UIC John Marshall Journal of Information Technology & Privacy Law

Volume 30
Issue 1 *2013*

Article 5

2013

How Far Can the Government's Hand Reach Inside Your Personal Inbox?: Problems With the SCA, 30 J. Marshall J. Info. Tech. & Privacy L.75 (2013)

Dana T. Benedetti

COMMENTS

HOW FAR CAN THE GOVERNMENT'S HAND REACH INSIDE YOUR PERSONAL INBOX?: PROBLEMS WITH THE SCA

DANA T. BENEDETTI*

I. INTRODUCTION

Imagine that the police believe you are involved in some type of criminal activity and that rummaging through your personal inbox will yield incriminating evidence of the crime.[1] So without telling you,[2] they force your internet service provider ("ISP"), for example Gmail or Yahoo, to hand over all of the emails you have received or sent that have anything to do with their suspicion of you.[3] After reading up to hundreds or thousands of your email messages,[4] the police plan to use any incriminating evidence against you in your soon-to-become criminal trial. Now is the first time you find out that the police have been watching you, and that they have been doing this without first having obtained a warrant.[5] At your trial, you argue that the police invaded your individual privacy and that they should not be allowed to use that incriminating evidence against you.[6] Unfortunately for you, the emails are admitted into evidence, the jury finds you

---

* J.D. Candidate, The John Marshall Law School, May 2014; Candidacy Editor, Journal of Information Technology & Privacy Law; Trial Team Member, Trial Advocacy & Dispute Resolution Honors Council; B.A., Law & Society, Purdue University, May 2011; B.A., Psychology, Purdue University, May 2011.

1. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (holding that government agents violated the defendant's Fourth Amendment rights by compelling his Internet Service Provider to turn over his emails, after suspecting he was involved in criminal activity, without first obtaining a search warrant based on probable cause).
2. *See id.* at 283.
3. *See id.*
4. *See id.*
5. *See id.*
6. *See* United States v. Warshak, 631 F.3d 266, 281 (6th Cir. 2010).

guilty, and you are now criminally convicted of those crimes.[7] You do not think this is fair? Neither did Steven Warshak ("Warshak") when he was in this same situation in October 2004.

The problem today lies in the unanswered question: how much privacy should be awarded to stored emails? Before addressing this question, it is important to first understand how privacy is viewed under the Fourth Amendment. The right to privacy is a fundamental human right and is reflected in the Bill of Rights of our Constitution.[8] The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[9] requiring that warrants be issued only upon a showing of probable cause and specifying "the place to be searched, and the persons or things to be seized."[10] The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."[11]

In order to fall under the protection of the Fourth Amendment, courts consistently apply the "reasonable expectation of privacy" standard.[12] This standard requires that people have both a reasonable[13] objective and subjective expectation of privacy.[14] For the past forty years, this test has helped courts conclude that certain mediums of traditional communication, including telephone conversations[15] and

---

7. *See id.*

8. U.S. CONST. amend. IV; *see* Casey Perry, Note, *U.S. v. Warshak: Will Fourth Amendment Protection be Delivered to Your Inbox?*, 12 N.C. J.L. & TECH. 345, 345 (2011) (noting that although the United States Constitution does not contain an explicit right to privacy, the courts have established there is an implicit right to privacy, as many of the first ten amendments in the Bill of Rights protect particular aspects of individual privacy).

9. U.S. CONST. amend. IV.

10. *Id.* "While some 'highly cherished freedoms, such as those relating to speech, religion, press and trial by jury were lumped in together with others,' the prohibition against unreasonable searches and seizures was considered important enough to constitute a single amendment." Perry, *supra* note 8, at 346 fn. 2 (citing Charles A. Reynard, *Freedom from Unreasonable Search and Seizure – A Second Class Constitutional Right?*, 25 IND. L.J. 259, 273 (1950)).

11. *Warshak*, 631 F.3d at 283.

12. *See* Katz v. United States, 389 U.S. 347, 347 (1967).

13. *See* Perry, *supra* note 8. "The language of the Fourth Amendment makes it clear that the founders intended to limit the use of searches and seizures to those that are reasonable." *Id.* at 346.

14. *See Katz*, 389 U.S. at 347.

15. *See id.* at 353 (holding that the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means); *see also* Smith v. Maryland, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting) ("[S]ince Katz, it has been abundantly clear that telephone conversations are fully protected by the Fourth and Fourteenth Amendments.").

postal letters,[16] are constitutionally protected by a reasonable expectation of privacy. The effects of these decisions require that law enforcement or governmental agents must obtain a valid warrant based on probable cause before searching and ultimately seizing these communications.[17]

Yet, these dated Supreme Court decisions do not answer the question of whether this protection extends to electronic communications, specifically emails. Furthermore, if emails are protected, the next question remains what procedural requirements the government must satisfy before it is justified in violating this constitutionally protected right to privacy. The Supreme Court has yet to rule on this issue. However, on December 14th, 2010, the Sixth Circuit Court of Appeals was the first and only federal appellate court to address the applicability of the Fourth Amendment protection to stored emails in the landmark case of *United States v. Warshak*.[18] The Sixth Circuit held that the reasonable expectation of privacy for communications via telephone and postal mail extends to stored emails, bringing this modern medium of communication within the protection of the Fourth Amendment.[19] The court concluded that the action of the government compelling Warshak's internet service provider ("ISP") to hand over the contents of his emails without a valid warrant was unconstitutional.[20] Nonetheless, the court agreed that the government had relied in good faith on the language of the Stored Communications Act ("SCA"), so reversal of Warshak's criminal conviction was unwarranted.[21]

While this decision was an important first step in determining the future of privacy in electronic communications in our current and modern information age, there still remains crucial questions regarding the efficiency and effectiveness of our current federal privacy laws. Such questions pertain to issues relating to the government's ability to search and seize stored electronic communications and the proper

---

16. *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (holding that letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy).

17. *See, e.g.*, *id.* ("Warrantless searches of [the general class of effects in which the public at large has a legitimate expectation of privacy] are presumptively unreasonable.").

18. *See generally* Unites States v. Warshak, 631 F.3d 266 (6th Cir. 2010); *see also* Perry, *supra* note 8, at 348.

19. *Warshak*, 631 F.3d at 288.

20. *Id.* at 282.

21. *Id.*

balance between governmental need to investigate crimes and the societal need to protect personal privacy.[22]

The purpose of this Comment is to demonstrate that our current procedural provisions regulating electronic communications under the Stored Communications Act[23] are unconstitutional to the extent that they make outdated and arbitrary distinctions that lead to illogical results regarding how much privacy protection is afforded to, arguably, functionally equivalent forms of communication. Part II of this Comment will introduce the background law on Fourth Amendment privacy protections and its application in the context of stored emails. Specifically, Part II.A. explores the protections afforded by the Fourth Amendment and what the Supreme Court has found to be the "reasonableness expectation of privacy" standard to apply in determining if those protections should extend to certain types of communications. Part II.B. introduces the "third party doctrine."[24] The third party doctrine has been found to decrease someone's reasonable expectation of privacy; and in turn, limit or even exclude certain communications from Fourth Amendment protection. Part II.C. examines Congress' attempt to extend Fourth Amendment protections to email by way of creating the SCA in 1986. However, this section will illustrate how certain provisions of the SCA have been criticized for being outdated, which has made it difficult for courts to apply the statute. Part II.D. further points out the inherent problem within the SCA by not providing an exclusionary remedy provision, and how violations of the SCA can have detrimental consequences for email users. Part II.E. discusses the first and only case, *United States v. Warshak*, which dealt with all of these email privacy issues.

Part III argues that stored emails should be given the same level of protection as traditional forms of communication. In order to do that, Congress must revise certain provisions of the SCA in order to prevent future Fourth Amendment violations. Part III.A. argues that stored emails are essentially the same as telephone calls and paper letters, in that they all share the same purpose and the privacy interest remain the same despite the differences in the manner in which one communicates, and the limitations of the third party doctrine. This section will further lay out certain policy considerations the court must keep in mind when finding a reasonable expectation of privacy

---

22. *See* Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").

23. *See* 18 U.S.C. § 2703 (2009).

24. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."); *see also* United States v. Jacobsen, 466 U.S. 109, 117 (1984).

in stored emails. Part III.B. expands on the various problems that result from the SCA as it stands today due to the arbitrary distinctions the statute makes. This section also introduces a few proposed solutions to these problems.

II. BACKGROUND

In order to fully understand the current law as it relates to email privacy, it is necessary to first discuss a brief history of the warrant requirements under the Fourth Amendment, while keeping in mind the limitations to protection that result from the "Third Party Doctrine."[25] It is also useful to understand why and how Congress' attempt to bring technological communications under statutory protections by enacting the Electronic Communications Privacy Act ("ECPA"), and the problems that result when applying this statute today. Lastly, looking to the 2010 *Warshak* case will be a useful guide for understanding how the courts have juggled all of these issues.

A. THE FOURTH AMENDMENT: WARRANT REQUIREMENT

"The Fourth Amendment was adopted in part due to the founders' concerns about the use of general warrants."[26] As stated from one commentator, general warrants in the past acted as "legal pass keys to all doors" and put "everyone's privacy at the capricious mercy of [their] holders."[27] As a result, the language of the Fourth Amendment specified that a warrant must satisfy the places, people, or things subject to search and seizure, which implied that wide-ranging searches authorized by general warrants were unreasonable.[28]

The Supreme Court of the United States, for the most part, has extended Fourth Amendment protections to traditional and newer forms of communications technology. In 1877, the Court ruled in *Ex parte Jackson* that the Fourth Amendment's warrant requirement applied to mail.[29] In that case, the defendant was arrested for mailing a lottery circular in violation of a law that prohibited mailings of that kind.[30] The Court held that Fourth Amendment protections extended to materials that were closed against inspection, wherever they may be,[31] including letters and sealed packages in the mail.[32] When such

---

25. *See Katz,* 389 U.S. at 351.

26. Courtney M. Bowman, Comment, *A Way Forward After Warshak: Fourth Amendment Protections for E-mail*, 27 BERKELEY TECH. L.J. 809, 810 (2012).

27. *Id.*

28. *See id.*

29. *Id.* at 811 (citing *Ex parte* Jackson, 96 U.S. 727, 733 (1877)).

30. *Ex parte Jackson*, 96 U.S. at 733; *see* Bowman, *supra* note 26, at 811.

31. *Ex parte Jackson*, 96 U.S. at 733.

materials were in transit, the Court held that governmental entities could only open and search through the mail if they obtained a warrant.[33] The Court thus recognized a privacy interest under the Fourth Amendment in the content of postal communications.[34]

However, it is important to note that not all governmental actions are invasive enough to implicate the Fourth Amendment.[35] "The Fourth Amendment's protections hinge on the occurrence of a 'search,' a legal term of art whose history is riddled with complexity."[36] A "search" does not occur unless the individual manifested a subjective expectation of privacy in the object of the challenged search, and society is willing to recognize that expectation as reasonable.[37]

This two-fold inquiry of objective and subjective expectations of privacy was recognized back in 1967 in *Katz v. United States*,[38] where the Court articulated the modern framework for determining the scope of privacy protection for traditional forms of communication.[39] The Court ruled that listening in on private telephone conversations required a warrant.[40] In *Katz*, the defendant was convicted of violating a law against transmitting gambling information over a public payphone after the government used an electronic listening device to pick up the defendant's words.[41] The Court found that an expectation of privacy in the content[42] of one's telephone calls was reasonable[43] and

---

32. *Id.*

33. Bowman, *supra* note 26, at 811 (citing *Ex parte Jackson*, 96 U.S. at 733).

34. *Id.*

35. United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).

36. *Id.* at 283 (citing Widgren v. Maple Grove Twp., 429 F.3d 575, 578 (6th Cir. 2005)).

37. Teri Dobbins Baxter, *Slow Expectations: How Changing Expectations of Privacy Can Erode Fourth Amendment Protection and a Proposed Solution*, 84 TEMP. L. REV. 599, 603 (2012) (citing Kyllo v. United States, 533 U.S. 27, 33 (2001) (quoting California v. Ciraolo, 476 U.S. 207, 211 (1986))).

38. Katz v. United States, 389 U.S. 347, 361 (1967). In *Katz*, the government sought to electronically surveillance Katz's conversations on a public phone booth in order establish that he was using the telephone in question to transmit gambling information to people in other states, in violation of federal law. *Id.* at 354; *see generally* Smith v. Maryland, 442 U.S. 735 (1979). In *Smith*, the Court held that Smith did not hold a reasonable expectation to privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate." Thus, the Court concluded by stating that the installation and use of a pen register was not a search and did not require a warrant. *Id.* at 745-46.

39. Bowman, *supra* note 26, at 811.

40. *Katz*, 389 U.S. at 361 (Harlan, J., concurrence).

41. *Id.* at 353.

42. *See, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 842-47 (11th Cir. 2010) (discussing privacy expectations in email and summarizing case law finding no expectation of privacy in non-content information).

43. *Compare Katz*, 389 U.S. at 351 (noting that "the Fourth Amendment protects people, not places, and what a person knowingly exposes to the public, even in his own

within Fourth Amendment protection.[44] The Court found there to be a reasonable expectation of privacy since the defendant could not expect that his conversation would be shared with the public.[45] Since the government had not obtained a search warrant before listening to the content of the call, the Court held that the government had conducted an impermissible search in part because "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions."[46] This modern framework for determining the scope and extent of privacy protections for traditional forms of communication is still in use today.

However, even though the Supreme Court has applied this reasonableness standard for the past forty years, the Court has been cautious to extend full Fourth Amendment protection to new forms of communication, specifically electronic communications. The Court has refrained from making the decision to extend full Fourth Amendment protection to emails until the societal role for these particular forms of communication becomes more apparent.[47] The Court's restraint was apparent in *City of Ontario v. Quon*, where the Court had to determine whether it was reasonable for the city police to order transcripts of the text messages the defendant sent from his employer-provided device.[48] The Court ultimately held that even though the defendant enjoyed a reasonable expectation of privacy in his text messages, the search itself by the police was reasonable and therefore did not violate his Fourth Amendment privacy rights.[49] The Court noted, "it must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment" because "the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[50] This decision illustrates that, although the

---

home or officer, is not a subject of Fourth Amendment protection, but what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected"), *with Smith*, 442 U.S. at 743-44 (holding that a pen register attached to a suspect's home telephone at the government's request and without a warrant was considered a reasonable search, since telephone users have no legitimate expectation of privacy in the numbers they dial, even from their home telephone).

44. Katz v. United States, 389 U.S. 347, 359 (1967). The Court reasons that "read[ing] the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Id.* at 352; *see also* 18 U.S.C. § 2703(c)(2) (2009).

45. *Katz*, 389 U.S. at 352; *see* Bowman, *supra* note 26, at 811.

46. *Katz*, 389 U.S. at 357; *see* Bowman, *supra* note 26, at 811.

47. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

48. *Id.* at 2624-26.

49. *Id.* at 2633.

50. *Id.* at 2629.

Court is willing to extend Fourth Amendment protection to new forms of communication, it still remains cautious to do so without a more complete understanding of the potential reverberations of such a decision.[51] It is, in part, for these concerns that the Supreme Court has yet to rule on a case dealing with email privacy.[52]

B. THIRD PARTY DOCTRINE

Although the Court has recognized that people are entitled to some amount of privacy in their communications, the "Third Party Doctrine" limits the amount of privacy people can expect, which is especially pertinent in analyzing email privacy due to the role third parties play in email communication.[53] The Third Party Doctrine holds that once an individual voluntarily exposes information to another individual, the original party who disclosed the information has a diminished expectation of privacy with regard to the information.[54] The Supreme Court noted, "when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs, the Fourth Amendment does not prohibit governmental use of that information."[55] As a result, information given to third parties have generally been found to fall outside the scope of Fourth Amendment protection, and accordingly, the government can access this information by requesting or subpoenaing it without informing the party under investigation without the Fourth Amendment's required "warrant."[56]

With the privacy limitations of the Third Party Doctrine in mind, the Supreme Court found, in a series of decisions known as the *Business Records Cases*[57] that the government could subpoena (without a warrant) a defendant's account records from his bank since the bank was a third party to this information, and the defendant voluntarily provided this information to the bank in the ordinary course of

---

51. *Id.*; *see* Bowman, *supra* note 26, at 813.

52. Rehberg v. Paulk, 611 F.3d 828, 844 (11th Cir. 2010).

53. *See* Bowman, *supra* note 26, at 813.

54. Kimberly S. Cuccia, Note, *Have You Seen My Inbox? Government Oversteps the Fourth Amendment Again: Goodbye Telephones, Hello Email*, 43 VAL. U. L. REV. 671, 673 (2009); *see also* Katz v. Unites States, 389 U.S. 347, 351 (1967) (explaining how voluntarily and knowingly exposing information to the public will decrease one's reasonable expectation of privacy).

55. United States v. Jacobsen, 466 U.S. 109, 117 (1984); *see also* Cuccia, *supra* note 54, at 673.

56. *See* Bowman, *supra* note 26, at 813.

57. *See id.* (citing Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1562 (2004)).

business.[58] In addition, the Court found that a warrant was not required for telephone dialing records from a telephone provider since the providers were acting as third parties and the records did not pick up the "contents" of the telephone conversation.[59] Therefore, these cases illustrate that a user who voluntarily provides his information to a third party intending to relay that information in the ordinary course of business does not maintain a reasonable expectation of privacy; thus, falling outside the Fourth Amendment protection.[60] Since the recipient (an ISP in the email context) then may be subpoenaed to disclose the contents of a conversation, message, or letter, and in such instances, the sender may not raise a Fourth Amendment objection.[61]

In order to assess how much invasive power the government has in the context of email, it is important to first understand the role that the Internet and Internet Service Providers ("ISP") play in the realm of the Third Party Doctrine.[62] Originally, emails were sent directly from the sender computer to the recipient computer, but both computers had to be online at the same time in order to complete and receive the transferred message.[63] However, now emails are sent using a "store and forward" model, where emails are first sent to an intermediary, for example an ISP, and then sent to the recipient.[64] Essentially, ISPs provide account holders the ability to send, receive, and store opened and unopened emails associated with the ISPs' systems.[65] It is important to keep in mind that, although the Third Party Doctrine diminishes one's expectation of privacy, courts still have found this expectation of privacy to exist in some cases.[66]

---

58. *See* United States v. Miller, 425 U.S. 435, 444 (1976). In doing so, a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id.* at 443.

59. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); Bowman, *supra* note 26, at 813-14 (citing Mulligan, *supra* note 57, at 1562. "The *Smith* court distinguished the case from *Katz* because the pen register device authorities used to obtain the dialing records in *Smith* did not access 'the contents of communications.'" Bowman, *supra* note 26, at 814 (citing *Smith*, 442 U.S. at 741).

60. *See* United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995); Cuccia, *supra* note 54, at 673.

61. See *King*, 55 F.3d at 1196; Cuccia, *supra* note 54, at 673.

62. *See* Cuccia, *supra* note 54, at 673.

63. Steven R. Morrison, *What Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents*, 16 VA. J.L & TECH. 253, 260 (2011).

64. *Id.*

65. Cuccia, *supra* note 54, at 673.

66. *See* Unites States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that an email user does have a reasonable expectation of privacy even though the contents of the email were sent first through an intermediary third party ISP).

C. CONGRESS' ATTEMPT TO EXTEND FOURTH AMENDMENT PROTECTIONS TO EMAIL: SCA

While the Fourth Amendment protects an individual's "right to be secure" in spacial terms, its protections are far weaker when applied to information stored online since these spacial terms do not directly apply to the "reasonable expectation of privacy" in an online context. Acknowledging the ill-suited scope of the Fourth Amendment's protections applied to new technologies, Congress attempted to remedy this gap in protection by passing Title III of the Omnibus Crime and Safe Streets Act.[67] At the time the Act was enacted, it covered communication interception, but the law only applied to voice transmissions by common carriers.[68] In other words, the protections the law afforded to voice communications did not apply to data, video, and other electronic communications that were becoming more prevalent.[69] Due to these gaps in protection, many companies in the communications industry began to lobby for legislation that could address their concerns regarding the lack of privacy safeguards for these increasingly new and popular forms of technology.[70]

The concern was that, in light of the *Business Records Cases* and the limiting privacy protections as a result of the third party doctrine, email would be granted lower standards of privacy than other forms of communications.[71] Therefore, eighteen years later, Congress passed the Electronic Communications Privacy Act ("ECPA") in 1986 to extend privacy protections to electronic communications.[72] The ECPA is broken down into three statutes: Wiretap Act[73], Stored

---

67. *See* The Omnibus Crime Control and Safe Streets Act, Pub. L. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2510-17 (2006)).

68. Bowman, *supra* note 26, at 814 (citing 132 Cong. Rec. S7991 (daily ed. June 19, 1986) (statement of Sen. Leahy)).

69. *See id.*

70. *See id.*; Electronic Communications Privacy Act: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the H. Comm. on the Judiciary on H.R. 3378, 99th Cong. 1-2 (1986) (statement of Rep. Robert W. Kastenmeier, Chairman, S. Comm. on Courts, Civil Liberties, and the Administration of Justice).

71. Mulligan, *supra* note 57, at 1563. The lack of privacy guarantees had the potential to jeopardize the growth of electronic communications since many people would be hesitant to use new technologies if their messages could not be safeguarded. *Id.* at 1565.

72. Simon M. Baker, Comment, *Unfriending the Stored Communications Act: How Technological Advancement and Legislative Action Have Rendered Its Protections Obsolete*, 22 DEPAUL J. ART TECH. & INTELL. PROP. L. 75, 81 (2011). Congress passed this Act in part to replace the Title III of the Omnibus Crime and Safety Streets Act, but also to create greater protections. *Id.*

73. 18 U.S.C. § 2510-22 (2009).

Communications Act ("SCA")[74] and the Pen Register.[75] All three statutes regulate criminal investigators' access to both in-transit electronic communications and stored content, including emails stored with third party ISPs.[76]

This Comment specifically addresses the SCA, also known as Title II of the ECPA. The SCA was drafted specifically with privacy for stored communications in mind.[77] Essentially, the SCA was created to supplement the Fourth Amendment and to help fill in the gaps of existing privacy law created by changing technologies.[78] Some have categorized the SCA to function as a "statutory version of the Fourth Amendment for computer networks."[79]

However, two sections of the SCA have been recent subjects of litigation because of the provisions that address both lack of notice and delayed notice when gathering the contents of email: section 2703 and section 2705 respectively.[80] Section 2703 of the SCA allows for a governmental entity to compel a service provider to disclose the contents of electronic communications in varying circumstances, widely known as "compelled disclosure."[81] Unlike the Wiretap Act and the Pen Register, the SCA only regulates retrospective surveillance.[82] Under the compelled disclosure provision, varying levels of protection are afforded depending on not only the type of service in which the email is held, but also the length of time the email has been in electronic storage.[83] The provision distinguishes between two types of services in which emails are stored, including the "electronic communication services" and the "remote computing services."[84] "Electronic communication services" allow users to send or receive wire or electronic communications, which covers basic email services.[85] "Electronic storage" is any

74. 18 U.S.C. § 2703 (2009).
75. 18 U.S.C. § 3127(3) (2009).
76. *See* Perry, *supra* note 8.
77. *See also* Katharine M. O'Connor, Note, *OMG They Searched My Texts: Unraveling the Search and Seizure of Text Messages*, 2010 U. ILL. L. REV. 685, 701-02 (2010) (explaining why the Stored Communications Act was created).
78. *See* Perry, *supra* note 8, at 350; O'Connor, *supra* note 77, at 701-02.
79. Perry, *supra* note 8, at 350.
80. *See* Warshak, v. United States 490 F.3d 455, 462-65 (6th Cir. 2007); 18 U.S.C. § 2703 (2009); 18 U.S.C. § 2705 (2009).
81. *See* 18 U.S.C. § 2703 (2009).
82. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1232 (2004) ("Retroactive surveillance has been defined as 'access to stored communications that may be kept in the ordinary course of business by a third party provider.' "). In contrast, prospective surveillance refers to "obtaining communications still in the course of transmission," which is the focus of the Wiretap Act and the Pen Register statute. *Id.* at 1213.
83. *See* 18 U.S.C. § 2703 (2009).
84. *See id.*
85. 18 U.S.C. § 2510(15) (2009).

temporary, intermediate storage of a wire or electronic communication and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.[86] "Remote computing services" provide computer storage or processing services to customers,[87] and are designed for longer-term storstorage.

In addition to the type of service, the privacy protections under the SCA vary depending on the length of time the email has been stored electronically.[88] For example, emails stored with an electronic communication service for less than 180 days may be acquired "only pursuant to a warrant."[89] Emails stored with a remote computing service and those stored with an electronic communication service for more than 180 days require the government to either obtain a search warrant, an administrative subpoena, or a court order.[90] Though probable cause is required to obtain a search warrant, the SCA allows subpoenas and court orders to be issued under much lower standards than those of the Fourth Amendment, requiring only that the government entity offers "specific and articulable facts" showing "reasonable grounds" to believe that the contents of the communication "are relative and material to an ongoing criminal investigation."[91]

However, rules almost always come with exceptions, and section 2703 is not unique in this respect.[92] Section 2703 states that when the government requests an account holder's information from an ISP, the government must notify the account holder of the request. However, section 2703 also stipulates that this notice may be delayed for email content that is defined in section 2705[93] – the second section under the SCA that has been subject to recent litigation.[94]

Section 2705 provides that the government may elect to delay notification to the account holder for up to ninety days.[95] In addition, this delayed notice may be continuously extended in ninety-day increments if the government submits the proper request for the court to grant such exception.[96] Theoretically, since the SCA allows for

---

86. 18 U.S.C. § 2510(17) (2009).
87. 18 U.S.C. § 2711(2) (2009).
88. *See* 18 U.S.C. § 2703(a) (2009).
89. *See* 18 U.S.C. § 2703(a) (2009); Perry, *supra* note 8, at 352.
90. *See* 18 U.S.C. § 2703(a) (2009); Perry, *supra* note 8, at 352; *see also* United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010).
91. 18 U.S.C. § 2703 (d) (2009); *see* Perry, *supra* note 8, at 352.
92. Cuccia, *supra* note 54, at 703.
93. *See* 18 U.S.C. § 2705 (2009); Cuccia, *supra* note 54, at 703.
94. *See* 18 U.S.C. § 2705 (2009); *see also* Warshak, v. United States 490 F.3d 455, 462 (6th Cir. 2007).
95. *See* 18 U.S.C. § 2705 (2009).
96. *See* 18 U.S.C. § 2703(a)(4)-(5) (2009).

continuous extensions to the delayed exception rule, the government may lawfully obtain the content of an individual's email without any notification to that individual for an unlimited amount of time.[97] However, according to the SCA, this theoretical situation would only occur when an "adverse effect" is likely.[98] In effect, this delayed notice provision leaves open the possibility that individuals do not have the opportunity to refute seizures that may be unlawful before Fourth Amendment violations occur.[99]

As the statutory law under the SCA stands today, electronic communications receive less protection than wire and oral communications. The government can potentially search through and seize your emails without obtaining a warrant, can do so without first providing you notice, and can delay that notice for seemingly infinite amount of times.[100] Since the SCA was enacted before the "advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994," the SCA "is best understood by considering its operation and purpose in light of the technology that existed in 1986."[101] Therefore, many today criticize the SCA for being outdated, ineffective, and inefficient.[102] Thus, the nature of the antiquated and

---

97. *See* 18 U.S.C. § 2705(a)(4) (2009); *see also* United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010) (demonstrating delayed notice).

98. *See* 18 U.S.C. § 2705(a)(2) (2009).

99. *See* Cuccia, *supra* note 54, at 704.

100. *See* Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. TECH. L. REV. 1, 42 (2003).

101. Perry, *supra* note 8, at 365 (citing Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (citing William Jeremy Robison, Note, *Free at What Cost? Cloud Computing Privacy Under the Stored Communication Act,* 98 GEO. L.J. 1195, 1198 (2010))); *see also* Baker, *supra* note 72, at 115 ("Most of [the] current issues regarding the SCA involve technology that was not even considered possible, let alone in use at the time of the SCA's enactment."); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (stating that "the difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web").

102. *See* Perry, *supra* note 8, at 365. "But courts, legislators, and even legal scholars have had a very hard time understanding the method behind the madness of the SCA. The statute is dense and confusing, and that confusion has made it difficult for legislators to legislate in the field, reporters to report about it, and scholars to write scholarship in this very important area." Kerr, *supra* note 82, at 1208. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (quoting Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (referring to the provisions of the ECPA as "famous (if not infamous) for [their] lack of clarity" and the "complex, often convoluted" intersection of the SCA and the Wiretap Act)); LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See,* 46 A.F. L. Rev. 155, 171 (1999) (noting that Congress's intent, while enacting the EPCA, to cover email transmission was obscured by the complexity of the statutory language).

ambiguous language of the SCA has left courts with the difficult job of interpreting and applying the statute.[103]

D. UNLIKE THE FOURTH AMENDMENT – SCA DOES NOT HAVE EXCLUSIONARY RULE

The exclusionary rule excludes from a criminal trial any evidence seized from a defendant in violation of his Fourth Amendment rights.[104] The primary rationale for the exclusionary rule is to deter future violations of the Fourth Amendment by the police.[105] It is a judicially designed remedy to protect citizens' Fourth Amendment rights prospectively, rather than to redress the past infringement of these rights.[106] While the exclusionary rule compels law enforcement agents to respect the guarantees of the Fourth Amendment, it is not a personal constitutional right of the accused.[107]

In order for the exclusionary rule to prohibit the introduction of incriminating evidence at trial, police action while obtaining the evidence must trigger the Fourth Amendment.[108] As stated earlier, a "search" must first occur.[109] Once it has been determined that a search has occurred, then the issue becomes whether the search and seizure was reasonable.[110]

However, it is significant to note that under the current version of the SCA, the exclusionary rule does not extend to electronic

---

103. *See* Baker, *supra* note 72, at 84 (illustrating how the goals of the SCA may appear simple, but their implementation has provided difficulties for courts since the Statute's enactment).

104. *See* Weeks v. United States, 232 U.S. 383, 393 (1914); Mapp v. Ohio, 367 U.S. 643, 648 (1961).

105. *See* Linkletter v. Walker, 381 U.S. 618, 636-37 (1965) ("[A]ll of the [recent] cases . . . requiring the exclusion of illegal evidence have been based on the necessity for an effective deterrent to illegal police action."); Nix v. Williams, 467 U.S. 431, 442-44 (1984); Stone v. Powell, 428 U.S. 465, 486 (1976).

106. *See* Ryan A. Ray, *The Warrantless Interception of Email: Fourth Amendment Search or Free Rein for the Police?,* 36 RUTGERS COMPUTER & TECH. L. J. 178, 185 (2010); United States v. Leon, 468 U.S. 897, 906 (1984) ("The exclusionary rule is neither intended nor able to 'cure the invasion of the defendant's rights which he has already suffered' ") (quoting *Powell*, 428 U.S. at 530 (White, J., dissenting))).

107. Ray, *supra* note 106, at 187-88 (explaining the Fourth Amendment exclusionary rule).

108. *See Weeks*, 232 U.S. at 398 (applying the exclusionary rule for evidence seized in violation of the Fourth Amendment to federal courts); Ray, *supra* note 106, at 190.

109. *See* Katz v. United States, 389 U.S. 347, 360-361 (1967) (Harlan, J., concurring); United States v. Jacobsen, 466 U.S. 109, 113 (1984); Kyllo v. United States, 533 U.S. 27, 33 (2001) (quoting California v. Ciraolo, 476 U.S. 207, 211 (1986)).

110. Ray, *supra* note 106, at 191.

communications.[111] In the absence of this statutory exclusionary rule, illegally intercepted electronic communications are subject only to the Fourth Amendment's exclusionary rule.[112] As a result, electronic communications receive less protection than wire communications in that illegal interception by private parties would not result in the suppression under Fourth Amendment analysis, which only limits the actions of government officers. Moreover, some electronic communications that are illegally intercepted by government officials may be admissible under Fourth Amendment analysis due to the good faith exception to the constitutional exclusionary rule.[113]

As the current law stands, electronic communications that have reached their destination and which are held in electronic storage no longer receive constitutional protection. Rather, the statutory scheme as interpreted by the courts distinguishes between the illegal interception of electronic communications during transmission and unlawful access to an electronic communication held in storage by a provider of electronic communication services (like an ISP).[114] Stated simply, as of today, emails that are illegally intercepted by the government without a warrant can be, and most likely will still be, used against a defendant in a criminal trial due to the lesser protections afforded under the SCA.[115]

1. *The Warshak Decision: Current Email Jurisprudence*

Although few cases analyze, or even discuss, the constitutionality of sections 2703 and 2705 of the SCA, one case that actually did was *United States v. Warshak*.[116] As the first and only court that has dealt with the issue of email privacy, *Warshak* nicely ties together the majority, if not all, of the reasons that email privacy should be afforded the same constitutional protection as traditional forms of communications. However, this case also illustrates the ramifications for applying the SCA as the act stands today.

---

111. Pikowsky, *supra* note 100, at 42 (discussing the different levels of protection awarded due to the fact that the statutory exclusionary rule does not apply to electronic communications).

112. Ray, *supra* note 106, at 190.

113. *See Leon*, 468 U.S. at 897; Michael Leib, *E-mail and the Wiretap Laws: Why Congress Should Add Electronic Communications to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 393 (1997).

114. *See* Ray, *supra* note 106, at 191.

115. *See* United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010); *see also* O'Connor, *supra* note 77, at 701-02 (noting the insufficiencies of the SCA).

116. *See Warshak*, 631 F.3d at 289..

a. Relevant Facts of the Warshak Case

In *Warshak*, Steven Warshak and his company, Berkeley Premium Nutraceuticals, were under investigation by the United States government for suspected mail and wire fraud and money laundering activities. The government sought access to Warshak's email. In 2005 federal investigators applied for court orders pursuant to section 2703(d) of the SCA[117], as opposed to a search warrant, compelling two of Warshak's internet service providers, NuVox Communications and Yahoo!, to disclose the contents of "wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled by" Warshak. Pursuant to section 2703(d) of the SCA, the government needed to merely provide the issuing court with "specific and articulable facts" that demonstrated that the material they sought was "relevant" to its ongoing criminal investigation of Warshak.[118] As ordered, NuVox and Yahoo! both complied by collectively handing over a total of 27,000 emails that Warshak had sent or received over the previous nine years.[119] During this process, the government had not notified Warshak that they were searching and seizing his emails.[120] It took one year after the issuance of the first court order for the government to notify Warshak of their investigation. At this point, Warshak filed suit against the government in the Southern District of Ohio, claiming that the government's court orders violated both the SCA and the Fourth Amendment.[121] Warshak eventually moved for a preliminary injunction prohibiting the government from using another §2703(d) court order or otherwise similar procedure to compel disclosure of future sent or received emails.

b. Warshak Court Opinions

After Warshak was convicted of the majority of the counts against him in the District Court,[122] he appealed. On appeal before the Sixth Circuit, Warshak argued, among other things, that the government's ex parte search and seizure of his emails without a warrant

---

117. *See* 18 U.S.C. § 2703(d) (2009).
118. *See id.*
119. *See Warshak,* 631 F.3d at 281-82.
120. *See id.*
121. Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email,* 2008 U. CHI. LEGAL F. 121, 130 (2008).
122. *See* United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010) (Warshak was charged with the majority of the 112 counts against him, including mail fraud, bank fraud, and money laundering).

violated his Fourth Amendment rights.[123] The government challenged Warshak, claiming that any Fourth Amendment violation that did occur was "harmless," and that the search and seizure of Warshak's email was protected by their "good faith reliance" on the SCA.[124] The court ruled in favor of Warshak, finding that the government did violate his Fourth Amendment rights when they compelled his ISP to turn over the contents of his emails without a warrant.[125] After analogizing email to other forms of communication, the court found that since email users do have an expectation of privacy, stored emails should receive the same Fourth Amendment protection that traditional forms of communication are awarded.[126] In addition, the court was not persuaded by the argument that just because emails go through a third party intermediary (an ISP) they should receive less protection.[127] Ultimately, the court found that Warshak enjoyed Fourth Amendment protection, and that the SCA was unconstitutional.[128] However, the court agreed with the government's good faith reliance on the language of the SCA argument, finding a reversal of Warshak's criminal conviction unwarranted.[129]

The *Warshak* decision is the current state of the law regarding email privacy. As a result of this, we are left with the question of whether courts should follow the decision from *Warshak*, and if so, the ramifications of that decision.

III. ANALYSIS

Email should be afforded the same level of constitutional protection as traditional forms of communication. In coming to this conclusion, one must recognize that the government's acquisition of stored emails constitutes a Fourth Amendment search, which would bring regulation of modern surveillance practices into the current Information Age and eliminate the strangely disparate treatment of mailed and telephonic communications on the one hand and electronic communications on the other.[130] Once stored emails receive proper Fourth Amendment protection, government agents will only be able to access our private-stored electronic communications after obtaining a warrant. While it is necessary to apply the "reasonableness" standard on a

123. *See id.* at 282.
124. *Id.*
125. *See id.*
126. *Id.* at 285-86.
127. United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010).
128. *Id.*
129. *Id.* at 282.
130. *See* Bellia & Freiwald, *supra* note 121, at 134.

case-by-case basis[131] to determine the level of constitutional protection, it is important for the court to strike the proper balance between governmental need to investigate crimes and the societal need to protect personal privacy. Now that the *Warshak* court has declared the SCA unconstitutional to the extent that it allows the government to compel ISPs to disclose the contents of emails without a warrant, it is time to reevaluate the current email privacy protection scheme, and looking to the *Warshak* case is a start.

A. EMAIL SHOULD RECEIVE THE SAME FOURTH AMENDMENT PROTECTION AS TRADITIONAL FORMS OF COMMUNICATION

"Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[132] Thus, email should receive the same Fourth Amendment protection as traditional forms of communications because it is reasonable to expect privacy in email. As a result, governmental entities should not be allowed to compel an ISP to disclose the contents of one's email without first obtaining a warrant. Although the Third Party Doctrine can limit the extent of privacy protection afforded, courts have still found email users to hold a reasonable expectation of privacy.[133] Either way, it is the responsibility of Congress to act now, and to amend the SCA to bring electronic communications under the same protection as traditional communications.

1. *Email and Traditional Forms of Communication are Functionally Equivalent*

Email is as important to Fourth Amendment principles today as protecting telephone conversations was in the past.[134] Regardless of the medium of communication, governmental intrusion upon the private exchange of communication should be regulated by the same standard. Our purpose in corresponding has not changed from traditional forms of communication, so neither should the protections

---

131. *See id.* at 137 (noting how the Katz reasonableness standard is "case specific").

132. United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010).

133. *See id. at* 266.

134. *See id.* (citing Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007)) ("It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shard communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past."); *see also* Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971, 980 (2012).

under the law.[135] Both forms of communication are used by citizens to transmit ideas between themselves in a manner that seeks to preserve the privacy of those ideas.[136] These two types of communication have been characterized as "functional[ly] equivalent"[137] to each other; thus, Fourth Amendment protections should extend to email communications because it is reasonable to expect privacy in those communications.[138]

However, the expectation of privacy that an individual can assert in email messages depends greatly on two things: the type of message sent and to whom the message was sent.[139] Basically, in determining whether and to what degree these communications are protected, the Court has varied the level of protection awarded depending on whether the information sought was considered "content" or "noncontent."[140] One way of looking at whether the type of information is considered "content" requires separating the question of content/noncontent status from the question of whether the information is protected under *Smith v. Maryland*.[141] *Smith* illustrates that one may give up his reasonable expectation of privacy in even intimate content if the user is found to have disclosed the "content" [142] to the carrier of the

---

135. *See* Morrison, *supra* note 63, at 255 (noting how the function of email today is "occupying the function that once belonged to the United States Postal Service").

136. *See* Ray, *supra* note 106, at 200.

137. *See Warshak,* 631 F.3d at 286. "Thus, the ISP is the functional equivalent of a post office or a telephone company." In making this assertion, the court relied on the premise that the police are forbidden from walking into a post office and intercepting a letter or using the phones system to make a secretive recording of a telephone call without a warrant, and since ISPs function the same as post offices and telephone lines, the protections for stored emails should be the same. *Id.*

138. *See* Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 648-49 (2011) ("Advances in technology spurred important developments in the role the Internet plays in people's everyday lives. While email increasingly replaces first-class mail, there is no reason to believe that such a replacement affects individual privacy expectations.").

139. *See* Ray, *supra* note 106, at 218.

140. *See* Katz v. United States, 389 U.S. 347, 352 (1967); Smith v. Maryland, 442 U.S. 735, 739 (1979); United States v. Miller, 425 U.S. 435, 442 (1976); United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010); *see also* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2125 (2009) (focusing on the distinctions between "content" and "noncontent" communications, arguing that this distinction is paramount to determining the level of protection afforded).

141. *See Smith*, 442 U.S. at 735; *see, e.g.,* Tokson, *supra* note 140, at 2155.

142. *See Smith,* 422 U.S. at 741 (distinguishing between information considered content from noncontent by comparing a pen register, which only picks up the numbers dialed, to a listening device, which picks up the actual contents of communications). The *Smith* Court held that, unlike in *Katz* where a listening device picked up the content of a telephone conversation, no actual expectation of privacy existed in a pen register since there was no "content" that could be searched. *Id.* at 745-46; *see also* Tokson, *supra* note 140, at 2125.

communication (the ISP in the email context).[143] Essentially, the Fourth Amendment protects the "content" of one's communications, while not protecting any "noncontent" information. This content/noncontent distinction was also paramount in *Katz*, where the Court made very clear that the "content" of one's telephone calls receives Fourth Amendment protection since the telephone user has a reasonable expectation of privacy because he "is surely entitled . . . that the words he utters into the mouthpiece will not be broadcast to the world."[144]

Applying this precedent to the context of emails, email users who store emails with their ISP have a subjective expectation to privacy that the government will not search through and read the contents of those emails without a proper warrant.[145] Just like an envelope holds the contents of the letter, an ISP server holds the contents of an email. Thus, ISP servers are essentially a form of a closed container, or according to one author, "today's virtual mailboxes."[146] Email messages

---

143. *But see* Tokson, *supra* note 140, at 2125 (suggesting that combining *Smith*'s analysis of the content/noncontent distinction in telephone calls with its analysis of reasonable expectation of privacy in such calls risks complicating the question of what actually is "content"). The author noted, as general semantic matter, the definition of "content" and how it has remained generally the same since before *Smith* was decided, and even the same back in the sixteenth century (citing III OXFORD ENGLISH DICTIONARY 815 (J.A. Simpson & E.S.C. Weiner eds., 2nd ed. 1989)). *Id.*

In laying out the different meanings of "content," the author noted that the first meaning of "content" is "that which is contained" in something; the second meaning is the "subject-matter" of a speech or piece of writing; and the third meaning is the "sum or substance of what is contained in a document; tenor, purport." *Id.* (citing III OXFORD ENGLISH DICTIONARY 815 (J.A. Simpson & E.S.C. Weiner eds., 2nd ed. 1989)). Accordingly, the author concluded that content is generally defined as not only the actual words of a document, but also the general subject matter of the document and the meaning of its message. *Id.*

144. *Katz,* 389 U.S. at 352. This was the decision that brought telephone conversations under full Fourth Amendment protection. *See also* Perry, *supra* note 8, at 359 (citing Warshak v. United States, 631 F.3d 266, 285 (6th Cir. 2010) (citing Smith v. Maryland, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting))).

145. *See Warshak*, 631 F.3d at 284 (finding that Warshak held a subjective expectation of privacy in his emails since his "entire business and personal life was contained within the . . . emails seized"); *Katz,* 389 U.S. at 351 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected"); United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (acknowledging the existence of a [subjective] expectation of privacy in email messages); Bellia & Freiwald, *supra* note 121, at 137 (agreeing that email users, like Warshak, generally have a subjective expectation of privacy in mails they store with their ISPs); *but see* Brett M. Frischmann, *The Prospect of Reconciling Internet and Cyberspace*, 35 LOY. U. CHI. L.J. 205, 219 (2003) (arguing that that email users do not have a subjective expectation to privacy).

146. Cuccia, *supra* note 54, at 694. Analogizing email to that of the traditional letter, an email's message "header" is to a physical letter's envelope (containing the mailing addresses of both the sender and recipient), as an email's message "body" is to the actual letter itself. Morrison, *supra* note 63, at 260.

contain the ideas and private expressions of their author, just like the constitutionally protected letters do. Given the often sensitive information contained in emails, it is unlikely that email users give up this expectation to privacy simply because they send an email rather than a letter.

2. *Email and Traditional Forms of Communication Have the Same Privacy Interests*

Furthermore, just because the manner in which we communicate has changed over the years does not mean that the privacy interests have changed.[147] The privacy interest in communicating through email remains the same for both traditional forms of communication and email communications,[148] if not greater in the context of email communications.[149] For example, Warshak's attorneys drew an appropriate conclusion when comparing the privacy interests in traditional forms of communication (sealed containers and letters) to the privacy interests in newer forms of technology (emails).[150] In that conclusion, the authors described an email as:

> [H]aving more privacy aspects than a traditional letter because the owner of the email can repossess a read-and-then-closed email at any moment, without any notice or permission from the ISP. The owner of

---

147. Ruth Gavison, *Privacy and the Limits of the Law*, 89 YALE L.J. 421, 423-24 (1980):

> Our interest in privacy . . . is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. This concept of privacy as a concern for limited accessibility enables us to identify when losses of privacy occur. Furthermore, the reasons for which we claim privacy in different situations are similar. They are related to the functions privacy has in our lives: the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society. The coherence of privacy as a concept and the similarity of the reasons for regarding losses of privacy as undesirable support the notion that the legal system should make an explicit commitment to privacy as a value that should be considered in reaching legal results.

148. *See* United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (holding that "[t]he privacy interests in [mail and email] are identical"); *see also* Pikowsky, *supra* note 100, at 45 (arguing that letters in the mail, telephone conversations, and email should all receive the same level of protection from surreptitious interception by law enforcement officers or private parties).

149. *See* Cuccia, *supra* note 54, at 708 ("Because e-mail evidentiary issues are analogous to telephone calls and emails likely retain an even higher expectation of privacy than telephone communications because e-mails are more similar to written letters, heightened privacy protections guaranteed by the Fourth Amendment should apply to e-mails.").

150. *See id.* at 695 (citing James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, PRACTICING LAW INST. NO. 11253 407 (2007)).

> the email can delete it from the mailbox, or do whatever he or she wants to do with the email. It is, for all purposes, in that person's possession, dominion, and control at all times. Consequently, if there is any difference, the privacy interests should be greater in the context of email than in the traditional carrier paradigm.[151]

Essentially, an email stored on an ISP's server may constitute a "closed container," as email accounts are typically password-protected, and the ISP has limited access to the contents of the communication.[152] Expanding on this conclusion, emails are not visible to the naked eye; instead, several intrusive searches must occur before the contents may be read.[153] Much like the nature of a traditional letter sitting inside a "real mailbox," an email remains hidden inside a subscriber's virtual mailbox. In order to read the contents of that email, one must physically intrude by using the computer's "open" function, which is arguably an act indistinguishable from the act of opening a sealed letter or package. Others have applied the storage locker analogy: "[w]hen an individual stores personal property with a third party, the owner of the property retains a privacy interest in the stored items, meaning that a warrant should be required to search the storage space."[154] Therefore, ISP-stored emails should be, and are entitled to, protection under the Fourth Amendment just as traditional forms of communication have been protected.[155]

In further support, the *Warshak* court applied this same reasoning and found that Warshak plainly manifested an expectation that his emails would be shielded from outside scrutiny.[156] The court reasoned that it was "highly unlikely" that Warshak expected his email to be made public due to its content" – content the court described as "often sensitive and highly damning."[157] Furthermore, the *Warshak* court specifically noted, "email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age."[158] Not only did the court find that email should be protected just like traditional forms of communications, the court went so far as to categorize email as "so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument . . . for self-expression, even

---

151. *Id.*
152. Kattan, *supra* note 138, at 651.
153. *See* Cuccia, *supra* note 54, at 708.
154. *Id.*
155. *See id.*, at 694 (arguing in favor of awarding email communications the same level of protection as traditional forms of communication).
156. United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).
157. *Id.* The court further noted the unlikelihood that Warshak expected his emails to be made public because it is seldom that "people unfurl their dirty laundry in plain view." *Id.*
158. *Id.* at 286.

self-identification."[159] Thus, when the police secretly learn of the contents of communication, they intrude on the same privacy interests regardless of the medium of communication. This is why the same protections that apply to traditional forms of communication should apply to email communications.[160]

3. *Email Users Maintain a Reasonable Expectation of Privacy Despite the Third Party Doctrine*

As stated earlier, the expectation of privacy that an individual can assert in email messages does not only depend on the type of message (content versus noncontent distinction), but also depends on to whom the message was sent.[161] Rightly so, the Court has found that voluntarily supplying a third party with your information diminishes your expectation that your information will be kept private.[162] Basically, the argument is that one assumes the risk that the third party ISP will disclose of the contents of his emails to the authorities; thus, diminishing the protection awarded.

As seen in *United States v. Miller*, the Court directly embraced the proposition that no legitimate expectation to privacy existed in revealing the contents of bank records to the third party bank because the records were voluntarily conveyed and exposed to the banks in the ordinary course of business.[163] The Court further elaborated that despite the fact that the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed, it still found there to be no reasonable expectation to privacy.[164]

Citing to *Miller* a few years later, the *Smith* Court also found no reasonable expectation of privacy in numbers dialed on a telephone.[165] The Court found that neither the defendant nor society in general

---

159. *See id.* (holding that email requires strong protection under the Fourth Amendment because otherwise, the Fourth Amendment would prove to be an ineffective guardian of private communication, an essential purpose it has long been recognized to serve).

160. *See* Pikowsky, *supra* note 100, at 46 (arguing that not providing email with the same level of protection from governmental intrusion that is otherwise granted to telephone calls is unjustified).

161. Ray, *supra* note 106, at 218.

162. *See, e.g.,* United States v. White, 401 US. 745, 751-52 (1971) (finding no expectation of privacy since a depositor takes the risk that in revealing his affairs to another, that information will be conveyed by that person to the Government).

163. United States v. Miller, 425 U.S. 435, 442 (1976). The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorizes. *Id.* at 443.

164. *Id.*

165. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979).

could have an expectation of privacy in the phone numbers dialed because those numbers were voluntarily given to the telephone company in the course of making a phone call; therefore, the caller assumed the risk that the dialing information could be handed over to the police.[166]

While it is true that the Third Party Doctrine has been found to limit one's expectation of privacy, courts have still found there to be an expectation to privacy, and that email users do not necessarily lose their Fourth Amendment protection. A New York District Court wrote:

> It is true . . . that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person, or obtained through a subpoena directed to that person . . . However, "[t]he same does not necessarily apply . . . to an intermediary that merely has the ability to access the information sought by the government." . . . Indeed, the "assumption of risk" so trumpeted by the Government, is far from absolute. "Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service's ability to access them." . . . These consequences of an extension of the assumption of risk doctrine are not acceptable under the Fourth Amendment. A caller "is surely entitled to assume that the words he utters into a mouthpiece will not be broadcast to the world,' and therefore cannot be said to have forfeited his right to privacy in the conversation."[167]

Although an ISP has access to the communication, it is a carrier – similar to the post office or telephone company – rather than a bona fide third party for purposes of the Fourth Amendment.[168] Since emails must pass through an ISP's server to reach their intended recipient (like a letter must pass through a postal office or a telephone call passing through the phone company), it serves the same function, so the warrant requirement should be the same. Even though a telephone call is "shared" with the telephone company, it is established that an individual still maintains a reasonable expectation of privacy as to the content of the conversation *vis-à-vis* the phone company.[169] This is because the phone company is not the intended recipient, but

---

166. Bowman, *supra* note 26, at 742-45.

167. Morrison, *supra* note 63, at 289.

168. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (distinguishing itself from *Miller* since Warshak's ISP was only an intermediary, not the intended recipient of the emails); *see* Bellia & Freiwald, *supra* note 121, at 165 ("[W]e view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In these cases, as in the stored email case, the customer grants access to the ISP because it is essential to the customer's interests."); Ray, *supra* note 106, at 215.

169. *See* Ray, *supra* note 106, at 215.

rather just an intermediary to get the message to the intended recipient.[170] The *Smith* Court specifically distinguished itself from *Katz* because the actual contents of the conversation were not sought, only the dialing records.[171] Even though an email is "shared" with an ISP, the ISP is not the intended recipient and it is not within their ordinary course of business to read the contents of those private emails, just simply pass the email along to its intended recipient.[172]

There is no reason to construe the user's assumption of risk (that the intermediary will discover the incriminating information in the course of its proper access) as the assumption of risk that the government will compel the ISP that resists to produce that information without following the proper procedures.[173] Agreeing with the words of two professors, unless the information the government discovers is a static, non-communication record of their business, or a communication to which the ISP itself is a party, the stored email's sender or recipient enjoys the protections of the warrant requirement.[174]

Expanding on this logic, the *Warshak* court held that email users maintain a reasonable expectation of privacy despite the fact that third party ISPs could access those emails.[175] By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.[176] Therefore, if the government could compel an ISP to give up the contents of one of their subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates the need for a warrant.[177] In forming this conclusion, the court analogized emails to traditional letters, and found that a warrant was still required despite the fact that the sealed letters were handed over

---

170. *Id.* (citing Warshak v. United States, 490 F.3d 455 (6th Cir. 2007)).

171. *See* Smith v. Maryland, 442 U.S. 735, 741-43 (1979); Katz v. United States, 389 U.S. 347, 352 (1967); *see also* Ray, *supra* note 106, at 233 (arguing that *Smith's* holding is completely inapposite in the context of email contents since the rationale in *Smith* was that the pen register at issue did not disclose any contents of the communication).

172. *See* Ray, *supra* note 106, at 215.

173. Bellia & Freiwald, *supra* note 121, at 167 (advocating that the "assumption of risk" argument with regards to an ISP does not defeat the necessity of first obtaining a warrant). However, the authors to that argument made clear that if the third party chooses to disclose the information so discovered to the government without requiring a warrant, the user cannot complain. *Id.* When the user assumed the risk that the intermediary would discover incriminating information or property in the course of its business, she also assumed the risk that the intermediary would choose to turn that information over to the government. *Id.* The authors went on to say that if the user mistakenly trusted the intermediary to protect its incriminating information, there is no reason for the Fourth Amendment to protect that misplaced trust. *Id.*

174. *Id.* at 168.

175. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

176. *Id.* at 284.

177. *See id.* at 286.

to possibly dozens of mail carriers, any of whom "could tear open the thin paper envelopes that separate the private words from the world outside."[178]

4. *Policy Considerations: Follow the Logic of Warshak*

It is important to keep in mind, as many courts have, that the judiciary must err on the side of caution when finding an objective expectation of privacy in email communications until its role in society becomes clearer.[179] While some courts are willing to extend Fourth Amendment protection to newer forms of communication, these courts have made clear that they must remain cautious to do so without a more complete understanding of the potential reverberations of such a decision.[180]

The *Warshak* court acknowledged two bedrock principles to keep in mind when finding a reasonable expectation of privacy in emails.[181] First, courts must keep in mind that the information in these emails is being passed through a communications network, which could diminish one's expectation that sending an email over the World Wide Web would remain private.[182] However, the court also pointed out the importance of keeping the Fourth Amendment at pace with the inevitable and constant technological progressions in today's Information Age and technological progression.[183]

These two principles must progress parallel with each other, or else risk losing the protections and guarantees of the Fourth Amendment.[184] Touching on the first principle, the fact that an email is sent over an Internet network should not diminish the expectation of

---

178. *Id.* at 285; *see* Katz v. United States, 389 U.S. 347, 351 (1967) ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

179. *See Warshak*, 631 F.3d at 285 (acknowledging the grave importance and enduring consequences of finding an objective expectation of privacy in email due to the prominent role that email has assumed in modern communication); City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) (erring on the side of caution of finding a reasonable expectation of privacy in email communications until it's role in society becomes more clear).

180. *See Warshak*, 631 F.3d at 286; Bowman, *supra* note 26, at 813 (citing *Quon*, 130 S. Ct. at 2629).

181. *See* United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010).

182. *Id.*

183. *See id.* The court noted that as some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise. *Id.* at 286.

184. *See id.* at 285; *see* Kyllo v. United States, 533 U.S. 27, 34 (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment"); Kattan, *supra* note 138, at 652 ("The law must advance with the technology to ensure the continued vitality of the Fourth Amendment.").

privacy far enough to exclude it from Fourth Amendment protection.[185] Referring back to the earlier quotation from the New York District Court, if email users were found to not maintain a reasonable expectation of privacy solely because an ISP could merely "access" that information, then the same should apply to telephone users and letter writers, but our precedent tells us otherwise.[186] If one accepts the argument that email communications are the same as traditional forms of communication (same purpose, same privacy interests, and same functionality), then it logically follows that the expectations or privacy should be the same.

Tying the first principle in with the second, it is important to accept the fact that technology is becoming even more prevalent in our everyday lives.[187] As a result, we will be faced with greater uncertainty about our privacy rights, which forces us to choose between outdated and cumbersome modes of communication declared private and protected by the courts, and the faster, more convenient modes of communication that may not be protected under the Fourth Amendment.[188] In other words, anyone who is concerned with privacy in email communications must either avoid technology and the opportunity to send emails or accept the risk that any expectation of privacy may not be recognized and protected by the law.[189] As one proponent of email privacy stated, "if the only way to maintain complete privacy is to avoid Internet communication altogether, they may decide to accept compromised privacy for the sake of fast, efficient communications."[190] Until the legislature ends this reluctance to modernize the

---

185. *See* Morrison, *supra* note 63, at 289.

186. *See Warshak*, 631 F.3d at 286-87; Katz v. United States, 389 U.S. 347, 352 (1967); Smith v. Maryland, 442 U.S. 735, 746-47 (1979) (Stewart, J., dissenting).

187. *See* Baker, *supra* note 72, at 113 (noting that as more information is stored online instead of in paper form, that right is put in jeopardy, not because of an inherent shift in legal doctrine, but due to both legislative inaction and the rapidly evolving nature of the relevant technology).

188. Baxter, *supra* note 37, at 630; *see* Kattan, *supra* note 138, at 649 (illustrating how new technology has not been captured by the SCA; therefore, the lack of guidance inhibits the efficiency of law enforcement, as officials must decide whether to take the chance of stepping over the like – risking suppression of evidence or even personal sanctions – or shy away from the line to avoid overstepping).

189. *See* Baxter, *supra* note 37, at 631 (illustrating the potential sacrifices resulting from choosing efficient modes of communication, which do not guarantee privacy protection, rather than choosing older forms of communication, which are guaranteed privacy protection under the Fourth Amendment).

190. *Id.* The Stored Communications Act and other legislation may provide some protection for such hesitant users, but protection is not absolute. There are exceptions that allow for certain government searches, and it is still unclear whether or under what circumstances those exceptions might violate the Fourth Amendment. *Id. Compare* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that email content is protected despite the fact that the service provider has access to the email),

law and sets a workable and clear standard for email privacy, the potential benefits of new technology will never fully be realized.[191]

B. REVISE THE SCA: CURRENT PROBLEMS AND PROPOSED SOLUTIONS

Even though emails should be awarded the same level of protection as traditional forms of communication, they currently do not. Since the Fourth Amendment only protects people's "right to be secure" in spacial terms, its protections are far weaker when applied to information stored online.[192] As a result, Congress attempted to fill the gaps of protections awarded to electronic communications when they drafted the ECPA, specifically the SCA.[193] Nevertheless, as one author points out, it seems the drafters of the statute were unable to anticipate a basic difference between telephone conversations and email messages.[194] Just as the Wiretap Act was considered obsolete in 1986, so too has the SCA met a similar fate.[195] It is for these reasons that portions of the SCA are unconstitutional.[196]

1. *PROBLEM: Arbitrary Distinctions Lead to Illogical and Disparate Levels of Protection*

Currently, telephone calls and letters are granted more protections than stored emails. The Wiretap Act and the Pen Register statute regulate prospective communications and require that governmental officials obtain a warrant before intercepting the contents of a telephone call or a letter while in transmission. Stated differently, the government cannot open a letter while sitting at the post office or listen to a phone call as it is occurring without first obtaining a warrant. However, the SCA only regulates retrospective communications – communications that are "stored" as opposed to "in-transit."[197]

---

with City of Ontario v. Quon, 130 S. Ct. 2619, 2629-30 (2010) (insinuating a reluctance to extend to modern technology the quality of protection afforded to letters and telephone conversations).

191. Baker, *supra* note 72, at 113.

192. *See* Kattan, *supra* note 138, at 652 ("Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.").

193. Baker, *supra* note 72, at 81; *see* O'Connor, *supra* note 77, at 701-02 (noting how the SCA was created to fill in the privacy gaps created by the Fourth Amendment).

194. *See* Pikowsky, *supra* note 100, at 50.

195. *See* Baker, *supra* note 72, at 115 ("Both scholars and judges alike have noted that the Stored Communications Act is unable to provide robust and adequate protections against search of communications stored in a physical location but in an intangible form, predominantly online communications and e-mail conversations."); *see also* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008) ("The Internet presents a host of potential privacy issues that the Fourth Amendment does not address.").

196. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

197. Kerr, *supra* note 82.

In effect, if a given message is not in the process of transmission, then it is subject to lesser protections under the SCA.[198]

This disparity in the level of protection afforded against law enforcement searches does not make sense.[199] There is no reason that the ECPA provides greater protection against governmental intrusion to prospective communications "in-transit" than to retrospective communications that are "stored."[200] As mentioned earlier, stored emails have been considered functionally equivalent to earlier forms of communication,[201] so then why are the levels of protection not the same?

These arbitrary distinctions within the ECPA, specifically the SCA, overlook the basic privacy interests at stake.[202] The intended recipient of an email message has the same privacy interest regardless of whether law enforcement officials intercept the message while it is in transmission or whether law enforcement officials access it after it has already arrived in the recipient's electronic mailbox. A person's privacy interest in a file on his computer (or a paper document in his desk) behind office doors is equivalent to the privacy interest in a telephone call or an email message. As one author points outs, the current statutory scheme sets out greater safeguards against the interception of a communication traveling over the public Internet than it sets out against electronic trespass to a person's electronic mailbox for the purpose of reading that same communication in storage.[203]

There is no reason for this arbitrary distinction. In an effort to illustrate how illogical it is to afford stored emails less protection, the Wiretap Act regulates the government's action when they seek to monitor a telephone call as it is occurring, since they cannot monitor it retrospectively because there is no permanent record left after the conversation has ended.[204] In this situation, the government must first obtain a warrant. However, in comparison, an email message cannot only be intercepted in transmission as it travels from the sender to the recipient, but can also be accessed while it is stored in a recipient's mailbox. In this respect, an email message shares some characteristics

---

198. Recent Development, *A Thinly Veiled Request for Congressional Action on E-Mail Privacy: United States v. Councilman*, 19 HAR. J.L. & TECH. 211, 217-18 (2005); *see* Bowman, *supra* note 26, at 818 (describing the different levels of protection afforded to communications "in-transit" versus "stored").

199. *See* Pikowsky, *supra* note 100, at 59 (arguing that the different levels of protections afforded to stored emails is arbitrary and illogical).

200. *See id.* at 46 (arguing that inconsistent statutory provisions lead to confusion about interception of email during transmission and access to email in storage).

201. *See Warshak*, 631 F.3d at 286.

202. *See* Pikowsky, *supra* note 100, at 53 (arguing that arbitrary statutory distinctions will lead to illogical results).

203. *Id.*

204. *See id*. at 50.

with a paper letter, in that they both leave a permanent record of that communication.

According to the Pen Register statute, the government needs a warrant if they want to intercept the letter before it reaches a recipient's "real" mailbox, and they certainty need a warrant if they wish to seize that letter once it has reached its intended destination. Despite the fact that emails share the same purpose as letters and are displacing paper documents in general,[205] the SCA only requires the government to obtain a court order or a subpoena if they wish to monitor any "stored" email.[206]

The SCA does not only distinguish between the level of protection based on the type of server and whether the electronic communication was in-transit or stored, but it also provides for an illogical and arbitrary distinction based on the length of time the email has been stored.[207] For example, governmental officials must first obtain a warrant in order to compel an ECS provider to disclose the contents of an email message held in electronic storage for 180 days or less.[208] However, seemingly arbitrarily, the SCA provides less protection for an email stored for more than 180 days or emails stored with an RCS provider.[209] In this situation, the government does not necessarily need a warrant, but rather only needs to obtain a subpoena or a court order.[210]

As a result, this 180-day storage time frame distinction set out in section 2703 of the SCA is ineffective and a product of the past.[211] If the government could not search through that inbox without a warrant for the first 180 days, then why should they be able to search through that inbox in 181 days? Emails stored for one day longer than the allotted statutory time period are no more or less private than emails stored on day 180.[212] Due to the fact that technology today

---

205. Cuccia, *supra* note 54, at 710.
206. *See* 18 U.S.C. § 2703(a) (2009).
207. *See id*.
208. *See id*.
209. *See* 18 U.S.C. § 2703(b) (2009).
210. *See id*.
211. *See* Kattan, *supra* note 138, at 650 (illustrating how other commentators argue that the SCA's denial of warrant protection for emails stored longer than 180 days by an ECS is unconstitutional, as a user reasonable expects the same level of privacy in his communications on day 181 as on day 180); Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1068 (2008); Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 397 (2009).
212. *See* Kattan, *supra* note 138, at 652 ("Logically, if a communication deserves the protection of a warrant when sent through the mail, the same communication – even if opened and stored by the user for 181 days – deserves the protection of a warrant . . . ").

allows email account holders to store up to thousands of emails in their inbox for up to infinite amounts of time,[213] it goes to show how truly outdated the SCA stands today.[214] The Fourth Amendment does not depend on how long the information has been stored because the analysis concerns whether the government's inquiry covers a period of time and not when that period of time occurred.[215]

Applying a useful analogy, if compared to the situation of physical search, the logic of the SCA follows that a letter stored in a file cabinet for 180 days or less in a person's office would be afforded greater protection from search and seizure than the same letter in the same drawer that was stored for one day longer.[216] This time distinction may have been appropriate when technology was at its beginning stages,[217] but applying these time distinctions today is ineffective. It is not justified that the procedural hurdles the government has to face in order to search through your emails have been significantly lowered just because an email sat in an inbox for one day longer. Whether an electronic communication is "in-transit" or "stored" for 180 days or 181 days, the privacy interest remain the same, so the protections should be the same. However, the similarity between privacy interests is often neglected because monitoring a prospective communication (like a telephone call) must always be conducted covertly, while searching retrospective communications (like stored emails) are most often conducted with prior notice to the owner. While section 2703 normally requires prior notice to be given to the owner of an email account when the government has been issued a subpoena or a court order, section 2705 allows the government to do this without first providing notice.[218] Of course, prospective searches of emails in transmission must be conducted in secret without prior notice because no suspect would

---

213. *See* Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 146 (2012) (citing Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 145-46 (2008) ("Email providers' storage capacity increased as the cost of computer memory declined, allowing them to offer enormous storage capacity to their customers.")).

214. Pikowsky, *supra* note 100, at 70 (acknowledging how technological developments, since the ECPA was drafted, has failed to keep pace with our current society).

215. Bellia & Freiwald, *supra* note 121, at 173.

216. *See* Pikowsky, *supra* note 100, at 59.

217. *See* Kennedy, *supra* note 213, at 146 (providing an explanation for why Congress created the 180-day distinction when drafting the SCA). When email server memory was scarce and service providers did not retain opened messages, it could be assumed that an email message stored on a service provider's server for more than 180 days effectively had been abandoned by its intended recipient. *Id.* (citing Kerr, *supra* note 82, at 1234). Therefore, it might have been appropriate to permit governmental access to those communications upon presentation of less than probable-cause warrant. *Id.*

218. *See* 18 U.S.C. § 2703(b)(1)(B) (2009); 18 U.S.C. § 2705 (2009).

send incriminating information over email if he knew that the police would intercept it. However, retrospective searches, which access the contents of a stored email without notice to the account holder, constitute the same invasion of privacy as prospective interception of a message during transmission, if not more.[219]

As the SCA stands today, the government can compel an ISP to disclose the contents of a subscriber's email, do so without a warrant, and continue to do so without notifying the subscriber.[220] Consequently, this delay provision leaves open the possibility that individuals do not have the opportunity to refuse seizures that may be unlawful before Fourth Amendment violations occur.[221] In other words, by the time the subscriber finds out about the search and seizure, it is too late for the person to correct the violations of his or her privacy. This could result in additional leads and information that may be allowed as evidence, which would never have been obtained but for the violating of the privacy interest a user has in his email account.[222]

Warshak perfectly demonstrates this very scenario.[223] In *Warshak*, the government searched through Warshak's email without a warrant while delaying notice for almost a year.[224] By the time Warshak received notice of what was occurring, his Fourth Amendment rights had already been violated and the government had used his incriminating emails against him at trial.[225] The court agreed that the government violated Warshak's Fourth Amendment rights when they compelled his ISP to turn over the contents of his email without a warrant based on probable cause.[226] Therefore, the court was correct when it concluded that, to the extent that the SCA allows the government to obtain such emails without a warrant, the SCA is unconstitutional. Regardless of the medium of communication – whether it be by a telephone, a written letter, or a typed email – the government should be held to the same procedural standard since the privacy interests are the same.

---

219. *See* Pikowsky, *supra* note 100, at 55 (arguing that retrospective and prospective searches from law enforcement officials invades the same privacy interests).

220. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

221. Cuccia, *supra* note 54, at 704 (illustrating how sections 2703 and 2705 of the SCA allow the government to secretly seize and search the entirety of an individual's private email correspondence and affirmatively prevent the individual from learning of the intrusion at a point at which he could lodge a judicial challenge in advance of the seizure).

222. *Id.* at 711.

223. *See Warshak*, 631 F.3d at 282.

224. *See id.*

225. *See id.*

226. *See id.*

2. *SOLUTION: Eliminate Arbitrary Distinctions From Sections 2703 and 2705*

Courts need to follow the logic set out in *Warshak*. The *Warshak* decision increases the pressure to reform the variable treatment of different stored communications under the SCA, and acknowledges that stored emails have the same privacy interest as traditional forms of communication. Fourth Amendment protection for stored emails should not hinge on the arcane terms embedded in the SCA. Therefore, it is time for Congress to bring much needed simplicity to the scheme of electronic communications privacy.[227]

Congress needs to eliminate the 180-day distinction set out in the SCA. This proposed amendment would bring section 2703 in line with modern email technology. By eliminating the 180-day distinction, the amended SCA would afford full Fourth Amendment protection to all emails in electronic storage and finally acknowledge the privacy interests that exist and confirm that email users do reasonably expect their private communications to remain private and protected.

This proposed amendment would not burden law enforcement agents seeking to access these stored communications, nor would it burden the courts in interpreting the language of the SCA. In fact, eliminating this arbitrary distinction would create a uniform standard for both law enforcement agents and the courts[228] since the government would have the same burden whenever they sought to intercept or access any content-based communication. As society grows to view telephone and Internet technologies as essentially one of the same, any distinction will become increasingly out of touch with the privacy expectations of the American people.

3. *PROBLEM: Balancing Privacy Protections and Law Enforcement Interests Without Exceeding the Scope of the Search*

Email searches are not supposed to be an all-access pass for the government.[229] Since the SCA currently allows the government to search through the contents of one's stored emails without a warrant, the privacy invasions that result due to this surveillance are too broad. This causes the government to frequently exercise its power to access the contents of stored emails without limiting the scope of the

---

227. *See* Bellia & Freiwald, *supra* note 121, at 173 (advocating that the SCA needs to be amended or struck down to the extent that the SCA provides less than a warrant requirement as the procedural hurdle to access stored email).

228. *See* Kattan, *supra* note 138, at 649 (arguing that the creation of a uniform standard that requires the government to access any content-based communication would be beneficial).

229. Cuccia, *supra* note 54, at 712.

communications sought, substantially increasing the potential to violate one's Fourth Amendment rights.[230] The reason for that is because, in order for the government to obtain a warrant, they must meet the "probable cause" standard by particularity and specifically identifying the things to be seized. Whereas, since the SCA allows the government to obtain only a court order or subpoena for stored emails, the government only need to show "specific and articulable facts" showing "reasonable grounds" to believe that the contents of the communication "are relative and material to an ongoing criminal investigation;"[231] – a standard significantly lower than the probable cause required for a warrant.By not requiring warrant-level protection for all types of communication, the SCA is essentially allowing the government limitless opportunities[232] to jump over a far smaller procedural hurdle and ultimately allowing them to conduct a "back-door" search. As the *Warshak* court recognized, email is the modern day analogy to a telephone conversation. Accordingly, the compelled disclosure of stored email accounts has the same potential to be as hidden, continuous, indiscriminate, and intrusive as wiretapping. Therefore, stored emails need to be protected in order to prevent the government from exceeding the scope of their search, dancing on the line of a Fourth Amendment violation.

A perfect example of this type of overbroad search was seen in *Warshak*, where the government sought and ultimately seized approximately 27,000 of Warshak's stored emails, which contained his entire business and personal life.[233] While stored emails are analogous to the traditional letter, the possibility of overstepping the scope of the search for stored emails is far greater than that of a traditional letter.[234] Today, "individuals may store personal letters, emails, financial information, passwords, family photos, and countless other items of personal nature" since the current technology allows email accounts to store what has been said to be a "universe of private information."[235]

---

230. *See* Friess, *supra* note 134, at 994-95 (illustrating the overbroad and problematic consequences of governmental entities not sufficiently narrowing the scope of their searches).

231. Perry, *supra* note 8 (citing 18 USC § 2703(d)).

232. *See* 18 U.S.C. § 2705(a) (2009). Not only does the SCA provide less protection to stored emails by not requiring the issuance of a warrant, but it also allows the government to continuously delay notice to the owner – increasing the potential of violating the Fourth Amendment and decreasing the owner's ability to challenge this violation as it is occurring. *See id*.

233. *See* United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010).

234. Robert M. Goldstein & Martin G. Weinberg, *The Stored Communications Act and Private E-mail Communications*, CHAMPION MAGAZINE, Aug. 2007.

235. *See* Friess, *supra* note 134, at 995 (citing United States v. Mitchell, 565 F.3d 1347, 1351-52 (11th Cir. 2009)); United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (noting the ability of computers "to store and intermingle a huge array of one's

By its very nature, this increases the government's ability to conduct wide-ranging searches, and accordingly makes the particularity requirement that much more important.[236]

However, individual privacy under the Fourth Amendment must be viewed through the lens of two competing interests.[237] One of the legislators' foremost intentions in passing ECPA involved striking a balance between protecting people's privacy[238] and allowing the government reasonable access to communications for law enforcement purposes.[239] This goal must be kept in mind today.[240] Recently, legislators have acknowledged that "replicating [this] balance will be the key to any possibility of being successful on proposed legislation" intended to amend ECPA.[241]

From the law enforcement perspective, the Department of Justice believes that "ECPA has never been more important than it is now" since "criminals, terrorists, and spies" are using more advanced technologies to carry out their plans.[242] From a legislative perspective considering individuals' privacy interests, legislators recognize that recent technological developments require Congress to formulate clear privacy protections in order to safeguard these privacy interests.[243] However, as one author points out, the SCA fails to serve the interest of law enforcement, service providers, and customers because

---

personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs . . .").

236. *Otero*, 563 F.3d at 1132.

237. Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth*, 13 FL. COASTAL L. REV. 33, 58-59 (2011); *see* Kattan, *supra* note 138, at 652 (noting that the SCA reflects Congress's attempt to strike the right balance between the interests and needs of law enforcement and the privacy interests of the American people).

238. Ghoshray, *supra* note 237, at 59.

239. *See id.* at 58-59 (discussing the effects that the 9/11 terrorist attacks have had on granting broader surveillance power to the government resulting in overreaching tendencies of law enforcement and erroneous Fourth Amendment jurisprudence application).

240. *See* Bowman, *supra* note 26, at 831.

241. *Id.* at 831-32 (citing *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age*: Hearing Before the S. Comm. on the Judiciary, 112th Cong. 17, at 3 (2011) (statement of Sen. Coons)).

242. *Id.* at 832 (citing *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary,* 112th Cong. 17, at 5 (2011) (statement of James A. Backer, Associate Deputy Att'y Gen., U.S. Dept. of Justice).

243. *Id.* (citing *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 17, at 14 (2011) (statement of Sen. Al Franken)).

emerging technology "demonstrates that the SCA no longer 'strikes the right balance.'"[244]

4. *SOLUTION: Email Protections That Place No Greater Burden on Law Enforcement*

The answer is simple: provide stored emails the warrant-level protection they deserve. There is no justification for the ECPA to afford letters and telephone calls more protection than stored emails.[245] Since it is reasonable for email users to expect privacy in the content of their stored emails,[246] then extending Fourth Amendment protection to these communications is necessary. By requiring the government to first obtain a warrant, the Fourth Amendment protections would prevent the government from exceeding the scope of their investigation by conducting wide-ranging rummaging searches – the very concern the founders had when drafting the Fourth Amendment.[247]

Adoption of this principle would eliminate ECPA's present distinction between content stored on ECSs and similar content stored on RCSs. It would also eliminate the outdated time-in-storage distinctions since all stored content would be subject to a probable cause warrant requirement. In effect, by requiring the government to obtain a warrant to access stored emails, the government would need to demonstrate to a judge that there are sufficient facts for a reasonable person to believe that a search of a specific place will turn up evidence of a crime,[248] rather than simply showing "specific and articulable facts" showing "reasonable grounds" to believe that the contents of the communication "are relative and material to an ongoing criminal investigation."[249]

Even after taking into consideration the two competing interests between individual privacy and law enforcement purposes, it is still necessary to extend Fourth Amendment protection to stored emails. Yes, coupling the elimination of the 180-day distinction with the requirement of a warrant does make it slightly more difficult for law enforcement agents to obtain emails more than 180-days old, but "it does not afford email any protection greater than which is deemed

---

244. *See* Kattan, *supra* note 138, at 652 (arguing that the SCA is outdated and no longer protects the privacy interest as it was intended to do when enacted).

245. *See id.* at 646-47 (arguing that under the current framework, different standards of privacy protections for the same communication contracts users' reasonable expectation of their rights).

246. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

247. *See* Bowman, *supra* note 26, at 810.

248. *Id.* at 819.

249. Perry, *supra* note 8, at 352 (citing 18 USC § 2703(d)).

appropriate for functionally similar forms of communication", like telephone calls and traditional letters.[250] Quite to the contrary, creating a consistent warrant standard would benefit law enforcement by providing a predictable framework that would allow the government to act affirmatively to compel disclosure of electronic communications, without the risk that evidence will be deemed inadmissible.[251] Therefore, there is no compelling reason that stored emails should not receive the same level of protection as traditional forms of communication.

5. *PROBLEM: The SCA Does Not Have a Statutory Exclusionary Rule*

Even if a court finds that an email user does maintain a reasonable expectation of privacy,[252] the government did violate his Fourth Amendment's rights by not obtaining a warrant prior to compelled disclosure,[253] and the SCA is unconstitutional to that extent,[254] there is still one huge concern that is left: the SCA does not have a statutory exclusionary rule.[255] Unlike the Wiretap Act,[256] any evidence obtained in violation of the SCA is arguably admissible in court against a defendant unless a constitutional exclusionary rule is implicated.[257] That is because the SCA only allows for civil damages[258] and criminal punishment whenever violations occur,[259] but nothing more. Not only does the SCA fail to include exclusion as a remedy, it goes so far as to expressly rule out exclusion as a remedy.[260]

Moreover, some electronic communications that are illegally intercepted by the government may be admissible under the Fourth Amendment's analysis due to the good faith exception.[261] Therefore in effect, governmental officials can slide past the warrant requirement, seize any and all incriminating evidence found in your stored emails,

---

250. Bowman, *supra* note 26, at 832.
251. Kattan, *supra* note 138, at 649.
252. *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010).
253. *Id.* at 282.
254. *Id.*
255. Pikowsky, *supra* note 100, at 48.
256. *See* 18 U.S.C. § 2515 (2009) (providing, in relevant part, that "whenever any wire . . . communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial").
257. Pikowsky, *supra* note 100, at 48 (arguing that the better view would prevent the introduction of any evidence obtained in violating of the Stored Communications Act, but the Act's exclusive remedies provision may weaken this proposition).
258. *See* 18 U.S.C. § 2707 (2009).
259 *See* 18 U.S.C. § 2701(b) (2009).
260. *See* 18 U.S.C. § 2708 (2009).
261. *See* Leib, *supra* note 113.

and then use that evidence against you in a criminal trial.[262] This is exactly what happened to the defendant in *Warshak*.[263]

In *Warshak*, the government argued that they relied in good faith on the language of the SCA, which allowed the government to obtain Warshak's emails without procuring a warrant, and that any "hypothetical Fourth Amendment violation was harmless."[264] Even though the court did agree that the agents relied on the SCA in good faith, the court ultimately held that reversal of Warshak's criminal convictions – based in large part on the illegally intercepted emails obtained – was unwarranted.[265] Although the court held that the government did violate Warshak's Fourth Amendment rights, the primary rationale for the exclusionary rule is to deter future violations of the Fourth Amendment by the police, not to redress the past infringement on these rights.[266]

However, it is important to note that the court elaborated on its view of the good faith exception in a footnote.[267] The court noted:

> Though we may surely do so, we decline to limit our inquiry to the issues of good-faith reliance. If every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations. In other words, if the exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries.[268]

In effect, the court held that the emails were not subject to the exclusionary remedy if the officers relied in good faith on the SCA to obtain them.[269] The *Warshak* court cited to *Illinois v. Krull*, where the Supreme Court noted that the exclusionary rule's purpose of deterring law enforcement officers from engaging in unconstitutional conduct

---

262. United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).
263. *Id.*
264. *Id.*
265. *Id.*
266. *See* Ray, *supra* note 106, at 186; Illinois v. Krull, 480 U.S. 340, 347 (1987); United States v. Leon, 468 U.S. 897, 906 (1984) ("The exclusionary rule is neither intended nor able to 'cure the invasion of the defendant's rights which he has already suffered.").
267. United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).
268. *Id.*
269. *Id.* at 288. Since it was not plain or obvious that the SCA was unconstitutional, the court concluded that it was therefore reasonable for the government to rely upon the SCA in seeking to obtain the contents of Warshak's emails. *Id.* at 289.

would not be furthered by holding officers accountable for mistakes of the legislature.[270]

Even if a statute is later found to be unconstitutional, as the SCA was found to be unconstitutional in *Warshak*, any officer "cannot be expected to question the judgment of the legislature."[271] However, again, the court noted in a footnote that any future good faith argument has changed and now requires that a reasonable officer cannot assume that the Constitution allows for warrantless searches of private emails.[272]

6. *SOLUTION: Allow the Fourth's Amendment Exclusionary Rule to Apply to Stored Emails*

In order for the exclusionary rule to prohibit the introduction of a given piece of evidence at trial, police action in obtaining the evidence must trigger the Fourth Amendment.[273] In other words, there must have been a "search," implying that the defendant maintained a reasonable expectation of privacy.[274] While courts still remain reluctant to take on an email privacy cases, they must not wait for Congress to act before finding that email users do in fact have a reasonable expectation of privacy in their stored emails.

In the absence of adequate legislative answers or Supreme Court precedent, the test for Fourth Amendment protection should change to reflect changing technology and social norms. Courts should follow *Warshak's* lead and acknowledge that technological advances have made it more difficult to maintain control over personal information and adapt the subjective requirement to reflect this reality. The Supreme Court itself appears reluctant to address privacy expectations involving new technologies, in part because of its own lack of understanding and discomfort with such technology.[275]

While not forgetting the two bedrock principles *Warshak* introduced when finding an objective expectation to privacy in emails,[276] courts should accept the Internet, and the way people view the role

---

270. *Id.* at 282.
271. *Id.* at 288.
272. *Id.* at 289.
273. *See* Baxter, *supra* note 37, at 599.
274. *Id.* (citing Kyllo v. United States, 533 U.S. 27, 33 (2001) (quoting California v. Ciraolo, 476 U.S. 207, 211 (1986)).
275. *Id.* at 630.
276. *See* United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) (illustrating that when finding an objective expectation of privacy, courts must keep in mind that emails are being passed through a communications network but also that the Fourth Amendment must keep pace with the constant technological progressions).

the Internet plays in today's society[277] and how it has changed drastically since the SCA was passed.[278] Courts need to find that letters in the mail, telephone conversations, and email messages should all receive the same level of protection from secret interception by law enforcement officers.

However, since the courts err on the side of caution when extending full Fourth Amendment protection to new forms of communication,[279] it is time for Congress to address the ambiguities in the language of the SCA and update the statute to avoid arbitrary interpretation and application. The SCA is twenty-six years old and is not keeping pace in today's growing technological and Internet era.[280] Understandably so, since most of the current issues regarding the SCA involve technology that was not even considered possible, let alone in use at the time of the SCA's enactment.[281]

As a result, these problems cannot be fixed by judicial interpretation of the SCA.[282] Congress needs to step in and create a new framework that specifically deals with the new issues that have surfaced.[283] Because as of now, we are left with an outdated statute that has defeated its original goals of advancing technological privacy.[284]

---

277. *See* Mulligan, *supra* note 57, at 1559 (arguing that the ECPA was designed for an Internet that was dominated by the business, not personal, uses at the time the statute was adopted and therefore needs to be revised).

278. Bowman, *supra* note 26, at 825 (citing Mulligan, *supra* note 57, at 1597) (illustrating how the SCA was originally created with business' use of the Internet in mind and did not anticipate the personal use that characterizes the Internet today, for example the use of the Internet to send personal emails or use social networking websites).

279. *See* City of Ontarion v. Quon, 130 S. Ct. 2619, 2629 (2010) (illustrating how the court must be cautious when analyzing privacy expectations to newer forms of communication to reduce the likelihood of error of elaborating too fully on Fourth Amendment implications when it's role in society is not quite clear).

280. *See* Bowman, *supra* note 26, at 825 (acknowledging how the Internet has changed since the ECPA was adopted in the late 1980s); *but see* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (noting that the SCA has been in existence since 1986 and has not been the subject of any successful Fourth Amendment challenges, in any context, whether to § 2703(d) or to any other provision).

281. *See* Baker, *supra* note 72, at 115.

282. *Id.* "If judges are tasked with trying to fix issues that were unforeseen at the time of the SCA's enactment they would not be engaging in interpretation of the statute at all, but would cross the line into judicial activism, yet another reason for the legislature to step in." *Id.*

283. *Id.* (arguing that Congress needs to step in and establish a new framework to include new technologies).

284. *See* Bowman, *supra* note 26 at 825.

IV. CONCLUSION

If we do not want the government to use the evidence they illegally intercepted in a criminal trial against us, then something needs to be done. Courts, and ultimately Congress, need to answer the question as to how much privacy should be awarded to stored emails. The answer is simple: email communications should receive the same warrant-level protection as traditional telephone calls and paper letters have received. Emails are not only functionally equivalent to traditional forms of communication, but the purpose in communicating has not changed just because the manner in which we communicate has.[285] The privacy interest that is compromised when the police conduct a covert search remains the same regardless of whether the material seized exists in wire, electronic, or paper format and regardless of whether the material is intercepted during transmission or accessed from storage.[286] In other words, the Fourth Amendment and the ECPA, specifically the SCA, should provide the same level of protection from governmental searches to any medium of communication that is deemed worthy of protection at all and the same procedural safeguards should govern.

Currently, individuals are affected by both the courts' inability to tread a consistent path and the legislature's reluctance to provide them with adequate protections. Whether one wants to accept it or not, technology is growing at a very rapid pace. While many have turned to email as their new way of communication, they are currently left wary because the laws are years behind technology.[287] Under the current law, this wariness is not ungrounded; stored emails are subject to lesser protections of the SCA, if it applies at all. Simply put, under its current interpretation the SCA does not adequately guarantee the right to privacy, which is hampering, or at least delaying, technological advancement.[288]

While *Warshak* is currently only law within the Sixth Circuit, the decision is a significant one and may have been the catalyst to end the SCA, and at the very least, amend it. The discrepancies between the lack of a search warrant and trained agents searching through thousands of emails are more than adequate to alert, not only the courts, but Congress as well, that the current laws protecting electronic privacy are insufficient.

---

285. *See* Gavison, *supra* note 147, at 423-24.

286. *See* Pikowsky, *supra* note 100, at 92.

287. *See* Baker, *supra* note 72, at 114 (noting that without adequate privacy protections, many consumers fear that their data will be mishandled).

288. *Id.* at 115.

Nevertheless, even *Warshak* is not the end-all-be-all of cases on email privacy. Yes, it concluded that email users do maintain a reasonable expectation of privacy in their emails stored with third-party ISPs and that any search of those emails without a warrant violates the Fourth Amendment.[289] Despite these conclusions, the court did not reverse the defendant's criminal convictions. Even though the court found in Warshak's favor and respected his Fourth Amendment rights, at the end of the day, he was left with the feeling of invasion and a jury verdict that read "GUILTY." Congress has ample opportunity to remedy this defect; however, until they do, we are left with uncertainty as to how much privacy one really has in their email.

289. United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).