Berkeley Technology Law Journal

Volume 27
Issue 4 *Annual Review 2012*

Article 21

6-1-2012

A Way Forward After Warshak: Fourth Amendment Protections for E-mail

Courtney M. Bowman

Link to publisher version (DOI)
http://dx.doi.org/https://doi.org/10.15779/Z38Z98D

Berkeley
technology law journal
ANNUAL REVIEW OF LAW AND TECHNOLOGY

A Way Forward After Warshak*: Fourth Amendment Protections for E-mail*

Courtney M. Bowman

VOLUME 27
AR ONLINE
2012
UNIVERSITY OF CALIFORNIA, BERKELEY
SCHOOL OF LAW
BOALT HALL

A WAY FORWARD AFTER *WARSHAK*: FOURTH AMENDMENT PROTECTIONS FOR E-MAIL

Courtney M. Bowman†

In *United States v. Warshak*,[1] the Sixth Circuit held that the Stored Communications Act ("SCA"), enacted as part of the Electronic Communications Privacy Act ("ECPA") of 1986,[2] is unconstitutional.[3] The statute's unconstitutionality arises from two main problems with the SCA as it currently stands. First, the SCA predicates the extent of privacy protection on technological distinctions, mainly pertaining to e-mail storage, that are either insignificant or irrelevant today.[4] Second, the statute was tailored to meet the needs of businesses in the 1980s and is ill-suited to deal with the modern technological landscape in which the Internet is used largely for personal reasons.[5] This Note posits that a new or revised version of the SCA must address these important issues and, in so doing, must take into account a number of complicated factors, including the balance between government prosecution of suspected criminals, individuals' Fourth Amendment right to privacy, and the adaptability of any new law to forthcoming forms of technology.

Most important, however, is that legislators shift their approach from the one they adopted when they first drafted the SCA. Those revising the statute should focus on the *functionality* of email and minimize the unnecessary technological distinctions written into the current version that make the law difficult to apply. This approach will ensure that the amended law will remain applicable in the event of changes to the e-mail technology and to new communications technologies.

---

† J.D. Candidate, 2013, University of California, Berkeley School of Law.

1. 631 F.3d 266 (6th Cir. 2010).

2. Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1565 (2004).

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

4. 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, 1214 (2003–2004) (explaining that the SCA makes distinctions that "freez[e] into the law the understandings of computer network use as of 1986").

5. Mulligan, *supra* note 2, at 1597.

The goal of this Note is to provide a clear explanation of why the SCA was adopted, highlight the *Warshak* court's reasoning, and suggest a course of action in line with that reasoning that will allow Congress to implement an e-mail privacy protection scheme that makes sense in the context of the modern internet landscape. Part I gives an overview of the privacy concerns that persuaded Congress to adopt the SCA. Part II analyzes the *Warshak* case and highlights the profound implications this case may have on e-mail privacy protection. Part III provides an overview of major problems with the SCA, as well as several key issues Congress should consider in amending the law and recommendations for how the law could be amended effectively.

I. BACKGROUND: THE FOURTH AMENDMENT AS APPLIED TO COMMUNICATIONS PRIVACY

The Fourth Amendment prohibits unreasonable government searches and seizures and is the constitutional provision upon which e-mail privacy is based. It ensures that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[6]

The Fourth Amendment was adopted in part due to the founders' concerns about the use of general warrants,[7] which had issued in the colonies in the seventeenth and eighteenth centuries[8] and did not constrain those executing them in terms of where, when, or what they could search.[9] Instead, in the words of one commentator, general warrants acted as "legal pass key[s] to all doors" and put "everyone's privacy at the capricious mercy of [their] holder[s]."[10] Accordingly, in stating that a warrant must specify the places, people, or things subject to search and seizure, the language of the Fourth Amendment implies that the wide-ranging searches authorized by general warrants are unreasonable.[11]

6. U.S. CONST. amend. IV.

7. WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING, 602–1791, 709 (2009).

8. *Id.* at 241–42.

9. *Id.* at lxv.

10. *Id.*

11. *Id.* at lxiv–lxv.

A. FOURTH AMENDMENT CASE LAW: THE EVOLUTION OF COMMUNICATIONS PRIVACY

For the most part, the Supreme Court has extended Fourth Amendment protections to traditional as well as newer forms of communications technology. In the 1877 case *Ex parte Jackson*, for example, the Court ruled that the Fourth Amendment's warrant requirement applied to mail.[12] The defendant in that case was arrested for mailing a lottery circular in violation of a law that prohibited mailings of that kind.[13] The Court held that Fourth Amendment protections extended to materials that were "closed against inspection, wherever they may be,"[14] including letters and "sealed packages" in the mail.[15] Furthermore, the Court held that when such materials were in transit, government authorities who wished to open the mail could only do so with a warrant, "as is required when papers are subjected to search in one's own household."[16] The Court thus recognized a privacy interest in the content of people's postal communications.

In *Katz v. United States*,[17] the Court ruled that listening in on private telephone conversations also required a warrant and, in so doing, articulated the modern framework for determining the scope of privacy protection.[18] The defendant in this case was convicted of violating a law against transmitting gambling information over the phone.[19] In the course of the investigation, government authorities had attached an electronic device to the outside of a telephone booth used by the defendant in order to listen in on his telephone conversations.[20] The Court held that the defendant could rely on Fourth Amendment privacy protections while using the phone booth because he could not expect that his conversation would be shared with the public and that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[21] Since the government had not obtained a search warrant before listening in on the call, the Court held that the government had conducted an impermissible search in part because "searches conducted

12. 96 U.S. 727, 733 (1877).
13. *Id.* at 727.
14. *Id.* at 733.
15. *Id.*
16. *Id.*
17. 389 U.S. 347 (1967).
18. *Id.* at 361 (Harlan, J., concurring); Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1050 (2008).
19. *Katz*, 389 U.S. at 348.
20. *Id.*
21. *Id.* at 352.

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."[22] The Court thus used what is now the modern framework for determining the scope of Fourth Amendment protection.[23] As summarized by Justice Harlan in his concurrence, this framework stipulates that the Fourth Amendment protects one's communications when (1) a person has a subjective understanding of privacy in a given situation and (2) society would deem such an expectation reasonable.[24]

However, the Court also has been cautious in extending full Fourth Amendment protection to new forms of communication, at times refraining from making a wide-ranging decision until the societal role of a particular form of communication becomes more apparent.[25] For example, in the 2010 case *City of Ontario v. Quan*,[26] the Court had to determine whether it was reasonable for the city police department to order transcripts of the text messages Quan sent from an employer-provided device.[27] The Court ultimately determined that even if Quan enjoyed a reasonable expectation of privacy in his text messages, the search itself was reasonable and therefore did not violate the Fourth Amendment.[28] In so holding, the Court noted that it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment" because "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[29] The *Quan* decision therefore illustrates that, although the Court is willing to extend Fourth Amendment protection to newer forms of electronic communication, it is hesitant to do so without a more complete understanding of the potential reverberations of such a decision.[30]

It is important to note that, although the *Katz* framework has proven very influential in determining the scope of Fourth Amendment privacy protection, it is not the sole determinant of the limits of such protection. In January 2012, the Supreme Court decided *United States v. Jones*[31] and, in so

22. *Id.* at 357.
23. Oza, *supra* note 18.
24. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); Oza, *supra* note 18, at 1049–50.
25. City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).
26. *Id.* at 2619.
27. *Id.* at 2624–26.
28. *Id.* at 2633.
29. *Id.* at 2629.
30. *Id.*
31. United States v. Jones, 132 S. Ct. 945 (2012).

doing, underscored the Amendment's respect for privacy in one's property. Stating that "for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates,"[32] the Court ruled that people have a right to privacy in their physical property.[33] It held that the Fourth Amendment still protects this right and that, despite the Court's articulation of the "reasonable expectation of privacy" test in *Katz*, that test does "not narrow the Fourth Amendment's scope."[34]

B. THE THIRD PARTY DOCTRINE

Although the Court has recognized that people are entitled to some amount of privacy in their communications, the so-called Third Party Doctrine limits the amount of privacy people can expect and is especially pertinent in analyzing e-mail privacy due to the role third parties play in e-mail communication. The Third Party Doctrine provides that when an individual knowingly supplies information to a third party, his expectation of privacy is diminished because that person is assuming the risk that the third party may reveal the information to government authorities.[35] As a result, information imparted to third parties generally falls 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.[36] In applying this reasoning in a series of decisions known as the "business records" cases,[37] the Court found that the government could subpoena a defendant's account records from his bank (since the bank was a third party to this information)[38] and a defendant's telephone dialing records from his telephone provider[39] (since the providers

32. *Id.* at 950 (quoting U.S. CONST. amend. IV).

33. *Id.* at 950–51.

34. *Id.* at 951.

35. *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("It is well-settled that 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.").

36. *See* Mulligan, *supra* note 2, at 1562.

37. *Id.*

38. *See* United States v. Miller, 425 U.S. 435, 444 (1976). The court here found that Miller had no "legitimate 'expectation of privacy' in [the] contents" of the bank records because they were exclusively comprised of "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442. In so doing, 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.

39. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

were acting as third parties).[40] Given the role of third parties in the process of sending e-mails, which is explained in greater detail in Part I.C.1, *infra*, the Third Party Doctrine proved to be a major concern when e-mail use developed and became more prevalent.[41]

C. ECPA BACKGROUND: AN ATTEMPT TO EXTEND FOURTH AMENDMENT PROTECTIONS TO E-MAIL

By the mid-1980s, Congress realized it needed to update existing law in order to protect the privacy of electronic communications.[42] At the time, Title III of the Omnibus Crime and Safe Streets Act covered communication interception, but the law only applied to voice transmissions by common carriers.[43] This meant that the protections the law afforded to voice communications did not apply to data, video, and other electronic communications that were becoming more prevalent, because, at the time of Title III's passage in 1968, "Congress could not appreciate—or in some cases even contemplate—telecommunications and computer technology" advances and, accordingly, did not address such concerns in Title III.[44] As a result of these gaps in protection, companies in the communications industry began to lobby for legislation that could address their concerns arising from the seeming lack of privacy safeguards for these increasingly popular forms of technology.[45] One particular worry was that, in light of the business records cases, e-mail would be granted lower standards of privacy protection due to

40. Mulligan, *supra* note 2, at 1562. The court in *Smith* 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." *Smith*, 442 U.S. at 741 (emphasis in original). The court then determined that neither Smith nor society in general could have an expectation of privacy in phone numbers dialed because these numbers voluntarily and necessarily were imparted to the telephone company in the course of making a phone call, and therefore callers were taking the risk that this dialing information could be given to the police. *Id.* at 742–45. Professor Achal Oza points out that a number of scholars have referred to this determination as the court's distinction between "content information" and "envelope information," in which people may have a recognized right of privacy in the enclosed content of their messages but not in routing information that must remain visible to others in order to send the communication properly. *See* Oza, *supra* note 18, at 1049.

41. Mulligan, *supra* note 2, at 1563.

42. *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) [hereinafter *1986 ECPA Hearings*] (statement of Rep. Robert W. Kastenmeier, Chairman, S. Comm. on Courts, Civil Liberties, and the Administration of Justice).

43. 132 CONG. REC. S7991 (daily ed. June 19, 1986) (statement of Sen. Leahy).

44. *Id.*

45. *1986 ECPA Hearings*, *supra* note 42, at 1–2 (statement of Rep. Robert W. Kastenmeier, Chairman, S. Comm. on Courts, Civil Liberties, and the Administration of Justice).

the role of third-party servers in transmitting and storing e-mail.[46] 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.[47] Congress subsequently passed ECPA in an effort "to ensure that the new technological equivalents of telephone calls, telegrams, and mail are afforded the same protection provided to conventional communications."[48]

Despite Congress's intention to close the gaps in privacy protections in the digital age, the statute, as drafted, created additional confusion about the extent of e-mail privacy. Furthermore, in spite of lawmakers' stated intent that ECPA provide equal levels of protection to traditional and more modern forms of communication,[49] the statute instead provided a lower level of protection to e-mail than it did to letters and phone calls. Before analyzing how the structure and language of ECPA led to such a result, however, an explanation of e-mail technology as it existed in the 1980s and a detailed overview of the statute itself is warranted.

1. E-mail Technology

An understanding of e-mail technology is important in determining the scope of protection one's e-mails receive under ECPA since these statutory protections generally hinge on how a user accesses his or her e-mail,[50] as well as how long and where a given email has been stored.[51] When a user composes an e-mail and clicks the "send" button, a program called Simple Mail Transfer Protocol ("SMTP") transmits the e-mail from the user's computer to the server belonging to the user's e-mail provider.[52] The server then determines how to route the e-mail and sends it to the server of the recipient's e-mail provider.[53] As the e-mail travels from one server to another, it passes through a network of routers, leaving whole or partial copies of itself on these routers along the way.[54] Once the e-mail arrives at the

46. Mulligan, *supra* note 2, at 1563.
47. *Id.* at 1565.
48. *1986 ECPA Hearings*, *supra* note 42, at 2 (statement of Rep. Robert W. Kastenmeier, Chairman, S. Comm. on Courts, Civil Liberties, and the Administration of Justice).
49. *Id.*
50. Oza, *supra* note 18, at 1050.
51. Mulligan, *supra* note 2, at 1568.
52. Oza, *supra* note 18, at 1051–52.
53. *Id.* at 1052.
54. Mulligan, *supra* note 2, at 1562–63.

receiving e-mail provider's server, it remains there until the recipient opens her e-mail program and retrieves the e-mail.[55]

There are several means by which a user can retrieve her e-mail, depending on whether she uses a Post Office Protocol ("POP"), Internet Message Access Protocol ("IMAP"), or web-based e-mail program. If she is using a POP program, her e-mail will reside on the server until the user tells her e-mail program (such as Microsoft Outlook) to retrieve the e-mail.[56] The e-mail program then uses POP to transfer the e-mail from the server to the user's computer via download.[57] Once the message is downloaded to the user's computer, the service provider deletes its copy of the e-mail on its server.[58]

In contrast, both IMAP and web-based programs leave copies of e-mails on the servers even after a user has viewed the e-mails. An IMAP program shows a user the e-mails that are stored on the provider's server, but does not delete these e-mails from the server.[59] A web-based e-mail service such as Gmail is similar in that it allows a logged-in user to view her e-mails without deleting them from the server.[60]

There are a number of advantages to using an IMAP or web-based service instead of a POP service. One advantage of using an IMAP or web-based e-mail service is that a user can access her e-mail from many different locations since it is stored on a server, rather than downloaded to a single computer.[61] Servers can also serve as storage and backup systems for IMAP and web-based e-mail users. If the user's computer crashes or is infected by a virus, for example, an IMAP user would be able to retrieve backup copies of her e-mail from the server, whereas a POP user who has downloaded copies of her e-mail to her computer and deleted them from the server would not

55. Oza, *supra* note 18, at 1052.

56. *Id.*

57. *Id.*

58. *Id.* Some POP services allow users to leave a copy of a downloaded e-mail on the server instead of deleting the e-mail from the server. *See Using Email*, MEDIATEMPLE, http://kb.mediatemple.net/questions/272/Using+Email#gs/how-pop-works (last visited Jan. 22, 2012). Users can instruct their POP clients to store e-mail in this manner. Usually, however, the POP client deletes e-mails from the server once a user downloads them. *See* Marshall Brain & Tim Crosby, *How E-Mail Works*, HOW STUFF WORKS, http://communication.howstuffworks.com/email4.htm (last visited Jan. 22, 2012).

59. Oza, *supra* note 18 at 1053.

60. *Id.* at 1053–54.

61. *IMAP vs. POP: What's the Difference?*, UNIVERSITY OF MINNESOTA E-MAIL AND INTERNET ACCOUNTS GUIDES, http://www1.umn.edu/adcs/guides/e-mail/imapvspop.html (last visited Dec. 20, 2011).

have such a backup.[62] Despite these differences, however, an e-mail sender cannot tell what kind of e-mail retrieving program an intended recipient is using.[63]

The ability of e-mail to provide such short- and long-term storage capacity was particularly relevant when the statute was drafted in the 1980s.[64] Before computer spreadsheet programs were adopted widely as efficient number-crunching tools, servers often provided remote storage services that allowed users to copy large amounts of their information to off-site computers in order to process data efficiently.[65] This type of storage, typically offered at offsite facilities, was known as remote computing service ("RCS").[66] Providers also offered electronic communications service ("ECS"), which was the temporary storage required to send or receive e-mails.[67] Many providers could act as both ECS and RCS providers, so the type of service a provider performed varied depending on the communication at issue.[68] For example, a service provider acted as an ECS provider for unopened e-mails remaining on the server, while the same service provider acted as an RCS provider when it hosted a document stored at one of its storage sites.[69] If a user downloaded an e-mail onto his computer and took it off the server (by using a POP program, for example), the service provider no longer served a storage function in regard to that particular e-mail.[70]

The nature of 1980s e-mail technology had several important implications, particularly its susceptibility to the Third Party Doctrine. In the 1980s, businesses began using e-mail on a more regular basis and accordingly became concerned about the privacy the e-mails would receive.[71] The Third Party Doctrine particularly worried e-mail users because e-mail service providers and networks acted as third parties when they transmitted and stored e-mails, meaning that, under the Court's business records holdings, the government could request or subpoena e-mails from any of the third parties charged with transmitting or storing them.[72] Congress worried that

62. *Id.*
63. Oza, *supra* note 18, at 1051.
64. Kerr, *supra* note 4, at 1213–14.
65. *Id.*
66. *Id.* at 1214.
67. *Id.*
68. *Id.* at 1215.
69. *Id.* at 1216.
70. *Id.* at 1216–17.
71. Mulligan, *supra* note 2, at 1559–62.
72. *Id.* at 1562–63.

the public would be hesitant to use electronic communications systems if people's privacy could not be safeguarded, and this was one of the concerns that prompted Congress to pass ECPA in 1986.[73]

Despite these intentions, however, the technical distinctions written into ECPA, particularly its Stored Communications Act ("SCA") provisions, have prevented this legislation from serving this goal satisfactorily. Although the SCA did provide e-mail some protection from the reach of the Third Party Doctrine, its language has been the source of much confusion as e-mail technology has grown more advanced. The next section of this note provides an overview of the structure of ECPA, which serves as a background for an explanation of why the SCA is problematic.

2. Structure of ECPA

ECPA is comprised of three statutes: the Wiretap Act at 18 U.S.C. §§ 2511–2522 (Title I), the Pen Register statute at 18 U.S.C. §§ 3121–3127, and the focus of this Note, the Stored Communications Act ("SCA"), at 18 U.S.C. §§ 2701–2711 (Title II).[74] The Wiretap Act and Pen Register statute apply to electronic communications that are traveling between users. These two acts give electronic communications similar protection to what letters and phone calls receive and prohibit the government from intercepting the content of electronic messages while the messages are in transit, although the Pen Register statute allows for the installation of certain devices in some instances to collect "non-content" data.[75] Most circuits read the Wiretap Act's text, specifically the word "intercepts"[76] that is included in the text, to make the statute applicable only to messages that are in transit from one user to another.[77] Under this theory, if a given message is not in the process of transmission, then it is subject to the protections of the SCA.[78]

---

73. *Id.* at 1564–65.

74. *Id.* at 1565.

75. *Id.* at 1565–67.

76. 18 U.S.C. § 2511(1) (2006).

77. *A Thinly Veiled Request for Congressional Action on E-Mail Privacy: United States v. Councilman*, 19 HARV. J.L. & TECH. 211, 217–18 (2005).

78. *Id.* Though this is the majority view, the statute is ambiguous as applied to current technology and may be interpreted differently. This is because e-mail messages are temporarily copied and stored on servers as they make their way from one user to another. Therefore, if a message is en route to its final destination but is intercepted while it is in temporary storage on a server (as opposed to traveling between servers), the interception conceivably could be covered by the Stored Communications Act instead of the Wiretap Act because it technically is in storage. *See id.* at 216–17. This ambiguity is another example of the difficulties caused by ECPA's "language of pre-digital-age privacy protections." *Id.* at 217. For an example of how this conundrum has played out in court, see United States v.

The SCA, the section of ECPA that regulates communications that are "stored" as opposed to "in transit," has proven particularly contentious because it mandates different levels of privacy protection based on how long e-mails have been stored on a server after reaching their destinations.[79] The statute is based on the ECS and RCS distinction, effectively "freezing into the law the understandings of computer network use as of 1986."[80] Specifically, § 2703 requires that the government obtain a warrant in order to compel an ECS provider to disclose a particular user's e-mails if those e-mails have been in temporary storage for 180 days or fewer.[81] In order to obtain a warrant, the government must meet the "probable cause" standard;[82] that is, the government must 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.[83] However, if the government wishes to obtain e-mails that have been in temporary storage for over 180 days, or e-mails that are stored with an RCS provider, the standards the government must meet are lower.[84] Although the government may seek a search warrant,[85] it may also compel disclosure with a subpoena or a court order issued upon a showing of "specific and articulable facts"[86]—a standard that is lower than the probable cause required for a warrant[87]—along with prior notice to the subscriber under investigation.[88] However, prior notice can be delayed for 90 days if notification may produce an "adverse result"[89] that "jeopardiz[es] an investigation."[90] Since any e-mails that a user downloads to his computer and removes from the server (by using a POP program, for example) are no

Councilman, 373 F.3d 197 (1st Cir. 2004), *rev'd on rehearing en banc*, 418 F.3d 67 (1st Cir. 2005), discussed *infra* Section I.D.4.

79. *See* Mulligan, *supra* note 2, at 1569; Oza, *supra* note 18, at 1044–46 (explaining through a hypothetical how the law creates different expectations of privacy based on storage time).

80. Kerr, *supra* note 4, at 1214.

81. 18 U.S.C. § 2703(a).

82. Fed. R. Crim. P. 41(d)(1).

83. *Search Warrants*, ELECTRONIC FRONTIER FOUNDATION, https://ssd.eff.org/your-computer/govt/warrants (last visited Feb. 25, 2012).

84. Kerr, *supra* note 4, at 1218.

85. 18 U.S.C. § 2703(b)(1)(A).

86. *Id.* § 2703(d).

87. Patricia L. Bella & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 128 (2008).

88. 18 U.S.C. § 2705 (1986).

89. *Id.* § 2705(a)(1)(B).

90. *Id.* § 2705(a)(2)(E).

longer stored by the server, these downloaded e-mails are subject not to the SCA but to typical Fourth Amendment protections.[91]

D. OVERVIEW OF ISSUES WITH THE SCA

Although the SCA—and ECPA as a whole—shielded email from the reach of the Third Party Doctrine to some extent, it raised an assortment of other issues that have compounded as e-mail technology has developed over time. Despite the seemingly clear-cut distinctions made by the statute, changes in e-mail technology and courts' differing statutory interpretations have rendered numerous provisions of the SCA ambiguous and the application of certain privacy standards questionable. Most of these issues relate to e-mail storage, an area that has changed greatly both in terms of technology and people's perceptions since the SCA was adopted.[92] In evaluating a course of action after *Warshak*, legislators should be aware not only of the SCA's unconstitutionality, but also of the conflicts the SCA has fostered in practice so they can adequately resolve these areas of confusion.

1. The 180 Day Distinction Mandates Different Levels of Privacy Protection Based on How Long an E-mail Has Been Stored on a Server

Despite legislators' declared intentions to give e-mail the same protections afforded to letters and phone calls,[93] the 180 day distinction mandates a comparatively lower level of privacy protection for e-mails that have been stored for more than 180 days.[94] Specifically, the government must obtain a warrant under the "probable cause" standard in order to access e-mails that have been stored for 180 days or fewer, while the government need only satisfy the less-stringent "specific and articulable facts" standard required to obtain a subpoena in order to access e-mails that have been stored for more than 180 days.[95]

The reasons Congress implemented this rule remain unclear.[96] Congress might have viewed any e-mails stored over 180 days as abandoned and

91. Kerr, *supra* note 4, at 1216–17.

92. *See* Oza, *supra* note 18, at 1045–46 (explaining how e-mail providers' expanded storage capabilities have prompted users to leave their e-mail stored on servers for longer periods of time).

93. *See 1986 ECPA Hearings*, *supra* note 42, at 2 (statement of Rep. Robert W. Kastenmeier, Chairman, S. Comm. on Courts, Civil Liberties, and the Administration of Justice) ("Congress needs to act to ensure that the new technological equivalents of telephone calls, telegrams, and mail are afforded the same protection provided to conventional communications.").

94. Oza, *supra* note 18, at 1057.

95. 18 U.S.C. §§ 2703(a)–(b); Oza, *supra* note 18, at 1056–57.

96. Bellia & Freiwald, *supra* note 87, at 161.

therefore less deserving of protection.[97] Furthermore, it is possible that, given the e-mail storage limitations in the 1980s, Congress did not foresee people keeping e-mail in storage for more than 180 days on a regular basis.[98]

Regardless of the reason Congress implemented this rule, the distinction is not a practical one today. People now routinely keep their e-mails for more than 180 days, partly because e-mail providers have the ability to store large amounts of e-mail and make them searchable by users, which encourages a user to store her e-mail indefinitely.[99] In fact, these "dramatic developments" in e-mail providers' storage capabilities and customers' willingness to take advantage of these capabilities recently were cited in Congressional hearings as reasons why Congress needs to consider amending ECPA.[100] Considering these technological changes, e-mails that have been stored for more than 180 days now do not seem any less deserving of the protection provided by the "probable cause" standard, despite that fact that the statute makes this distinction.[101]

2. *Different Levels of Privacy Protection Depending on How Users Retrieve E-mails*

Under the SCA, e-mails are afforded different amounts of privacy protection based purely on how users choose to retrieve their e-mails.[102] If a person uses a POP program, which downloads e-mails to the user's computer and deletes them from the server upon retrieval,[103] these retrieved e-mails are out of the reach of the SCA since the statute only applies to service providers and the government must obtain a warrant in order to gain access to the e-mails, regardless of how long they have been stored because they only reside on the individual's personal computer.[104] However, if a person uses an IMAP or web-based program, the e-mails remain on the server and therefore are subject to the SCA, including its 180 day

97. Kerr, *supra* note 4, at 1234; Oza, *supra* note 18, at 1045.

98. Bellia & Freiwald, *supra* note 87 at 162; Oza, *supra* note 18, at 1061 n.124.

99. *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 10 (2010) [hereinafter *2010 ECPA Reform Hearing*] (prepared statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy and Technology).

100. *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 (2011) [hereinafter *2011 ECPA Hearing*] (statement of Sen. Coons).

101. Oza, *supra* note 18, at 1068–69.

102. *Id.* at 1054.

103. *See IMAP vs. POP: What's the Difference?*, *supra* note 61.

104. *See* Oza, *supra* note 18, at 1059–61.

distinction.[105] Therefore, the level of protection for e-mails varies based on the type of program a person is using, with POP-retrieved e-mails generally remaining subject to the a warrant requirement and IMAP and web-based e-mails subject to the SCA's 180 day distinction.[106]

This difference in treatment is significant for a number of reasons. First, IMAP programs generally are considered more advantageous than POP,[107] yet e-mails retrieved using POP receive greater privacy protection than e-mails retrieved with IMAP, potentially counseling against the adoption of the more technologically advanced IMAP standard by users concerned about their privacy. Furthermore, these results seem arbitrary when considered from the perspective of an e-mail sender, who cannot tell whether the recipient of her e-mail is using a POP, IMAP, or web-based program to retrieve e-mail.[108] It even is likely that the recipient is not aware of the type of e-mail retrieval program he is using, thereby making the SCA's distinction seem arbitrary and unjustifiable based on user habits.

3. Conflicting Statutory Interpretations of "Electronic Storage"

Further complicating the SCA's storage-based distinction is the conflicting statutory interpretations of the term "electronic storage."[109] The term is a key one in the SCA, since the statute allows for a cause of action against a person who has intentionally gained unauthorized access to an electronic communication when that communication "is in electronic storage."[110] Although the statute defines the term "electronic storage" as "temporary, intermediate storage . . . incidental to . . . electronic transmission" or alternatively, "storage . . . for purposes of backup protection,"[111] the phrase's precise meaning in practice has proven contentious enough to cause a split in interpretation between the federal government and the Ninth Circuit.[112] Currently, the government advocates a definition of "electronic storage" that excludes e-mails people have accessed and the Ninth Circuit has held that the definition includes accessed e-mails.[113]

105. *Id.*
106. *Id.* at 1060–61.
107. *See IMAP vs. POP: What's the Difference?*, *supra* note 61.
108. *See* Oza, *supra* note 18, at 1051.
109. 18 U.S.C. §§ 2701(a)(1), 2707(a) (2006).
110. *Id.* § 2701(a).
111. *Id.* § 2510(17).
112. OFFICE OF LEGAL EDUCATION, SEARCHING AND SEIZING COMPUTERS 123 (2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.
113. *Id.* at 123–25.

The origin of this interpretive split was *Theofel v. Farey-Jones*.[114] The case arose during discovery in another case between the same parties. The defendant, Farey-Jones, requested that his lawyer subpoena the plaintiffs' ISP so the defendant could access the plaintiffs' e-mails.[115] The lawyer drafted a subpoena that was overbroad in violation of the Federal Rules of Civil Procedure.[116] However, the defendant was able to read the unlawfully subpoenaed e-mails before a magistrate judge struck down the subpoena.[117] The plaintiffs then brought a suit against the defendant alleging, among other things, a violation of the Stored Communications Act.[118]

The case hinged on the court's statutory interpretation of the term "electronic storage." Defendants maintained that since the messages had been delivered to the intended recipients at the time the defendants accessed them, the e-mails had not been in "electronic storage" and therefore were outside the purview of the SCA.[119] However, the court believed that there was "no dispute that messages remaining on NetGate's server after delivery [were] stored 'by an electronic communication service.' "[120] In contrast to other courts that had limited the "temporary, intermediate storage" classification to e-mails that had not yet been delivered, the *Thoefel* court focused instead on whether the messages were stored as a form of "backup."[121] The court concluded through a "plain language" reading of the Act that the ISP's copy of the message served as a "backup" for its subscriber and that, since "nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user[,] [s]torage under these circumstances thus literally falls within the statutory definition" of electronic storage.[122] Accordingly, the court reversed the lower court's dismissal of the plaintiffs' SCA claim.[123]

As a result, the Ninth Circuit construed the category of "electronic storage" in a wider fashion than did the government.[124] Currently, the Ninth Circuit includes previously accessed e-mail in its definition and thereby affords it the more stringent privacy protection afforded to e-mails in ECS,[125]

114. 359 F.3d 1066 (9th Cir. 2003).
115. *Id.* at 1071.
116. *Id.* at 1071–72.
117. *Id.*
118. *Id.* at 1072.
119. *Id.* at 1075.
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.* at 1079.
124. OFFICE OF LEGAL EDUCATION, *supra* note 112.
125. *Id.* at 123–25.

while the government views electronic storage as "temporary storage made in the course of transmission by a service provider and . . . backups of such intermediate communications made by the service provider to ensure system integrity,"[126] which effectively excludes e-mail that has been accessed by recipients from electronic storage and relegates it to RCS categorization and its less-stringent protections.[127] The government's guide to prosecutors seeking guidance on how to deal with such issues advises its readers that prosecutors outside the Ninth Circuit should apply the government's "traditional interpretation," while prosecutors within the Ninth Circuit should follow that court's directives.[128] This interpretive split, therefore, has profound implications on e-mail security because it creates a significant difference in the amount of privacy protection e-mail users can expect solely based on their geographic locations.

4. The "In Transit" and "In Storage" Distinctions

Another significant area of controversy is the distinction between e-mails that are "in transit" and those that have reached their destinations and are "in storage." This is an important distinction because if an e-mail is intercepted while in transit, the Wiretap Act applies, but an e-mail that is accessed while it is in storage falls under the SCA.[129] This distinction was at issue in *United States v. Councilman*,[130] in which Councilman, an ISP operator, was accused of violating the Wiretap Act by writing a program that copied subscribers' incoming e-mails before the e-mails reached their destinations.[131] A First Circuit panel took a strict textual approach when it looked at the statute and determined that the e-mails at issue were in storage, not transit, when they were copied by the program and therefore fell outside the act.[132] Despite the fact that the e-mails had not yet reached their intended recipients, the court held that since the messages were within the computer system's random access memory or hard disks, they had been in temporary storage when Councilman's employees had accessed them.[133] The First Circuit, sitting en

126. *Id.* at 123.

127. *See Theofel*, 359 F.3d at 1077 (stating that the court, unlike the government, does not believe that a user's having opened an e-mail necessarily relegates that message to storage); Mulligan, *supra* note 2, at 1569 (explaining the implications of the government's interpretation).

128. OFFICE OF LEGAL EDUCATION, *supra* note 112.

129. *A Thinly Veiled Request for Congressional Action on E-Mail Privacy: United States v. Councilman*, *supra* note 77, at 217–18.

130. 373 F.3d 197 (1st Cir. 2004), *rev'd on rehearing en banc*, 418 F.3d 67 (1st Cir. 2005).

131. *Id.* at 199.

132. *Id.* at 203.

133. *Id.*

banc, then reversed this decision.[134] After examining the text and legislative history of the Wiretap Act, the court determined that "the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications."[135] Accordingly, the e-mails in question were in transit when Councilman's employees intercepted them, and Councilman could be prosecuted under the Wiretap Act.[136] The case demonstrates that even the technological distinctions that seem clear-cut within the SCA can be ambiguous and confusing when applied to technology in practice.

5. The Internet Has Changed Since ECPA was Adopted in the 1980s

As a twenty-six-year-old statute in an age of rapid technological change, one of the main sources of problems with ECPA, and the SCA in particular, is the outdated nature of the statute. The Internet itself, as well as the way people use and think about the Internet, has changed dramatically since ECPA was passed in 1986, rendering the original goals of the statute at odds with its current application.[137] The statute was created with business' use of the Internet in mind and did not anticipate the personal use that characterizes the Internet today.[138] The transcripts of the House Judiciary Committee hearings on ECPA reflect this approach, as they contain scant mention of personal privacy issues that should inform a statute such as ECPA—witnesses instead focused on business-related issues such as teleconferencing, the need to protect trade secrets,[139] and companies' desire for Congress to implement "clear standards" regarding when the government can access companies' subscriber data.[140] Significantly, at the time of ECPA's adoption, there had been very few cases of the government accessing e-mail accounts in the context of criminal investigations.[141]

134. United States v. Councilman, 418 F.3d 67, 84 (1st Cir. 2005) (en banc).

135. *Id.* at 79.

136. Councilman likely was concerned about whether the Wiretap Act or the SCA applied, not because of any differences in the punishment proscribed by the two acts, but because the government had only charged him with violating the Wiretap Act. Therefore, had the court held that Councilman's actions fell outside the scope of the Wiretap Act, he could not be found guilty of that particular charge. *See Id.* at 69.

137. Mulligan, *supra* note 2, at 1559 (arguing that 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).

138. *Id.* at 1597.

139. *1986 ECPA Hearings*, *supra* note 42, at 4 (statement of Sen. Patrick J. Leahy).

140. *Id.* at 21 (statement of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association).

141. *Id.*

However, internet usage has changed dramatically since ECPA was enacted.[142] Today, the Internet is not just a technology used by businesses. Instead, a substantial portion of internet usage is personal in nature. Individuals use the Internet to send personal e-mails, access cloud computing networks, and use social networking websites, among other activities.[143] This major societal shift suggests that ECPA must be revised so it can better protect individuals as they use the Internet for personal reasons.[144]

Despite all these interpretative difficulties and the dynamic nature of technology, the statute has remained unchanged since its inception twenty-six years ago.[145] The *Warshak* case and its constitutional holding, however, may be the catalyst that prompts Congress to revisit the statute.

II. THE *WARSHAK* DECISION

The importance of *United States v. Warshak*[146] lies not just in its holding that the SCA is unconstitutional, but the manner in which the court approached the decision. Instead of focusing on the technological minutiae relating to e-mail storage set out in the SCA, the court reached its decision by analogizing e-mail to other forms of communication in order to determine the proper extent of protection.[147] In so doing, the court highlighted the best approach to amending the SCA: recognizing that e-mail is an important form of personal communication and affording it privacy protection on that basis, rather than on the basis of its complicated and dynamic underlying technology.

The SCA faced its first constitutional challenge in *Warshak*.[148] The plaintiff in this case, Steven Warshak, was the owner and president of Berkeley Premium Nutraceuticals, which produced a popular supplement called Enzyte. In 2006, Warshak and several of his associates were indicted for mail fraud, bank fraud, money laundering, and additional offenses related to their operation of the company.[149]

---

142. *2010 ECPA Reform Hearing*, *supra* note 99, at 1 (statement of Rep. Jerrold Nadler, Chairman, S. Comm. on the Constitution, Civil Rights, and Civil Liberties); Mulligan, *supra* note 2, at 1597.

143. *2010 ECPA Reform Hearing*, *supra* note 99, at 1 (statement of Rep. Jerrold Nadler, Chairman, S. Comm. on the Constitution, Civil Rights, and Civil Liberties).

144. *Id.*; Mulligan, *supra* note 2, at 1597.

145. Oza, *supra* note 18, at 1045.

146. 631 F.3d 266 (6th Cir. 2010).

147. *Id.* at 285–86.

148. Susan Freiwald & Patricia L. Bellia, *The Fourth Amendment Status of Stored E-Mail: The Law Professors' Brief in Warshak v. United States*, 41 U.S.F. L. REV. 559, 559 (2007).

149. *Warshak*, 631 F.3d at 281.

The privacy issue in this case involved the way the government authorities investigating Warshak employed the SCA to obtain Warshak's e-mails. During its investigation, the government requested, pursuant to the SCA, that Warshak's ISP, NuVox, start preserving the e-mails Warshak sent and received.[150] NuVox complied, and after the ISP had stored the e-mails for several months, the government compelled NuVox to disclose them.[151] Warshak did not find out that the government had compelled the disclosure of his e-mails until a year later.[152] Warshak subsequently accused the government of violating his Fourth Amendment rights by obtaining his private e-mails without a warrant.[153]

In 2010, the Sixth Circuit Court of Appeals held that the government violated Warshak's Fourth Amendment rights by forcing the disclosure of the e-mails without a warrant.[154] The court began its analysis by determining whether the government's actions constituted a "search" under the Fourth Amendment.[155] First, the court used the two-part inquiry from *Katz* to determine whether Warshak had a reasonable expectation of privacy in his emails.[156] Under this standard, the court considered a subjective element—whether Warshak had an expectation of privacy in his e-mails—and an objective element—whether society recognized an expectation of privacy in e-mails.[157] The court quickly determined that the "often sensitive and sometimes damning substance of his e-mails" clearly indicated that Warshak expected his e-mails to remain private since "people seldom unfurl their dirty laundry in plain view."[158]

With the subjective element settled, the court moved on to the objective component of the test. The court began by examining the expectations of privacy that accompanied "traditional forms of communication" like letters and phone calls as set out in *Ex parte Jackson* and *Katz*.[159] Based in part on the holdings in these cases, the court determined that both forms of communication carried with them "a reasonable expectation of privacy" that the government would be held to violate if it recorded people's phone calls

150. *Id.* at 283.
151. *Id.*
152. *Id.*
153. *Id.* at 282.
154. *Id.* at 274.
155. *Id.* at 284.
156. *Id.*
157. *Id.*
158. *Id.*
159. *Id.* at 285.

or intercepted letters in transit without a warrant.[160] As a result, "[g]iven the fundamental similarities between e-mail and traditional forms of communication, it would defy common sense to afford e-mails lesser Fourth Amendment protection" than that afforded to phone calls and mail.[161] In so holding, the court dismissed claims that the ability or right of a third party, such as an ISP, to access e-mail contents diminished a subscriber's reasonable expectation of privacy.[162] While the court did note that an ISP's intention to "audit, inspect, and monitor" a subscriber's e-mails as expressed within the context of a subscriber agreement may "render an expectation of privacy unreasonable," there was no such language in Warshak's agreement with NuVox.[163]

Having determined that e-mail users, therefore, are afforded a reasonable expectation of privacy in the contents of their e-mails, the court held that since an "ISP is the functional equivalent of a post office or a telephone company" and that e-mail "is the technological scion of tangible mail,"[164] the government's compelling an ISP to turn over a subscriber's e-mails constitutes a search under the Fourth Amendment and therefore requires a warrant.[165] Since government agents did not procure a warrant prior to compelling NuVox to turn over Warshak's e-mails, the agents' actions violated Warshak's Fourth Amendment rights.[166] Furthermore, the court ruled that "to the extent that the SCA purports to permit the government to obtain such e-mails warrantlessly, the SCA is unconstitutional."[167] In so holding, the court stated that depriving e-mail "strong protection under the Fourth Amendment" would render the Fourth Amendment "an ineffective guardian of private communication, an essential purpose it has long been recognized to serve."[168]

The court's decision carries with it a number of highly significant implications. First, the court declared that the SCA was unconstitutional on its face, not just unconstitutional as applied to Warshak's case.[169] This aspect of the decision is crucial, since it makes the holding much broader and renders the decision more threatening to the continued existence of the SCA

160. *Id.*
161. *Id.* at 285–86.
162. *Id.* at 286–87.
163. *Id.* at 287.
164. *Id.* at 286.
165. *Id.*
166. *Id.* at 288.
167. *Id.*
168. *Id.* at 286.
169. *Id.* at 288.

as it currently stands.[170] Second, the court's constitutional analysis was not based purely on existing case law such as *Ex parte Jackson* and *Katz*, nor did it rely on any of the technological distinctions written into the SCA, such as those between ECS and RCS. Instead, the court arrived at its conclusion by comparing e-mail to its more traditional communicative counterparts and giving great credence to its important societal role as a communications medium.[171] This reasoning is important because it provides a guideline for legislators in amending the law; namely, by focusing on the overall role and functionality of e-mail rather than technological distinctions that could make any amendment quickly outdated or more difficult to apply. The next Part contains a comprehensive analysis of the problems with the SCA and applies the reasoning in *Warshak* to suggest possible amendments to the SCA.

III. AMENDING THE SCA

Now that the *Warshak* court has declared the SCA unconstitutional, it is time to reevaluate the current e-mail privacy protection scheme. *Warshak* is particularly instructive in this regard. Not only did the court declare the SCA unconstitutional,[172] perhaps providing the catalyst needed to encourage Congress to amend the law, but it also set out the best framework for evaluating how to amend the SCA—namely, by focusing on e-mail's role as a communications medium rather than focusing on its underlying technology. However, amending the SCA will be a complicated process due to all the competing interests that must be considered in order for the resulting statute to serve its purpose adequately. This Part presents different factors that Congress should take into account when considering how to amend or replace the SCA in light of the issues discussed above and offers recommendations about how the law should be amended. This Part then analyzes why a legislative, not judicial, approach is the most efficient and effective way to solve these privacy protection issues.

A. ISSUES AND PROPOSED SOLUTIONS

1. Issue: The Public's Reasonable Expectation of Privacy in E-mail

The court's reasoning in *Warshak* is important because it may indicate how the public thinks about e-mail, which in turn helps determine the extent of privacy protection e-mail should receive under the Fourth Amendment.

170. In contrast, an "as applied" ruling only applicable to Warshak's case would make the holding more limited (i.e. applying only to cases similar to *Warshak*) and less of a challenge to the statute itself.

171. *Warshak*, 631 F.3d at 286.

172. *Id.* at 288.

According to the test laid out in *Katz*, the Fourth Amendment provides protection to a form of communication when a person has a subjective expectation of privacy and society has an objective interest in privacy in a given communication.[173] Therefore, what individuals and society as a whole think about e-mail is important in determining the extent of privacy protection it receives.

The *Warshak* court's analysis may be indicative of the way the public thinks about e-mail today and thus is important in determining the scope of privacy protection for e-mail. Rather than focusing on the technical minutiae of how an e-mail winds its way from one user's inbox to another and making its decision based solely on these technicalities, the court emphasized "the fundamental similarities between e-mail and traditional forms of communication," like letters and telephone calls.[174] This analogy served as the basis for the court's ruling that e-mail should be afforded the same protection letters and phone calls receive; namely, that the government should have to obtain a warrant before searching an individual's e-mail.[175] Since this view is less technologically-based and more focused on e-mail's role as a communications service, it is more likely that this view represents the public perception of e-mail, since regardless of any competing public views of how e-mail technology works, the public is likely to think of e-mail primarily as a mode of communication.

The *Warshak* court is not alone in its reasoning, as some scholars have favored an approach that eschews the technical distinctions of the SCA in favor of viewing e-mail as a communications medium and extending Fourth Amendment protections to it accordingly.[176] Since these proposals correspond to the public's likely conception of e-mail as primarily a mode of communication, these views are instructive as to how the public thinks about e-mail and, accordingly, its expectation of privacy in e-mail. For example, Professors Patricia L. Bellia and Susan Freiwald believe that stored e-mail should receive the same Fourth Amendment protection afforded to phone calls and letters because e-mail has replaced these more traditional channels of communication.[177] According to Bellia and Freiwald, e-mail is "at least as important as the telephone" in modern communication and contains the same private information as telephone calls, thereby rendering government

173. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Oza, *supra* note 18, at 1049–50.

174. *Warshak*, 631 F.3d at 285–86.

175. *Id.* at 286.

176. *See* Bellia & Freiwald, *supra* note 87, at 138; Mulligan, *supra* note 2, at 1579 .

177. Bellia & Freiwald, *supra* note 87, at 138.

searches of private e-mail accounts "at least as intrusive as surveillance of other forms of communication."[178] Stored e-mails, in particular, contain much of this private information and therefore are deserving of full Fourth Amendment protection, instead of the limited protection the SCA currently provides.[179] Professor Mulligan also advocates for more stringent Fourth Amendment protection based on technological displacement, arguing since "e-mail is a replacement for telephone communications as well as postal mail," it should receive protection similar to that afforded to the other two mediums.[180]

Both the *Warshak* opinion and these scholarly proposals illustrate the extent to which e-mail is considered a communications medium in the public eye. Since the public most likely considers e-mail to be a mode of communication and holds a corresponding expectation of privacy in e-mail, e-mail should be protected to the same extent as other forms of communication, rather than being subjected to lesser protection based purely on its storage capabilities, as it currently is under the SCA. Given the constitutional implications of this public perception, Congress needs to keep this perspective in mind when drafting an amended SCA.

a) Solution: A Statute that Corresponds to the Public's Understanding and Expectations of Privacy

The provisions in the SCA relating to e-mail storage—namely, the 180 day provision and the distinctions the statute makes between ECS and RCS storage—should be eliminated. The bases for these distinctions are outdated and largely irrelevant today[181]; accordingly, they do not correlate to the public's understanding of e-mail technology and almost certainly do not figure into the average person's expectation of privacy in his e-mail account. A statute that eliminates the differing levels of protection for e-mails based on storage type and time and gives e-mail the same protection afforded to phone calls and letters more directly corresponds to the public's expectation of privacy and understanding of the nature of e-mail communication.

2. Issue: Maintaining the Privacy Protection-Law Enforcement Balance

One of legislators' foremost intentions in passing ECPA involved striking a balance between protecting people's privacy and allowing the

178. *Id.*
179. *Id.*
180. Mulligan, *supra* note 2, at 1579.
181. *See* Oza, *supra* note 18, at 1045–46 (explaining that at the time the SCA was adopted, the government reasonably could infer that e-mails left on the server after 180 days were abandoned, but that such an inference would not be warranted today).

government reasonable access to communications for law enforcement purposes, and this goal must be kept in mind today.[182] Recently, legislators have acknowledged that "[r]eplicating [this] balance will be the key to any possibility of being successful on proposed legislation" intended to amend ECPA.[183] On the law enforcement side, 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.[184] On the other hand, legislators recognize that the recent developments such as cloud computing programs and social networking websites require Congress to formulate clear privacy protections in order to safeguard individuals' personal information and communications in order to promote the growth of these technology-based businesses.[185]

a) Solution: E-mail Protections That Place No Greater Burden on Law Enforcement

E-mail should receive the same extent of protection afforded to phone calls and letters. Under an SCA amended pursuant to this Note's proposal, law enforcement officials who wish to access e-mail from an individual's account will have to obtain a warrant, regardless of how long the e-mail has been in storage. Although this modification makes it more difficult for law enforcement to obtain e-mails more than 180 days old, it does not afford e-mail any protection greater than that which is deemed appropriate for other functionally similar forms of communication. Indeed, even the Department of Justice recognizes that the 180 day distinction in particular is in need of revisiting and has expressed its willingness to work with legislators in

182. *2011 ECPA Hearing*, *supra* note 100, at 3 (statement of Sen. Chuck Grassley) (stating that ECPA is "a carefully crafted compromise" that strikes "a balance then between privacy and law enforcement"); *2010 ECPA Reform Hearing*, *supra* note 99, at 2 (statement of Rep. Jerrold Nadler, Chairman, S. Comm. on the Constitution, Civil Rights, and Civil Liberties) ("[W]e must consider whether ECPA still strikes the right balance between the interests and needs of law enforcement and the privacy interests of the American people."); 132 CONG. REC. S7991 (daily ed. June 19, 1986) (statement of Sen. Leahy) ("These provisions are designed to protect legitimate law enforcement needs while minimizing intrusions on privacy of system users as well as the business needs of electronic communications system providers.").

183. *2011 ECPA Hearing*, *supra* note 100, at 3 (statement of Sen. Chuck Grassley).

184. *Id.* at 5 (statement of James A. Baker, Associate Deputy Att'y Gen., U.S. Dept. of Justice).

185. *Id.* at 14 (statement of Sen. Al Franken) ("[Companies] are losing business because they cannot definitively tell their prospective clients when and how the Government will access their information. Because of this uncertainty, people are not deciding to put their documents on the cloud.").

addressing this specific provision,[186] thereby suggesting that law enforcement may be amenable to such as solution.

Furthermore, the proposed revisions to the SCA do not interfere with the Third Party Doctrine. While the doctrine as a whole is controversial,[187] eliminating the doctrine entirely likely would allow criminals to use third parties to hide their illegal activity because law enforcement would have to obtain a warrant before gathering evidence about any criminal activity.[188] Therefore, instead of advocating for the wholesale elimination or revision of this doctrine, e-mail should be afforded the same amount of protection as the phone calls and letters to which it is analogous.[189]

3. Issue: Applicability to Future Technology

Congress should also consider whether it wants to amend the SCA so it is a technology-specific or technology-neutral law. Congress could adopt a technology-specific statute tailored to the current state of e-mail as we know it, or adopt a more general, technology-neutral statute focused on the communicative role of e-mail, which would result in a statute flexible enough to apply to variations on this current technology. Despite the fact that a technology-specific statute might better address the "subtlety and nuance" of e-mail technology,[190] a technology-neutral statute may prove more enduring and efficient. As explained in Section I.D, *supra*, the SCA's technological distinctions and definitions have led to significant confusion in interpreting the statute as technology has progressed. This history suggests that legislators charged with revising or replacing the SCA should not tie the language of the Act so strongly to the current state of e-mail infrastructure that the law cannot be adapted to encompass new forms of e-mail and communications technology without substantial legislative revisions. In other words, Congress should strongly consider removing many of the technology-specific

186. *Id.* at 12 (statement of James A. Baker, Associate Deputy Att'y Gen., U.S. Dept. of Justice).

187. *See generally* Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009) (summarizing and evaluating critiques of the Third Party Doctrine).

188. For example, a person could order third parties to commit a crime on his behalf "knowing that the police could not send in undercover agents, record the fact of his phone calls, or watch any aspect of his internet usage without first obtaining a warrant." A world without a Third Party Doctrine, then, would allow criminals to hide their activities more easily. Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 576 (2009).

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

190. Paul Ohm, *The Argument Against Technology-Neutral Surveillance Laws*, 88 TEX. L. REV. 1685, 1696 (2010).

provisions from the SCA and instead adopt a technology-neutral statute that could be adapted more easily and efficiently to emerging technologies.

Some scholars believe Congress should adopt technology-specific legislation across the board. Professor Paul Ohm, for example, has highlighted what he believes are a number of advantages of technology-specific laws.[191] He believes that technology-specific surveillance laws in particular force Congress to re-evaluate these statutes on a more regular basis due to continuous technological advancements.[192] This in turn increases Congress's role in determining the extent of surveillance and, accordingly, makes surveillance law subject to "more participatory democratic oversight."[193] He further claims technology-neutral laws may risk being overinclusive if they are applied to new technologies that were not included in the deliberation and research that helped formulate the statute at its time of adoption.[194] The solution he suggests is that Congress should not pass legislation regarding a particular technology until Congress has taken the time to understand that particular technology so as to "tailor" laws that are appropriate for that technology.[195]

The legislative history of ECPA, however, shows that a technology-specific approach to e-mail privacy protection would be impractical. Specifically, it shows that, even when Congress knows that it needs to amend a particular statute, the logistics behind drafting or amending a law are onerous and lengthy. For example, the House Judiciary Committee has been holding hearings about amending ECPA since 2010,[196] yet no solution has been reached. Given this legislative history, the more practical option would be to forgo the potentially substantial period that would be required to pass a technology-specific law under Professor Ohm's approach and instead pass a technology-neutral law that regulates e-mail based on its overall communicative function and could be applied regardless of changes in its underlying technology.

a) Solution: Technological Neutrality Accounts for Future Innovation

The SCA, as it currently stands, is an example of how detailed technological distinctions, such as the SCA's storage-based provisions, can

191. *See generally* Paul Ohm, *The Argument Against Technology-Neutral Surveillance Laws*, 88 TEX. L. REV. 1685 (2010) (describing the benefits of technologically-specific laws).

192. *Id.* at 1686.

193. *Id.*

194. *Id.* at 1697–98.

195. *Id.* at 1695.

196. *2010 ECPA Reform Hearing*, *supra* note 99, at 2.

make a law outdated and difficult to apply in a relatively short amount of time.[197] Therefore, Congress should amend the SCA by removing these technology-based distinctions and revising the statute so as to make it technology-neutral. The law often lags behind technology,[198] so a less-specific law that focuses more on a medium's overall function than details likely will guarantee a longer life for the legislation.

B. THE IMPORTANCE OF A LEGISLATIVE SOLUTION

Notwithstanding the logistical difficulties inherent in adopting a legislative amendment to the SCA, a solution in the form of a statute is preferable to relying on judicial interpretation to provide a clear solution. As discussed above, judicial interpretation of the SCA already has led to a circuit split regarding the definition of "electronic storage."[199] The *Warshak* decision only adds to this confusion, as the court's determination that the SCA is unconstitutional currently is law only within the Sixth Circuit.[200] Adding to this unevenness is the fact that some courts may be less willing to take on these determinations than others: some, like the *Quon* court, may prefer to wait until the role of a particular technology has solidified,[201] while others, like the *Warshak* court, may be ready to make significant constitutional interpretations about the law.[202] As a result, individuals' privacy protections currently vary from jurisdiction to jurisdiction and more variation could occur in the future. The most effective way to remedy this disparity is for Congress to adopt a statute that resolves these conflicts on a national level rather than to allow courts to make their own, likely conflicting, determinations.

IV. CONCLUSION

Although *Warshak* is currently only the law within the Sixth Circuit, the decision is a significant one and may spell the end of the SCA as we know it. In amending the statute, legislators will have to address a number of interrelated considerations, including public opinion related to e-mail and the balance between law enforcement needs and the public's desire for privacy in

197. *See supra* Section I.D.

198. *See* Berger v. State of New York, 388 U.S. 41, 49 (1967) ("The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge.").

199. *See supra* Section I.D.3.

200. *2011 ECPA Hearing*, *supra* note 100, at 58 (statement of Cameron F. Kerry, General Counsel, U.S. Dept. of Commerce).

201. City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

202. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

communications. However, by following the spirit of *Warshak* and enacting a statute that correlates to the public's use and conceptions of e-mail, rather than one that is based on the underlying technology, Congress should be able to pass a new law that will regulate e-mail privacy effectively for years to come.