See e.g. Hately*, 917 F.3d at 787; *Theofel*, 359 F.3d at 1075 (9th Cir. 2004); *Fraser*, 352 F.3d at 114; Strategic Wealth Group, LLC v. Canno, No. CIV.A. 10-0321, 2011 WL 346592, at *3-4 (E.D. Pa. Feb. 4, 2011); Cornerstone Consultants, Inc. v. Prod. Input Sols., L.L.C., 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); Bailey v. Bailey, 2008 WL 324156, at *6 (E.D. Mich. 2008); Flagg v. City of Detroit; 252 F.R.D. 346, 362 (E.D. Mich. 2008).

36. *See* Jennings v. Jennings, 736 S.E.2d 242, 248 (S.C. 2012) (Toal, C.J., concurring in the result); OFF. OF LEGAL EDUCATION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 125 (3d ed. 2009); 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, 1216-17 (2004).

37. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510(14).

38. *See Weaver*, 636 F. Supp. 2d at 772.

39. *Id.*

40. *See* Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 287 (2013); *see also Jennings*, 736 S.E.2d at 245.

41. *See Weaver*, 636 F.Supp. 2d at 772.

services.[42] Also, most email service providers today operate email clients, browser webmail, and mobile applications utilizing temporary storage. Proving that the communications in question fall within the definitions of all three terms (electronic storage, electronic communication, and electronic communication service) is critical for establishing SCA protection.[43]

C. A Circuit Split Over Whether Subsections A and B Should Be Read Together and Whether "Backup Protection" Requires an Original Email and a Backup Copy

The circuit split at issue here that has formed over the interpretation of section 2510(17)(B), whether backup protection includes opened emails, is grounded in three primary cases from three appellate circuits: *Theofel v. Farey Jones* from the Ninth Circuit, *Anzaldua v. Northeast Fire Protection District* from the Eighth Circuit, and *Hately v. Watts* from the Fourth Circuit. The Ninth Circuit's *Theofel* ruling proffered the original superfluity and grammatical arguments for the broad interpretation of section 2510(17)(B), and the Fourth Circuit adopted some of this reasoning.[44] The Eighth Circuit in *Anzaldua* discussed the primary arguments made against the broad interpretation of the subsection.[45] However, the Eighth Circuit case dealt with unauthorized access of a user's sent or draft messages, rather than messages received in an inbox, and the Fourth Circuit in *Hately* rebutted the arguments discussed in *Anzaldua* thoroughly in its application to opened emails.[46] In *Hately*, the appellee claimed to have viewed previously opened emails only, making the case an ideal set of facts under which to analyze the unopened/opened divide bearing on SCA protection.[47] Ultimately, the Fourth Circuit's decision and its underlying arguments are more thorough and more compelling than those made by the Ninth Circuit seventeen years ago.

---

42. *See, e.g.*, Vista Mktg., LLC v. Burkett, 812 F.3d 954, 963-64 (11th Cir. 2016) (holding that the defendant "qualified as an [electronic communication service] because it was a service that provided employees with the ability to send and receive electronic communications, including emails"); Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (holding that the definition of electronic communication service "covers basic e-mail services"); In re United States for an Ord. Pursuant to 18 U.S.C. § 2705(b), 289 F.Supp. 3d 201, 209 (D.D.C. 2018) (holding that online booking company was an electronic communications service for the purposes of a dispute related to disclosing messages from the company's "user-to-user electronic messaging system").

43. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701(a).

44. *See* Hately v. Watts, 917 F.3d 770, 797 (4th Cir. 2019); Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

45. Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-42 (8th Cir. 2015).

46. *Id.*; *Hately*, 917 F.3d at 792-96.

47. *See Hately*, 917 F.3d at 773-74.

1. Ninth Circuit in *Theofel v. Farey-Jones* (2004) Holds that Opened, Previously Read Emails Are Covered by the SCA

Wolf and Buckingham became engaged in commercial litigation against Farey-Jones in their capacity as officers of Integrated Capital Associates, Inc. (ICA).[48] During discovery, Farey-Jones sought access to ICA's email and had lawyer Iryna Kwasny subpoena NetGate, ICA's ISP.[49] Rather than requesting only emails related to the subject matter of the litigation consistent with Fed. R. Civ. P. 45(d)(1), Kwasny "ordered production of "[a]ll copies of emails sent or received by anyone" at ICA, with no limitation as to time or scope."[50] NetGate responded by posting 339 messages on their website where Kwasny and Farey-Jones read them.[51] Most of them were unrelated to the litigation, while many were also privileged and personal.[52] This resulted in Wolf, Buckingham, and other affected ICA employees filing suit against Farey-Jones and Kwasny, which included an SCA claim.[53] In its analysis, the Ninth Circuit compared parties who knowingly take advantage of mistaken consent to trespass violations, in addition to assessing the earlier issued subpoena as being patently unlawful, and determined that Farey-Jones and Kwasny did access the emails without authorization.[54]

The court found that opened emails were in 'electronic storage' under section 2510(17)(B) and thereby subject to SCA protection.[55] The Ninth Circuit originated the arguments that reading subsections (A) and (B) of the "electronic storage" definition together contravenes basic grammar and renders subsection (B) superfluous.[56] With respect to the grammatical argument, the court asserts that because both subsections outline a type of communication and then a type of storage, "such communication" in subsection (B) is simply referencing "wire or electronic communication" in subsection (A), rather than the type of communication and the type of storage.[57] In other words, because the "incidental to the electronic transmission thereof" language modifies the noun "storage," it does not modify "wire or electronic communication."[58] The court also asserts, in making the superfluity argument, that a narrow interpretation of section

48. *Theofel*, 359 F.3d at 1071.
49. *Id.*
50. *Id.*; FED. R. CIV. P. 45(d)(1) (stating "A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense[.]")
51. *Theofel*, 359 F.3d at 1071.
52. *Id.*
53. *Id.* at 1072.
54. *Id.* at 1073-74.
55. *Id.* at 1075-77.
56. *Id.* at 1075-76.
57. *Id.*
58. *Id.*

2510(17)(B) renders subsection (B) superfluous because pre-transmission backup storage would be covered under subsection (A).[59]

2. Eighth Circuit in *Anzaldua v. Northeast Ambulance and Fire Protection Dist.* (2015) Presents the Opposing Arguments

Steven Anzaldua worked for the Northeast Ambulance and Fire Protection District as a full-time paramedic and firefighter.[60] The Fire District suspended Anzaldua for failing to respond to a directive given by Chief Kenneth Farwell regarding an email Anzaldua purportedly sent that had been forwarded from his email account to Chief Farwell.[61] After the suspension, Anzaldua sent another email expressing concerns with the department and Chief Farwell, and it was somehow forwarded from Anzaldua's Gmail account to Chief Farwell once again; his employment was subsequently terminated.[62] Anzaldua had given his password to his ex-girlfriend Kate Welge, later an employee at Chief Falwell's restaurant, for the sole purpose of sending out resumes on his behalf.[63] Anzaldua alleges that she either gave the password to Chief Falwell, or that she forwarded the relevant emails herself, which she deleted from the outbox, in violation of the SCA.[64] The Eighth Circuit found that Anzaldua had sufficiently alleged unauthorized access of his account, but dismissed the SCA claim because the emails were not in "electronic storage" within the meaning of the statute.[65] The court cited to opinions and commentators disagreeing with and differentiating *Theofel* regarding the breadth of the SCA's definition of "electronic storage."[66] The court also raised two primary arguments made against the broad interpretation. The first argument is that subsection (A) and (B) must be read together, meaning that "such communication" in subsection (B) only covers emails stored temporarily during transmission from sender to addressee.[67] The second argument is that "backup protection" implies that there must be an original email which the secondary email copy backs up; this means that an original opened email is not stored for the "purposes of backup protection."[68] The Eighth Circuit decided that sent email stored in due course

59. *Id.*
60. *See* Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 827-28 (8th Cir. 2015).
61. *Id.* at 828-30.
62. *Id.*
63. *Id.* at 838.
64. *Id.*
65. *Id.* at 839.
66. *See id.* at 841.
67. *See* Jennings v. Jennings, 736 S.E.2d 242, 248 (S.C. 2012) (Toal, C.J., concurring in the result); Kerr, *supra* note 36, at 1214.
68. *See* Lazette v. Kulmatycki, 949 F.Supp. 2d 748, 758 (N.D. Ohio 2013); *Jennings*, 736 S.E.2d at 245 (2012).

with a sender's ECS, rather than for a user's backup purposes as alleged by *Anzaldua*, does not fall under the SCA's definition of electronic storage.[69]

3. The Fourth Circuit in *Hately v. Watts* (2019) Comprehensively Addresses the Circuit Split

Patrick Hately brought an action alleging that David Watts unlawfully accessed messages in Hately's web-based Gmail inbox.[70] One of Hately's claims was that Watts had violated the SCA when he accessed Hately's emails using login and password information provided by an ex-partner.[71] Watts admitted that he browsed through Hately's emails, but insisted that he did not "change the status of, or modify, any email in anyway," and that he "did not open or view any email that was unopened, marked as unread, previously deleted, or in the 'trash' folder."[72] The Fourth Circuit held that opened emails are protected under section 2510(17)(B), meaning that Watts' actions did violate the statute.[73] This section will cover the court's plain meaning and superfluity arguments, as these were largely taken from the Ninth Circuit, while the remaining arguments will be addressed in the analysis section.

Assuming that section 2510(17) lays out two distinct types of storage, the court stated a need to inquire into whether opened emails fall into (1) storage "incidental to transmission," or (2) "backup" storage.[74] *Hately v. Watts* provides an ideal set of facts under which to analyze the unopened/opened discrepancy in SCA protection, as Watts insisted he exclusively viewed emails that had been opened previously.[75] With respect to the first category, the plain, dictionary meanings of temporary, "existing or continuing for a limited time," and intermediate, "lying or being in the middle," demonstrate that section 2510(17)(A) protects electronic communications for a limited time while they are in the middle of transmission to their final destination.[76] Previously delivered and opened emails are clearly no longer in the middle of transmission, which places them

69. *See Anzaldua*, 793 F.3d at 840-42.
70. *See* Hately v. Watts, 917 F.3d 770, 773 (4th Cir. 2019).
71. *Id.*
72. *Id.*
73. *Id.* at 797.
74. *See e.g. Hately*, 917 F.3d at 787; Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003); Strategic Wealth Grp, LLC v. Canno, No. CIV.A. 10-0321, 2011 WL 346592, at *3-4 (E.D. Pa. Feb. 4, 2011); Cornerstone Consultants, Inc. v. Prod. Input Sols., L.L.C., 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); Bailey v. Bailey, 2008 WL 324156, at *6 (E.D. Mich. 2008); Flagg v. City of Detroit; 252 F.R.D. 346, 362 (E.D. Mich. 2008).
75. *See Hately*, 917 F.3d at 774.
76. *See Temporary*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY (1961); *Intermediate*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY (1961); In re DoubleClick Inc. Priv. Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001).

outside the plain meaning of section 2510(17)(A), but that still leaves questions concerning the plain meaning of section 2510(17)(B).[77]

a. Plain Meaning of "Storage"

The Fourth Circuit properly broke section 2510(17)(B) down into four elements: any (1) storage of (2) such communication (3) by an electronic communication service (4) for the purposes of backup protection of such communication.[78] With respect to electronic storage, the court asserted "storage" should simply mean "reserved for future use."[79] Given the plain meaning and Congress speaking directly to the issue, the Fourth Circuit determined the same result as the Ninth Circuit finding that prior access is irrelevant to whether an email is in storage.[80] When an email user opens an email and then decides to keep the message in their inbox rather than delete it, the message remains "reserved for future use" by the user.[81] In the alternative, email services also "reserve for future use" the relevant communication in case the user needs to subsequently access it or they experience technical issues.[82] In either case, opened emails fall under the section 2510(17)(B) definition of electronic storage.

b. Arguments Regarding the Plain Meaning of "Such Communication" and the Superfluity Doctrine

In the discussion of the "such communication" language, the Fourth Circuit largely adopts the Ninth Circuit's argument regarding the subsections, outlining two discrete types of protected electronic storage. Specifically:

---

77. *See* United States v. Councilman, 418 F.3d 67, 81 (1st Cir. 2005) (holding that Subsection (A) "refers to temporary storage, such as when a message sits in an email user's mailbox after transmission but before the user has retrieved the message from the mail server"); *Theofel*, 359 F.3d at 1075; *Fraser*, 352 F.3d at 114 (holding that an email in "post-transmission storage" was "not temporary, intermediate storage").

78. Stored Communications Act, 18 U.S.C. § 2510(17)(B); *see Hately*, 917 F.3d at 786.

79. *Store*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (5th ed. 2018).

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

81. *See Theofel*, 359 F.3d at 1077; Cheng v. Romo, No. CIV.A. 11-10007-DJC, 2013 WL 6814691, at *7-9 (D. Mass. Dec. 20, 2013) (holding that copies of delivered and opened emails accessed through a web-based email client were in "storage" for purposes of Subsection (B)); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) ("The majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service's systems after it has been delivered … is a stored communication subject to the SCA."); Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *5-6 (E.D. Mich. Feb. 6, 2008) ("The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service.").

82. *See Hately*, 917 F.3d at 786.

> 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).[83]

The phrase "temporary, intermediate … incidental to the electronic transmission thereof" modifies the noun "storage," but does not modify the noun "communication"—the term referred to in subsection (B).[84]

As the statute is written, "such communication" is then simply an easy way to reference "wire or electronic communication," meaning the statute does cover post-transmission, opened emails.[85]

In addition to the Fourth Circuit's grammatical analysis,[86] the court argues a narrow interpretation excluding opened emails would also render section 2510(17)(B) superfluous.[87] Courts should generally avoid an interpretation that renders a clause, sentence, or word "inoperative … void, superfluous, or insignificant."[88] In theory, if "such communication" were read to only encompass wire or electronic communications in "temporary, intermediate storage," subsection (B) would become superfluous because temporary backup storage pending transmission would already be in "temporary, intermediate storage… incidental to the electronic transmission thereof" within the meaning of subsection (A).[89]

However, the broad interpretation of the statutory language has not been universally accepted. For example, Judge Toal of the South Carolina Supreme Court asserted that the two statutory provisions, section 2510(17)(A) and (B), must be read together.[90] Judge Toal emphasized the statute's use of the word "and," rather than "or," at the end of subsection A to support this argument, asserting that the Fourth Circuit's reading would essentially provide two definitions for "electronic storage" when the term is meant to subsume both subsections.[91] Under this reading, "electronic storage" would refer "only to temporary storage, made in the course of transmission,

---

83. *Hately*, 917 F.3d at 787, *citing Theofel*, 917 F.3d at 1076.
84. *Hately*, 917 F.3d at 787.
85. *Id.*
86. *Id.*
87. *Id.*
88. *See* Panjiva, Inc. v. U.S. Customs & Border Prot., 342 F. Supp. 3d 481, 490 (S.D.N.Y. 2018) ("[C]ourts must give effect to all of statute's provisions so that no part will be inoperative, void or insignificant.") (citing *United States v. Harris*, 838 F.3d 98, 106 (2d Cir. 2016)).
89. *See Hately*, 917 F.3d at 787 (citing *Theofel*, 359 F.3d at 1075-76 ("Were we to construe "such communication" as encompassing only wire or electronic communications in "temporary or intermediate storage," Subsection B would be rendered "essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as 'temporary or intermediate storage' within the meaning of [S]ubsection A.")).
90. Jennings v. Jennings, 736 S.E.2d 242, 247-48 (S.C. 2012) (Toal, C.J., concurring in the result).
91. *Id.*

by an ECS provider, and to backups of such intermediate communications," excluding opened emails.[92] This interpretation also finds support from the Department of Justice and other commentators.[93]

c. Arguments Regarding the Plain Meaning of "Purposes of Backup Protection"

Having already addressed that "electronic communication service" includes both email clients and webmail,[94] the plain meaning interpretation of "for the purposes of backup protection," which has generated the most legal controversy, will be addressed next. The term "backup protection" is not defined in the statute and the Fourth Circuit properly turned to the dictionary meaning of the statutory definition's language. The court defined "backup" as a copy of computer data, and "protection" as the act of covering or shielding from exposure, injury, damage, or destruction.[95] A wire or electronic communication is therefore stored for "purposes of backup protection" if it is a copy of the communication stored to prevent destruction or damage.[96] Copies of previously delivered and opened emails retained on the servers of email service providers fall within this reading of section 2510(17)(B). The primary argument made against this plain meaning interpretation of "backup protection" is that the plain meaning of the term implies the existence of an original copy and a backup copy.[97] Under this understanding of the statutory language, the opened email, as the original copy, cannot be stored for the "purposes of backup protection."[98]

III. ANALYSIS

This section will first argue that the Fourth Circuit's arguments favoring its plain meaning interpretation of the statutory language are far

92. *Id.*

93. *See* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 125 (3d ed. 2009); Kerr, *supra* note 36, at 1216.

94. *See, e.g.*, Vista Mktg., LLC v. Burkett, 812 F.3d 954, 963-64 (11th Cir. 2016) (holding that the defendant "qualified as an [electronic communication service] because it was a service that provided employees with the ability to send and receive electronic communications, including emails"); Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (holding that the definition of electronic communication service "covers basic e-mail services"); In re United States for an Ord. Pursuant to 18 U.S.C. § 2705(b), 289 F. Supp. 3d 201, 209 (D.D.C. 2018) (holding that online booking company was an electronic communications service for the purposes of a dispute related to disclosing messages from the company's "user-to-user electronic messaging system").

95. *See* Hately v. Watts, 917 F.3d 770, 791 (4th Cir. 2019); *Backup*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/backup [https://perma.cc/RCW8-5SCS]; *Protection*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/protection [https://perma.cc/86FA-U5BQ].

96. *Id.*

97. *See* Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013); Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012).

98. Electronic Communications Privacy Act, 18 U.S.C. § 2510(17)(A), (B).

more compelling than those of the dissenting voices. Following this discussion, the analysis will cover the legislative history of the SCA and the absurd results created by the narrow interpretation of section 2510(17)(B). Next, this Note will analyze the Fourth Circuit's key interpretive innovations, and address counterarguments further. The analysis will then look to policy considerations that strongly point towards the broader reading of section 2510(17)(B). Finally, this analysis will conclude by presenting alternative solutions to the circuit split and the inconsistent application of this SCA language across jurisdictions.

A. The Fourth Circuit Settles Differences in the Interpretation of Section 2510(17)(B) Among Courts

1. Reading Section 2510(17)(A) and (B) Together Does Not Make Grammatical Sense and Does Create a Superfluity Issue

The argument that the two subsections must be read together contravenes basic grammar principles and does not resolve the superfluity issue, consistent with the Fourth Circuit's argument. Subsection (A) outlines a type of storage, "temporary, intermediate . . . incidental to the electronic transmission thereof," and a type of communication, "wire or electronic."[99] Common sense dictates that subsection (B) should be read the same way, with the type of storage being "any storage . . . by an electronic communication service for the purposes of backup protection," and the communication being "such communication" as a reference to "wire or electronic" from the previous subsection.[100] "Such communication" was just an easy way to reference the previously used "wire or electronic communication" language.[101] Also, the language "temporary, intermediate . . . incidental to the electronic transmission thereof" in the first subsection simply does not refer to the type of communication used in the subsection, when its purpose is to modify the type of storage.[102] Additionally, if Congress had intended this language to carry over into subsection (B), they certainly could have said so explicitly rather than leaving the answer ambiguous. Furthermore, Judge Toal's argument, mentioned in Part II, Section C of this Note, overemphasizes the importance of the word "and."[103] The word "and" does not preclude subsection (B) from outlining a different kind of electronic storage under the same definition. It is not uncommon for statutory definitions to include more than one category under the umbrella of one term.

99. *Id.*
100. *Id.*
101. *Id.*
102. Hately v. Watts, 917 F.3d 770, 787 (4th Cir. 2019).
103. *See* Jennings v. Jennings, 736 S.E.2d 242, 247-48 (S.C. 2012); U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 125 (3d ed. 2009); Kerr, *supra* note 36.

Reading the subsections together, or, rather, inserting subsection (A) language into subsection (B), also creates a major superfluity issue. If the definition in subsection (B) is read to refer to "any storage . . . for the purposes of backup protection," but only "incidental to the electronic transmission thereof," subsection (B) is stripped of independent meaning.[104] If an email is stored for backup protection before the email has been delivered, this would be precisely "any temporary, intermediate storage . . . incidental to the electronic transmission thereof" language from subsection (A).[105] This alternative reading violates the canon of surplusage by making subsection (B) completely unnecessary.[106] A statute should not be interpreted in such a way that congressionally drafted language is left without a purpose.[107] Some commentators claim subsection (B) was added in order to clarify that permanent or semi-permanent copies of communications made by ISPs back in 1986 during transmission do not lose strong SCA protection from cybercriminals and from government overreach, hence the insertion of the "temporary, intermediate . . . incidental to the transmission thereof" language into subsection (B).[108] However, subsection (A) can be easily interpreted to cover this form of storage "incidental to the transmission thereof," truly making subsection (B) superfluous under the narrow interpretation of section 2510(17)(A) and (B).[109] Also, given how much faster Internet connections have become and the advancements in cloud storage,[110] the question remains: how many copies of emails are made intermediately during transmission from place to place, rather than by the webmail providers of the sender and recipient upon being sent and received? Even if Congress's intention was to clarify subsection (A) protections, the usefulness of this subtle clarification has disappeared. For these reasons, the Fourth Circuit's arguments demonstrate that these two subsections should not be read together by inserting subsection (A) language into subsection (B), and that the definition

104. *See Hately*, 917 F.3d at 787 (citing *Theofel*, 359 F.3d at 1075-76 ("Were we to construe "such communication" as encompassing only wire or electronic communications in "temporary or intermediate storage," Subsection B would be rendered "essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as 'temporary or intermediate storage' within the meaning of [S]ubsection A.")).

105. Electronic Communications Privacy Act, 18 U.S.C. § 2510(17)(A).

106. *See* Panjiva, Inc. v. U.S. Customs & Border Prot., 342 F. Supp. 3d 481, 490 (S.D.N.Y. 2018) (citing *United States v. Harris*, 838 F.3d 98, 106 (2d Cir. 2016)).

107. *Id.*

108. Kerr, *supra* note 36, at 1217 n.61.

109. Electronic Communications Privacy Act, 18 U.S.C. § 2510(17)(A).

110. Antonio Villas-Boas, *'Red Dead Redmption 2' Would Have Taken Almost 48 Hours to Download a Decade Ago – Here's How Far Internet Speeds Have Come*, BUS. INSIDER (Nov. 5, 2019), https://www.businessinsider.com/internet-speeds-have-gotten-dramatically-faster-over-past-decade-2019-11#:~:text=Indeed%2C%20as%20more%20of%20us,%2Dtesting%20site%20Speedtest.net ("Average internet speeds in American homes grew from around 5 Mbps in 2009 to 96.25 Mbps in 2018…") [https://perma.cc/W3MV-ZZVS]; *The Dawn of the Cloud*, MINDFIRE TECHNOLOGIES (June 23, 2018), https://www.mindfireit.com/cloud-computing/the-dawn-of-the-cloud/ ("Public cloud adoption in recent years is expected to reach a whooping £197 billion ($274 billion) in spending within just three years…").

of "electronic storage" in section 2510(17)(B) does in fact lay out two discrete forms of storage.

2. The Distinction Between an Original Email and a Copy Does Not Undermine the Broad Interpretation of "Backup Protection"

The other argument made against the broad reading of "backup protection," that the terminology only applies to copies retained in case the "original" email is rendered unusable, thereby presupposing the existence of an "original" email, also fails under closer scrutiny.[111] The logic is that emails opened by email users are the originals, rather than copies, and retaining this original for future viewing does not fall within the meaning of "for the purposes of backup protection."[112] However, the true original under this analysis would be the email typed in the sender's email service, while copies of this original would then be transmitted to the recipient's email service.[113] The recipient's email service never receives nor stores this true original.[114] Every copy held by the recipient email service would then be a copy of the true original, undermining this line of argument. Even if opened emails that a user decides to keep were interpreted to be an "original," this would still fall under the "backup protection" definition because of the redundancy built into the systems of these services, which will be discussed subsequently.[115]

B. Congress's Intent in Passing the Stored Communications Act and the Absurdity Doctrine

To the extent the SCA's legislative history articulates Congress's purpose in enacting the SCA, the House and Senate reports clearly point towards broader protections for email communications.[116] The SCA was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy via illicit access to "stored communications in remote computing operations and large data banks that stored e-mails."[117] To Congress, this legal uncertainty created potential problems in a number of areas.[118] First, the

111. *See, e.g.*, Cobra Pipeline Co. v. Gas Natural, Inc., 132 F. Supp. 3d 945, 952 (N.D. Ohio 2015) (holding the term "stored for backup purposes" does not encompass "primary" copies); Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013); Jennings v. Jennings, 736 S.E.2d 242, 250 (S.C. 2012) ("Congress's use of 'backup' necessarily presupposes the existence of another copy to which this e-mail would serve as a substitute or support.").

112. *See* Hately v. Watts, 917 F.3d 770, 796 (4th Cir. 2019).

113. *Id.*

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

115. *See infra* notes 143-148.

116. *See* King v. Burwell, 135 S. Ct. 2480, 2496 (2015) ("[A] fair reading of legislation demands a fair understanding of the legislative plan."); *Hately*, 917 F.3d at 782-83.

117. *See* H.R. REP. NO. 99-647, at 18 (1986); S. REP. NO. 99-541, at 2 (1986).

118. *See* H.R. REP. NO. 99-647, at 19.

former uncertainty surrounding legal protections afforded to electronic communications "promote[d] the gradual erosion of the precious right [to privacy]."[119] This potential for erosion connects to the negative sentiment Americans have about their privacy and to a potential restoration of agency through expanding the circumstances under which a civil action can be brought under the private right of action. Second, it "unnecessarily discourage[d] potential customers from using innovative communications systems."[120] This aligns closely with the concept that current uncertainty rooted in the circuit split can discourage people from opening their emails unless absolutely necessary. Third, the former legal uncertainty "encouraged unauthorized users to obtain access to communications to which they are not a party."[121] This concern clearly lines up with the issue of limited protections emboldening cyber-criminals and identity thieves when they can easily avoid liability for unauthorized access of email accounts. The three primary issues Congress sought to address in passing this legislation, issues which still exist today, are better served by interpreting the statutory language broadly to protect opened emails, rather than by leaving these emails vulnerable to cybercriminals. In fact, the narrow interpretation fatally clashes with Congress's intent.

Congress's discussion of the issues involved points to the need to protect the privacy and security of emails, regardless of whether someone has opened them previously. In addition, the Office of Technology Assessment, in a report cited extensively throughout the House and Senate reports, also emphasized the lack of legal protection for email.[122] The report identified "stages at which an electronic message could be intercepted and its contents divulged to an unintended receiver," critically including messages "in the electronic mailbox of the receiver" as one of these stages.[123] Given this evidence, to protect unopened and opened emails differently under the SCA is an absurd result that Congress almost certainly did not intend, as the Fourth Circuit asserts.[124] The absurdity of this result only grows when one recognizes that opened emails tend to have more sensitive personal or business information than emails the user never even viewed, including spam. In the words of the Fourth Circuit, "[i]t 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."[125] From the United States' earliest days,

119. *Id.*

120. S. REP. NO. 99-541, at 5; *see* H.R. REP. NO. 99-647, at 19.

121. *Id*

122. *See* S. REP. NO. 99-541, at 3 (quoting OFF. OF TECHNOLOGY ASSESSMENT, OTA- CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 44 (1985)); H.R. REP. NO. 99-647, at 18 (quoting OFF. OF TECHNOLOGY ASSESSMENT, OTA- CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 44 (1985)).

123. OFF. OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 45 (1985).

124. *See* Hately v. Watts, 917 F.3d 770, 798 (4th Cir. 2019).

125. *Id.*

the Supreme Court and lower courts have subscribed to the idea that judges may deviate from even the clearest statutory texts when a given application would produce otherwise absurd results, as is the case here.[126]

1. The Legislative History's Description of Email Communications in 1986 Provides Support for the Broad Interpretation of Section 2510(17)(B)

While some courts, including the Eighth Circuit, have asserted that the SCA enacted in 1986 is often difficult to reconcile with modern email services,[127] the common form of email outlined in the SCA's legislative history bears many similarities to modern webmail.[128] For example, the Senate Report used the following language:

> [M]essages are typed into a computer terminal, then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer 'mailbox' until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer.[129]

Similarly, modern webmail services have senders from one service transmit a message to the recipient's webmail service.[130] The webmail service then stores the messages on a cloud server until the recipient retrieves it through an Internet connection on a browser, mobile application, or email client.[131] Congress's understanding of email in 1986 could apply to webmail simply by replacing "telephone lines" with 'internet connection.'[132]

Congress also seems to explicitly envision protection for emails in inboxes, opened or unopened, in the legislative history. For example, "[a]n 'electronic mail' service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to Section 2701."[133] In modern parlance, emails stored on a webmail provider's servers until someone opens their inbox to view those emails closely aligns with this language. The House Report provides very little evidence that Congress intended to limit section 2701's protections to the period before a recipient opens an email.[134] The Senate Report notes that

126. John F. Manning, *The Absurdity Doctrine*, 116 HARV. L. REV. 2387, 2388 (2003).
127. *See* Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 839 (8th Cir. 2015) ("It is not always easy to square the decades-old SCA with the current state of email technology.").
128. *See Hately*, 917 F.3d at 792.
129. S. REP. NO. 99-541, at 8 (1986).
130. *See Hately*, 917 F.3d at 792.
131. *Id.*
132. S. REP. NO. 99-541, at 8.
133. H.R. REP. NO. 99-647, at 63 (1986).
134. *See Hately*, 917 F.3d at 793.

"a computer mail facility authorizes a subscriber to access information in their portion of the facilit[y]'s storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of the [SCA]."[135] Here, the cloud as supported by a webmail provider's servers matches up closely with "computer mail facility."[136] This report also does not draw a distinction between the periods before and after a user first views a message.[137] Technology may have advanced significantly, but email still works similarly enough to reconcile how Congress understood email in 1986 with modern email services. This again points to the unopened/opened divide in legal protections being an unnecessary, judicially created distinction contravening Congress's intent.

C. The Fourth Circuit's Key Interpretive Innovations

The Fourth Circuit's key interpretive innovations in *Hately*, compared to the Ninth Circuit's opinion in *Theofel*, should make the more recent opinion's advocacy for a broad reading of section 2510(17)(B) and protecting opened emails under the SCA a definitive next step for courts. Most importantly, *Hately* recognizes that modern email services create any number of backup copies of a given email for their own purposes and those of a user: meaning that an opened email is just another copy made for the "backup purposes" of both the email service and the user.[138] The court also directly addressed the counterargument to the broad reading of section 2510(17)(B) that "backup protection" only refers to messages stored for the purposes of the email service.[139]

1. Mass Data Redundancy Maintained by Email Service Providers Should Control the Interpretation of Section 2510(17)(B)

One of the weaknesses of the Ninth Circuit's *Theofel* ruling is that it was decided in the context of an email client before webmail had gained widespread adoption.[140] The Fourth Circuit, on the other hand, brings the broad reading of section 2510(17)(B) into the modern era in its discussion of the email services provided today. The *Hately* ruling both acknowledges and incorporates the reality of modern email services. Specifically, the court recognizes that services such as Gmail or Outlook typically "utilize completely redundant systems consisting of multiple data servers."[141] In these systems, a single email is stored on multiple servers, likely in different

135. S. REP. NO. 99-451, at 36.
136. *Id.*
137. *See Hately*, 917 F.3d at 793.
138. *Id.* at 793-94.
139. *See infra* notes 150-57.
140. *See generally* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).
141. Brief for the Center for Dem. & Technology et al. as Amicus Curiae Supporting Plaintiff-Appellant and Reversal at 22, Hately v. Watts, 917 F.3d 770 (4th Cir. 2019).

locations around the country, or even around the world.[142] Email services store copies of messages on multiple servers to decrease email downtime and prevent loss of information from servers.[143] For email services, each copy of an email message serves as a substitute for the many other copies stored by the service.[144] Furthermore, when a recipient of an email chooses to view the email via a web browser or application on some device, a copy of the message is sent to the user's device and temporarily stored in the device's short-term or long-term memory.[145] For this reason, the copies retained by the email service also provide backups for any copies downloaded to a physical device and vice versa.[146] In light of this redundancy and the plain meaning of backup protection being to protect computer data from damage or destruction, the argument that unopened emails are stored for the "purposes of backup protection," but opened emails are not, strains credulity. Using the Eighth Circuit's understanding of the statutory language in *Anzaldua*, the emails are stored in due course *and* for the purposes of backup protection by email service providers.[147]

2. "Backup Protection" Does Not Just Apply to Copies Made for the Service Provider's Purposes

One argument made against the broad interpretation of "backup protection"—that this language exclusively covers copies made for the service provider's own administrative purposes rather than also covering copies made for a user's purposes—does not pass analytical muster.[148] Theoretically, this reading would exclude opened emails, as these would be considered copies made solely for the user's purposes when the user decided not to delete them. This argument is based on the assertion that section 2704's

142. *See Id.*

143. *See Id.*

144. *See id.*; *see also Reliability*, GOOGLE CLOUD HELP, https://support.google.com/googlecloud/answer/6056635?hl=en (last visited Feb. 6, 2021) ("[A]ll Google systems are inherently redundant by design, and each subsystem is not dependent on any particular physical or illogical server for ongoing operation. Data is replicated multiple times across Google's clustered active servers so that, in the case of machine failure, data will still be accessible through other systems."); Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECHNOLOGY L. 359, 361 (2010) ("Cloud computing services provide consumers with vast amounts of cheap, redundant storage and allow them to instantly access their data from a web-connected computer anywhere in the world.").

145. *See* Hately v. Watts, 917 F.3d 770, 792 (4th Cir. 2019).

146. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004); Cheng v. Romo, No. 11-10007-DJC, 2013 WL 6814691, at *7-9 (D. Mass. 2013) (holding that copies of delivered and opened emails accessed through a web-based email client were in "storage" for purposes of Subsection (B)); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008); Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *5-6 (E.D. Mich. 2008) ("The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service.").

147. *See* Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 840-42 (8th Cir. 2015).

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

definition of backup copy, "a copy made by the service provider for administrative purposes," should be interchangeable with that of "backup protection."[149] However, section 2704 reads in full that the government "may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of contents of the electronic communications sought in order to preserve communications."[150] The term "backup copy" in the context of section 2704 then refers to copies of electronic communications created by a service provider pursuant to a court order, rather than copies made during an email service's day-to-day operations. Also, nothing in the SCA's definition of "electronic storage," section 2704, or the statute's legislative history provides support for the argument that Congress intended for "backup protection" and "backup copy" to have the same meaning.[151]

Even assuming that "backup protection" does only refer to copies made for the service provider's own administrative purposes, opened emails would still fall under this definition because of the redundancy discussed above.[152] "Administrative" simply means "relating to the running of a business, organization, etc."[153] Numerous copies of emails are created for the administrative purposes of decreasing email downtime, protecting against data loss, and advertisement targeting.[154] Therefore, even under this more restrictive definition of "backup protection," copies made by the service provider of both unopened and opened emails are made for administrative purposes under the "backup copy" definition from section 2704. However, this insertion of section 2704's definition of "backup copy" into section 2510(17)'s definition of "electronic storage" does not make sense. Furthermore, nothing in the SCA requires that "backup protection" be solely for the benefit of the email service provider, while conversely, the legislative history expressly envisions "backup protection" for the benefit of the user.[155]

D. Policy Considerations

1. Unopened/ Opened Distinction as an Unreliable Proxy for the Receipt of Email Communications

Because modern email services have a feature that enables a user to mark an email as read or unread, the unopened/opened distinction advocated by some courts and commentators becomes even more arbitrary, and possibly

149. Kerr, *supra* note 36, at 1217.

150. Stored Communications Act, 18 U.S.C. § 2704(a)(1).

151. *See Hately*, 917 F.3d at 794.

152. *Id.*; *see supra* Part III, Section C1.

153. *Administrative*, Meriam-Webster.com, https://www.merriam-webster.com/dictionary/administrative [https://perma.cc/VS2S-URY9].

154. Brief for the Center for Dem. & Technology et al. as Amicus Curiae Supporting Plaintiff-Appellant and Reversal at 22, Hately v. Watts, 917 F.3d 770 (4th Cir. 2019).

155. *See* H.R. NO. 99-647, at 68 (1986) (noting "[b]ackup protection preserves the integrity of the electronic communication system and to some extent preserves the property of users of such a system.").

unworkable. Under the narrow reading of section 2510(17)(B), opened emails do not fall under the SCA's definition of electronic storage because their storage is not incidental to the transmission of that message.[156] Essentially, once the email message has been opened, it no longer falls under this interpretation's understanding of electronic storage because the communication is complete, received, and no longer stored "incidental to the electronic transmission thereof."[157] However, if protections under the law are supposed to turn on this distinction, raising the ability to mark emails as read or unread as a defense would require courts to perform an inquiry into whether emails were actually opened, instead of simply being marked as read. Alternatively, an email could have been opened and then marked as unread by the user. Otherwise, courts ascribing to this interpretation would not know the truth of whether the transmission of the email had actually been completed under their own standard. Furthermore, cybercriminals and hackers could simply mark an unopened email that they opened as unread to cover their tracks, potentially requiring further investigation by courts.

The unopened/opened distinction can raise serious judicial efficiency issues if most section 2701 cases involving email would require forensic analysis of metadata by Google or Microsoft employees to determine whether this feature was used to distort the relevant facts under what is already an arbitrary, absurd interpretation. The email service provider may not retain this data indefinitely or may not have the capability to perform analysis with the granularity required to differentiate actions taken by the user from those of a cybercriminal using their username and password. This process could also substantially increase litigation costs, depending on whether an email service can proffer this information or whether further experts would need to be brought in. The very first rule of the Federal Rules of Civil Procedure outlining their scope and purpose focuses on securing just, speedy, and inexpensive determinations of every action or proceeding.[158] From a policy perspective, interpreting section 2510(17)(B) narrowly to exclude previously opened emails directly contravenes the goal of both speedy and inexpensive determinations.

2. Holding Cybercriminals Accountable, Making Americans Feel Safer and More in Control of Their Personal Data, and Providing Standing for Victims of Certain Data Breaches

Other practical policy considerations also weigh heavily in favor of the broad interpretation of section 2510(17)(B). Holding a cyber-criminal accountable for accessing your emails, unopened and opened, prior to full-fledged identity theft or other fraud, is a substantial government interest consistent with the SCA's intended purpose: to address the growing problem of unauthorized persons deliberately gaining access to electronic

156. Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 842 (8th Cir. 2015).
157. Kerr, *supra* note 36, at 1216.
158. FED. R. CIV. P. 1 (last amended Dec. 1, 2015).

communications not intended for the public.[159] Protecting email inboxes more thoroughly can also contribute to more positive views of data security by making citizens feel safer, or, at a minimum, to restore some agency by expanding the SCA's private right of action. Another practical rationale for this form of protection is the difficulty data breach plaintiffs face in demonstrating Article III standing, in particular, the injury-in-fact element, following *Clapper v. Amnesty International*.[160] Taking a broader view on inbox protections can enable victims of hacks, including those affected by the Yahoo incident, to hold wrongdoers accountable for their efforts to take personal or business data from inboxes, despite some divided authority on whether actual damages are a prerequisite for awarding statutory damages.[161]

3. The Supreme Court Should Grant Certiorari or Congress Should Amend the SCA

Although widespread adoption of the *Hately* decision's broad interpretation of section 2510(17)(B) is a starting point for consistent application of the relevant statutory language, the depth of the circuit split and the sheer number of courts that have weighed in on the issue may make this adoption difficult. For this reason, the Supreme Court should take up a case involving the unopened/opened divide concerning SCA protections to resolve the circuit split once and for all. Some such cases have been appealed to the Supreme Court, including *Jennings v. Jennings*, but certiorari has never been granted.[162] In the alternative, Congress should update and amend the SCA to clearly protect opened emails. Congress could also take steps to protect email inboxes even further by removing the outdated "facility" language, which does not protect against someone simply accessing your email account through your personal device, from any subsequent proposed legislation.[163]

IV. CONCLUSION

Congress passed the SCA to fill gaps in legal protections for electronic communications and the resulting legal uncertainties.[164] Although technology has developed rapidly in the last thirty-five years, Congress's discussion of email services in 1986 bears striking resemblance to modern webmail.[165] The arbitrary distinction between the protections afforded to unopened and opened emails is an absurd result Congress almost certainly did not intend, even back

159. H.R. REP. NO. 99-647, at 62.

160. *See* Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1140-1141 (2013) (holding speculative, future harms do not establish Article III standing).

161. *See supra* notes 29-30.

162. Jennings v. Jennings, 736 S.E.2d 242, 250 (S.C. 2012), *cert. denied sub nom.* Jennings v. Broome, 133 S. Ct. 1806, 1806 (2013).

163. *See generally* Electronic Communications Privacy Act, 18 U.S.C. § 2701(a).

164. *See supra* Part III, Section B.

165. *See supra* Part III, Section B1.

in 1986.[166] The jurisprudential influence of the Ninth Circuit's *Theofel* decision is inhibited by its discussion of traditional email clients, rather than webmail, and its failure to respond to some of the key arguments against the broad reading of section 2510(17)(B). The Fourth Circuit's *Hately* decision resolves both issues while accounting for other facets of modern technology. Most importantly, the *Hately* decision recognizes the reality of mass email redundancy within the systems of email service providers and the impact this has on the interpretation of "for the purposes of backup protection."[167] Furthermore, the ability to mark an email as read or unread may make the unopened/opened distinction advocated by some courts and commentators unworkable if this were to be raised as a defense. In the meantime, Americans face uncertainty in the protection of their email inboxes which leaves them vulnerable to cybercriminals and identity theft. Courts across the country should adopt the Fourth Circuit's interpretation of section 2510(17)(B) of the SCA which protects opened emails because of the comprehensive nature of the court's arguments regarding the statute's plain text, legislative history, the absurdity doctrine, the superfluity doctrine, and technological developments, as well as common sense and independent policy considerations. The last thirty-five years have seen technologies, including email communications, evolve and develop at an unprecedented rate. Given the compelling arguments made by the Fourth Circuit and the important policy considerations discussed above favoring the broad reading of section 2510(17)(B), opened emails should be and must be protected under the Stored Communications Act.

166. *See supra* Part III, Section B.
167. *See supra* Part III, Section C1.