
NOTES

AMEND THE ECPA: FOURTH AMENDMENT PROTECTION ERODES AS E-MAILS GET DUSTY

*Achal Oza**

INTRODUCTION	1044
I. FOURTH AMENDMENT PROTECTION FOR INFORMATION REVEALED TO THIRD PARTIES	1047
A. <i>Historical Background of the Fourth Amendment</i>	1047
B. <i>Knowledge Requirement: Smith v. Maryland</i>	1048
C. <i>The Content/Envelope Distinction</i>	1049
II. THE ECPA: THIRD-PARTY DOCTRINE APPLIED TO E-MAIL COMMUNICATIONS	1050
A. <i>Overview of E-mail Technology: Three Hypothetical Recipients</i>	1050
1. Post Office Protocol	1052
2. Internet Message Access Protocol	1053
3. Web-Based E-mail	1053
B. <i>The EPCA</i>	1054
1. The ECPA's 180-Day Distinction	1056
2. The Content/Envelope Distinction Applied to E-mail.....	1057
3. Application of the ECPA to Three Hypothetical Recipients	1059
4. The ECPA Case Study.....	1062
III. SIXTH CIRCUIT PANEL HELD 180-DAY DISTINCTION UNCONSTITUTIONAL	1062
A. <i>Warshak v. United States: Factual Background and District Court Ruling</i>	1063
B. <i>The Sixth Circuit Panel Ruling</i>	1064
C. <i>Sixth Circuit Exception for ISP Waiver of Privacy Expectation Through Auditing</i>	1066
D. <i>En Banc Rehearing and Implications of Warshak</i>	1067
IV. PROPOSAL TO AMEND THE ECPA	1068
A. <i>Proposed Amendment</i>	1068

* J.D. Candidate, Boston University School of Law, 2009. M.S., Computer Systems Engineering, Northeastern University, 2006. B.S., Electrical Engineering & Computer Science, University of California, Berkeley, 2003. I would like to thank Professor Tracey Maclin and Daniel V. McCaughey for their guidance in helping me formulate this Note topic.

B. <i>Proposed Amendment Applied to Three Hypothetical Recipients</i>	1071
CONCLUSION.....	1072

INTRODUCTION

Imagine two e-mail users, Jack and Jane. Jack and Jane each receive the same e-mail from Tommy Trafficker. Jack uses Microsoft Outlook to read Tommy's e-mail while Jane uses Google's Gmail service to read Tommy's e-mail. Because Jack is using Outlook, the e-mail from Tommy is transferred from Jack's e-mail service provider to Jack's laptop. Because Jane is using Gmail, however, her e-mail from Tommy remains on Google's server and is not transferred to Jane's laptop.

One-hundred-eighty days pass. Suppose the government – lacking probable cause – suspects Jack and Jane of trafficking drugs and wants to read the e-mails they received from Tommy. Because Jack's e-mail is stored on his laptop in his home and not on his e-mail service provider's server, the government can only read the e-mail through seizure of his laptop.¹ However, the government cannot obtain a warrant because it lacks probable cause, thus Tommy's e-mail to Jack remains private.

Jane's e-mail, however, is stored on Google's server. The Electronic Communications Privacy Act of 1986 ("ECPA") § 2703 governs Fourth Amendment protection of e-mails stored on third-party servers.² Section 2703 requires that the government obtain a warrant to read e-mails stored with an e-mail service provider for 180 days or less.³ Jane's e-mail from Tommy has been in storage for exactly 180 days. The government lacks probable cause and, therefore, cannot meet the warrant requirement. Accordingly, the government can read neither Jack's nor Jane's e-mails from Tommy.

One day passes. The government still lacks probable cause and Jack's e-mail from Tommy remains on his laptop. Accordingly, the government still cannot obtain a warrant to seize Jack's e-mail and Tommy's e-mail to Jack remains private. Jane's e-mail from Tommy has now been in storage on Google's server for longer than 180 days. Section 2703 of the ECPA no longer ensures that this e-mail will receive full Fourth Amendment protection at a probable cause standard.⁴ Under the ECPA, the government – still lacking

¹ See *infra* note 116 and accompanying text.

² 18 U.S.C. § 2703(a) (2000). Section 2703(a) states:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.

Id.

³ *Id.*

⁴ *Id.*

probable cause – can now compel Google to disclose the contents of Jane’s e-mail from Tommy.⁵

One-hundred-eighty-one days after Tommy sent identical e-mails to both Jack and Jane, the government, lacking probable cause, is unable to compel disclosure of Jack’s e-mail but is able to compel disclosure of Jane’s e-mail. Jane receives less Fourth Amendment protection than Jack because Jack used Outlook while Jane used Gmail. This ought to strike an average e-mail user as strange.

Congress enacted the ECPA over twenty years ago.⁶ At that time e-mail technology was still maturing.⁷ The ECPA reflects the technology of the 1980s: most e-mail users routinely downloaded their messages to a home computer and would never have considered permanently storing messages with their service provider.⁸ This practice demonstrates the technological limitations of using a modem, tying up a phone line, and downloading communications at an incredibly slow speed.⁹ For example, the industry standard for modems in 1985 was 2400 bits per second.¹⁰ It would take 2.5 minutes at that speed just to download the Constitution of the United States of America.¹¹ Accordingly, if a user did not download his e-mails to his home computer within six months, a reasonable inference might be drawn that the user had abandoned his e-mails.¹² Today, however, a user could download an

⁵ 18 U.S.C. § 2703(b) (2000) (authorizing a governmental entity to require a provider of remote computing services to disclose the contents of any electronic communication held or maintained on that service for more than 180 days under certain circumstances); 18 U.S.C. § 2705 (2000).

⁶ 18 U.S.C. § 2510 (2000) (effective Oct. 21, 1986).

⁷ There were an estimated one million e-mail users in the United States in 1986 compared to an estimated 210 million in 2007. *Compare Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 475 (1986) [hereinafter *ECPA Hearings*] (memorandum from ACLU Project Staff), with Li Weitao, *Internet Users to Log In at World No. 1*, CHINA DAILY, Jan. 24, 2007, http://www.chinadaily.com.cn/china/2007-01/24/content_790804.htm.

⁸ See *infra* note 124 for a discussion of the committee hearings that explored how individuals used e-mail technologies in 1986.

⁹ *ECPA Hearings*, *supra* note 7, at 24 (testimony of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association).

¹⁰ Victor P. Nelson, *New Products: 2400-Baud Modem Aims at Business Market*, IEEE MICRO, Feb. 1985, at 81, 81, available at <http://csdl.computer.org/comp/mags/mi/1985/01/04089379.pdf>.

¹¹ A plain text version of the United States Constitution is 45,118 bytes. See U.S. CONST., available at <http://www.usconstitution.net/const.txt>. A 2400 bits per second (“bps”) modem can transfer up to 300 bytes per second (“Bps”) because there are 8 bits in a byte. At 300 Bps, it would take 2.51 minutes to transfer a 45,118 byte file.

¹² See *infra* note 124 for an explanation of Congress’s inclusion of a 180-day distinction in the ECPA based on people’s tendency to download all of their e-mails to their personal

entire season of a television series in that same 2.5 minute time span.¹³ With the advent of always-on broadband and web based e-mail sites that offer nearly unlimited storage, many users choose to permanently store their e-mails off site.¹⁴ An average e-mail user would be surprised to learn that her choice to store e-mails off-site could affect the extent of Fourth Amendment protection she receives regarding governmental access to her e-mails.

This Note argues that Congress should amend § 2703(a) of the ECPA to bring it in line with modern technology and practices. Part I of this Note provides an overview of Fourth Amendment protection for information revealed to third parties. It explains the historical background of the Fourth Amendment, the evolution of third-party doctrine, the requirement to *knowingly* reveal information to third parties, and the content/envelope distinction. Part II of this Note explains how third-party doctrine is applied to the e-mail context. It first provides a detailed analysis of the technology behind e-mail and presents three hypothetical e-mail users who each use slightly different technologies. Part II then discusses the Electronic Communications Privacy Act of 1986, with an emphasis on the 180-day distinction the ECPA draws between e-mails in storage that are afforded full Fourth Amendment protection at a probable cause standard and those e-mails which are not. Following this discussion of the ECPA, Part II then applies the ECPA to the three hypothetical e-mail users to show the varying results. Part II concludes with a case study of the ECPA. Part III of this Note discusses *Warshak v. United States*,¹⁵ a case which shows that courts are ready to hold the 180-day distinction unconstitutional. Finally, Part IV of this Note proposes an amendment to § 2703(a) of the ECPA which would resolve the inconsistent Fourth Amendment protection of e-mails.

computers in the 1980s.

¹³ The approximate size of a forty-five minute television show is 200 megabytes. See iTunes Store: Download Times Will Vary, http://support.apple.com/kb/HT1577?viewlocale=en_US (last visited Aug. 31, 2008). High-speed internet is commonly available at speeds up to twenty megabytes per second. See RCN – High Speed Broadband Internet, <http://www.rcn.com/internet/index.php> (last visited Aug. 31, 2008). Thus, a forty-five minute show can be downloaded in approximately ten seconds or fifteen shows in 2.5 minutes.

¹⁴ See, e.g., Yahoo! Mail – Unlimited Storage!, <http://help.yahoo.com/l/us/yahoo/mail/original/tools/tools-08.html> (last visited Aug. 31, 2008) (“Unlimited storage gives normal email account users like yourself an opportunity to not have to worry about hitting a storage limit. Basically, the idea is that now you can save your correspondence and memories and never worry about deleting older messages to make room for more.”).

¹⁵ 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

I. FOURTH AMENDMENT PROTECTION FOR INFORMATION REVEALED TO
THIRD PARTIES

A. *Historical Background of the Fourth Amendment*

The Fourth Amendment requires that searches by the government must be reasonable.¹⁶ Courts historically contextualized Fourth Amendment protection with property rights.¹⁷ The Supreme Court shifted that focus in 1967 with *Katz v. United States*,¹⁸ stating that “the Fourth Amendment protects people, not places.”¹⁹ With this change in focus, the Court initiated the modern era of privacy protection.²⁰ Under this paradigm, an individual has an expectation of privacy where (1) the individual possesses a subjective expectation of privacy; and (2) that expectation is “one that society is prepared to recognize as ‘reasonable.’”²¹

Third-party doctrine governs the Fourth Amendment privacy protection for information revealed to third parties.²² The starting point is that “when an individual reveals private information” to a third party, that individual “assumes the risk” that the third party may reveal the information to authorities.²³ If the third party willingly reveals that information to the authorities, the government does not violate the Fourth Amendment by using it.²⁴ Moreover, an individual assumes this risk even where she reveals information to a third party within the context of a confidential relationship.²⁵ The question then becomes: under what circumstances does an individual *knowingly* reveal information to a third party?

¹⁶ U.S. CONST. amend. IV.

¹⁷ *Katz v. United States*, 389 U.S. 347, 352-53 (1967); *Olmstead v. United States*, 277 U.S. 438, 464 (1928); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004) [hereinafter Kerr, *Fourth Amendment and New Technologies*].

¹⁸ 389 U.S. 347 (1967).

¹⁹ *Id.* at 351; Kerr, *Fourth Amendment and New Technologies*, *supra* note 17, at 815 (citing JEROLD H. ISRAEL & WAYNE R. LAFAVE, *CRIMINAL PROCEDURE IN A NUTSHELL* 60 (5th ed. 1993)).

²⁰ Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a “Crazy Quilt” of Fourth Amendment Protection*, UCLA J.L. & TECH., Spring 2007, at 1, 5.

²¹ *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

²² See Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528 (2006).

²³ *United States v. Jacobsen*, 466 U.S. 109, 117 (1984).

²⁴ *Id.*

²⁵ *United States v. Miller*, 425 U.S. 435, 443 (1976) (holding that there is no legitimate expectation of privacy in the contents of original checks and deposit slips despite the Bank Secrecy Act of 1970).

B. *Knowledge Requirement: Smith v. Maryland*

*Smith v. Maryland*²⁶ helped establish the knowledge requirement of third-party doctrine.²⁷ In *Smith*, the police suspected the defendant had committed a robbery.²⁸ The police asked the telephone company to install a pen register, a device that records the digits dialed over a telephone line, to record a log of all telephone calls the defendant made from his home.²⁹ The telephone company complied with this warrantless request.³⁰ The log file indicated that the defendant called the victim, who confirmed receiving an obscene phone call from the robber.³¹ Based on this phone call, as well as on other evidence, the police obtained a warrant to search the defendant's home, eventually leading to a trial at which the court convicted and sentenced the defendant to six years in prison.³²

The Supreme Court granted certiorari to determine the "restrictions imposed by the Fourth Amendment on the use of pen registers."³³ The Court held the defendant probably had no subjective expectation of privacy in the phone numbers he dialed from his home, and even if he did, that expectation was not one society would accept as reasonable.³⁴ Accordingly, the Court decided the police do not need a warrant to request that a telephone company install a pen register to log the numbers dialed by an individual.³⁵

The *Smith* court addressed the knowledge requirement by expressing doubt "that people in general entertain any actual expectation of privacy in the numbers they dial."³⁶ Moreover, the Court reasoned that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."³⁷ The Court concluded that the defendant should have known the digits he dialed were revealed to the telephone company and could potentially be logged.³⁸ Furthermore, it is sufficient that the "telephone company has the capacity to make a record of such relationships, even though the company has had the good sense not to offend its subscribers by making or keeping those records for no reason."³⁹

²⁶ 442 U.S. 735 (1979).

²⁷ *Id.* at 743-44; Solove, *supra* note 22, at 528.

²⁸ *Smith*, 442 U.S. at 737.

²⁹ *Id.*; *see also* 18 U.S.C. § 3127(3) (2000).

³⁰ *Smith*, 442 U.S. at 737.

³¹ *Id.*

³² *Id.* at 737-38.

³³ *Id.* at 738.

³⁴ *Id.* at 745-46.

³⁵ *Id.*

³⁶ *Id.* at 742.

³⁷ *Id.*

³⁸ *Id.* at 745.

³⁹ 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT

In other words, the courts look for technological capacity.⁴⁰ To determine whether an individual has knowingly transmitted information to a third party, the court does not look at the likelihood of the third party acquiring the information, but rather whether the third party has the technological capacity to acquire the information.

C. *The Content/Envelope Distinction*

In *Smith*, the Court was careful to draw a distinction between content information and envelope information.⁴¹ The Court did this by distinguishing a pen register from a listening device: while listening devices acquire the content of a communication, pen registers do not.⁴² *Smith* drew this distinction because in *Katz* the Court found a privacy interest in a telephone conversation.⁴³ Such a conversation could be characterized as the content of a communication. However, in *Smith*, the Court found no privacy interest in the digits dialed.⁴⁴ These digits could be considered envelope information because the digits are the information required by the telephone company to transmit the content. In other words, under such a distinction, an individual may have no privacy interest in the “information that the third party sees (i.e., envelope information),” while still maintaining a privacy interest in the “information that is hidden from the third party (i.e., letter information).”⁴⁵

Analogized to postal mail, a sender gives her envelope to a third party, the postal service.⁴⁶ By doing so, the sender has revealed the envelope information to the postal service – the “to” address, the “from” address, and the size, weight, and color of the envelope.⁴⁷ However, the sender retains a reasonable expectation of privacy in the content of her communication.⁴⁸ This

§ 2.7(b) (4th ed. 2007).

⁴⁰ See *Smith*, 442 U.S. at 745.

⁴¹ See Lawless, *supra* note 20, at 8-13 (discussing various aspects of the content/envelope distinction including the traditional-analogical view, criticisms of a literal understanding, and a messenger/recipient view); Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 611-12 (2003).

⁴² *Smith*, 442 U.S. at 741.

⁴³ *Katz v. United States*, 389 U.S. 347, 353 (1967).

⁴⁴ *Smith*, 442 U.S. at 745.

⁴⁵ Lawless, *supra* note 20, at 9; see also Brian D. Kaiser, Note, *Government Access to Transactional Information and the Lack of Subscriber Notice*, 8 B.U. J. SCI. & TECH. L. 648, 676 (2002); *Smith*, 442 U.S. at 745; *Katz*, 389 U.S. at 353. See generally Kerr, *supra* note 41, at 611-13 (describing the difference between content information and envelope information in a number of contexts).

⁴⁶ Kerr, *supra* note 41, at 611 (“The essential distinction between content and envelope information remains constant across different technologies, from postal mail to email.”).

⁴⁷ *Id.*

⁴⁸ *Id.*

content information corresponds to the letter contained within the envelope.⁴⁹ “This distinction enables courts to recognize that while a third party may have physical control over an individual’s information, such control does not make all expectations of privacy unreasonable.”⁵⁰

To summarize third-party doctrine, the starting point is that an individual has an expectation of privacy where (1) the individual possesses a subjective expectation of privacy; and (2) that expectation is “one that society is prepared to recognize as ‘reasonable.’”⁵¹ However, where an individual knowingly reveals information to a third party, the individual assumes the risk that the third party will reveal that information to the government.⁵² The issue then becomes which information was revealed to the third party. While the individual has no reasonable expectation of privacy in her envelope information, she may under certain circumstances still retain a reasonable expectation of privacy in her content information.

II. THE ECPA: THIRD-PARTY DOCTRINE APPLIED TO E-MAIL COMMUNICATIONS

A. *Overview of E-mail Technology: Three Hypothetical Recipients*

A firm understanding of the technology behind e-mail is necessary to properly apply Fourth Amendment protection to this realm. There are several methods of accessing e-mail, and as this Note explains, current Fourth Amendment protection turns on which method an individual uses.⁵³ This Section presents three hypothetical e-mail communications and explains the technologies underlying each of those communications.

The four characters in these three hypothetical communications are Alice, Bob, Charlie, and Tommy Trafficker. Suppose that Alice, Bob, and Tommy all use Microsoft Outlook – albeit each with slightly different settings – to access their university e-mail accounts, while Charlie uses Google’s Gmail service.⁵⁴

⁴⁹ *Id.*

⁵⁰ Lawless, *supra* note 20, at 8-9.

⁵¹ *Katz v. United States*, 389 U.S. 347, 361 (1967).

⁵² *United States v. Jacobsen*, 466 U.S. 109, 117 (1984); *see Solove, supra* note 22, at 528.

⁵³ *See infra* Part II.B.3 (applying the ECPA to the three hypothetical e-mail recipients of Part II.A).

⁵⁴ For the purposes of this discussion, equivalents to Microsoft Outlook are Mozilla Thunderbird and Apple’s Mail application. *See* Apple – Mac OS X Leopard – Features – Mail, <http://www.apple.com/macosex/features/mail.html> (last visited Mar. 30, 2008); Microsoft Office Online, Outlook Home Page, <http://office.microsoft.com/en-us/outlook/default.aspx> (last visited Mar. 30, 2008); Thunderbird, <http://www.mozilla.com/en-US/thunderbird> (last visited Mar. 30, 2008). Examples of equivalents to Gmail are Yahoo! Mail and Windows Live Hotmail. *See* Gmail: Email from Google, <http://www.gmail.com>

In each hypothetical, Tommy Trafficker wants to send an e-mail to one of the other three characters. The events are the same from Tommy's point of view for each e-mail. He opens Outlook and starts composing the new e-mail message.⁵⁵ In this window, Tommy enters the recipient's address (e.g., Alice's e-mail address), the subject of the e-mail, and then the body of the e-mail itself. Then Tommy clicks the "send" button, and Outlook immediately converts the message into Internet e-mail format.⁵⁶

After Outlook properly formats Tommy's e-mail message, the message must then start its journey to the recipient's computer.⁵⁷ The first step in the journey

(last visited Mar. 30, 2008); Windows Live Hotmail, <http://login.live.com> (last visited Mar. 28, 2008); Yahoo! Mail: The Best Web-Based Email!, <http://mail.yahoo.com> (last visited Mar. 30, 2008).

⁵⁵ Outlook is acting as his *mail user agent* ("MUA"), which is an application that allows a user to send and receive mail. Wayne Pollock, Email Tutorial, <http://www.hccfl.edu/pollock/Unix/EmailNotes.htm> (last visited Mar. 8, 2008) (describing a mail user agent or "email client" as "software that allows [the user] to compose, send, and read . . . email"). See *supra* note 54 for examples of other MUAs.

⁵⁶ This format consists of a plain text document containing two sections, a header and a message body. LARRY L. PETERSON & BRUCE S. DAVIE, *COMPUTER NETWORKS: A SYSTEMS APPROACH* 643 (4th ed. 2007). See RFC822: Standard for the Format of Arpa Internet Text Messages, <http://www.w3.org/Protocols/rfc822/> (last visited March 8, 2008) for the exact specifications of e-mail messages. The header is a series of single lines that contain pairs of types and values. PETERSON & DAVIE, *supra* at 643-44. For example, "To: oza@bu.edu" is a pair tying the "To:" type to the value of "oza@bu.edu." The message body follows the header separated by a blank line. *Id.* at 644. An example of a formatted e-mail message is:

```
Date: Mon, 08 Sep 2008 02:54:00 -0400
From: Tommy T. <tommy@bu.edu>
To: Alice R. <alice@berkeley.edu>
Subject: "Hot" FedEx Shipment
```

Dear Alice,

I shipped the Springsteen tickets overnight with FedEx.
You should receive them tomorrow.

Enjoy the show,
Tommy

⁵⁷ Recall that an e-mail message is actually a plain text document. See *supra* note 56 and accompanying text. As an e-mail transfers from server to server – ultimately reaching its final destination – it transfers as a plain text document. PETERSON & DAVIE, *supra* note 56, at 643. Because e-mails are moved around as plain text documents, it is possible that "children, snoops, and others within the general public could easily seize another's email with no more effort than taking someone's garbage bag and rummaging through the contents." E. Parker Lowe, *Mailer Beware: The Fourth Amendment and Electronic Mail*,

is to transfer the e-mail from Outlook to Tommy's e-mail server belonging to his university.⁵⁸ The Internet is not a single computer server, but rather, a collection of many servers.⁵⁹ The e-mail server will determine which servers the e-mail has to hop through to eventually reach its final destination.⁶⁰ The technology that transfers an e-mail from a user's computer to an e-mail server is the Simple Mail Transfer Protocol ("SMTP").⁶¹ Using SMTP, Outlook transfers Tommy's e-mail from his computer to his university's e-mail server.⁶² Here, Tommy's university is acting as his Internet Service Provider ("ISP"), or more specifically, his e-mail service provider.

1. Post Office Protocol

In the first hypothetical, Tommy's e-mail server determines the proper routing for his e-mail and then sends it off to Alice. The mail eventually arrives and is accepted by Alice's e-mail server belonging to her university.⁶³ The e-mail temporarily resides on Alice's e-mail service provider's server until Alice opens Outlook on her computer and clicks "get mail." Outlook then picks up the message using the Post Office Protocol ("POP"), and transfers it to Alice's computer.⁶⁴ At this point, the e-mail service provider's server will

2 OKLA. J.L. & TECH. 28, at *14 (2005). An e-mail user could mitigate that possibility by using encryption, but there still remains an off chance that a hacker could bypass the encryption. *Id.* at *15; see WILLIAM STALLINGS, CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE 355-90 (2d ed. 1999) (explaining the workings of two schemes for authentication and confidentiality services - pretty good privacy (PGP) and S/MIME).

Accordingly, it is possible to analogize an e-mail to a postcard, for which there is no Fourth Amendment protection. See Kerr, *supra* note 41, at 628-29. Therefore, it could be possible for a court to conclude an e-mail user does not have a reasonable expectation of privacy because an e-mail is more like a postcard than a sealed letter. *Id.* at 629. However, because "Internet surveillance law" is "predominantly statutory law," courts are unlikely to make this determination. See *id.* (citing *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002)); see also *Warshak v. United States*, 490 F.3d 455, 474 (6th Cir. 2007) ("[P]ortions of the [ECPA] itself strongly support an e-mail user's reasonable expectation of privacy in the content of his e-mails."), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

⁵⁸ Pollock, *supra* note 55. The e-mail server is also known as a Mail Transport Agent ("MTA"). *Id.* More specifically, the MTA is an application running on a server that can accept e-mails and route them to their destination. *Id.*

⁵⁹ PETERSON & DAVIE, *supra* note 56, at 297.

⁶⁰ Pollock, *supra* note 55. A user can see all the servers an e-mail passed through by looking at the "Received:" field in their e-mail header. *Id.*

⁶¹ PETERSON & DAVIE, *supra* note 56, at 646.

⁶² An example of an e-mail server address name is smtp.bu.edu.

⁶³ Pollock, *supra* note 55.

⁶⁴ RFC 1939 – Post Office Protocol – Version 3, <http://tools.ietf.org/html/rfc1939> (last visited March 8, 2008) [hereinafter Post Office Protocol] (specifying the standards for POP, which "allow[s] a workstation to retrieve mail that the server is holding for it").

delete its copy of the e-mail.⁶⁵

2. Internet Message Access Protocol

In the second hypothetical, Tommy sends an e-mail to Bob. The only difference between Alice and Bob is a Microsoft Outlook setting. Specifically, instead of using POP to retrieve e-mail from his e-mail server like Alice does, Bob has set Outlook to use the Internet Message Access Protocol (“IMAP”).⁶⁶ Recall that with POP, the e-mail server only *temporarily* holds e-mails in the user’s inbox.⁶⁷ The user downloads these e-mails to her computer and then the server deletes its copy.⁶⁸ In contrast, when using IMAP, the server is the primary storage location for the user’s e-mails.⁶⁹ Moreover, the user can maintain various e-mail folders on the server to facilitate organization.⁷⁰ In other words, an IMAP user does not download e-mails from her e-mail server to her personal computer. Rather, the user’s personal computer uses IMAP to display her e-mails residing on the e-mail service provider’s server.

Accordingly, all of Bob’s e-mails, including the one he received from Tommy, are stored on his university’s e-mail server because he switched Outlook from using POP to IMAP. From Bob’s point of view, Outlook operates the same whether it uses POP or IMAP. In either situation, Bob may view all of his e-mails within the software. However, the two are different under the hood. With POP, Bob’s e-mails would be removed from his e-mail service provider’s server, but with IMAP they remain on his university’s server.

3. Web-Based E-mail

In the third hypothetical, as in Alice’s and Bob’s situations, the e-mail eventually arrives on Charlie’s e-mail service provider’s server, but the server here belongs to Google, the provider of Gmail. If Charlie wants to access this e-mail, he does not load Outlook but instead goes to Gmail’s website in his

⁶⁵ This is not entirely true. The e-mail service provider’s server will often retain these “deleted” e-mails for at least one week. See Microsoft Office Online, Leave E-mail Messages on Your E-mail Server, <http://office.microsoft.com/en-us/outlook/HA011507931033.aspx> (expand “POP3 e-mail accounts” hyperlink) (last visited Mar. 29, 2008) (explaining that “the most common setting for people who want to read their messages at work but also download them for permanent storage on their home computer” is to have Outlook “downloaded to [the user’s] computer but remain on the e-mail server for the number of days that [the user] specif[ies]”).

⁶⁶ See generally RFC 3501 – Internet Message Access Protocol – Version 4rev1, <http://tools.ietf.org/html/rfc3501> (last visited Mar. 8, 2008) [hereinafter Internet Message Access Protocol] (specifying the standards for IMAP).

⁶⁷ Post Office Protocol, *supra* note 64.

⁶⁸ *Id.*

⁶⁹ Internet Message Access Protocol, *supra* note 66.

⁷⁰ *Id.*

web browser. After logging in, Charlie is able to view his e-mails – including the new one from Tommy – through the browser. Once Charlie is done, he closes the browser window. At no point does the e-mail transfer from Google’s server to Charlie’s home computer; the e-mail remains on Google’s server even after Charlie has finished reading it.

The differences between these three examples appear trivial from an e-mail user’s point of view. To an average user, Alice, Bob, and Charlie are all doing the same thing. Two are accessing their e-mail through Outlook – albeit each with different settings – and the third is accessing his e-mail through Gmail. Many e-mail users would perceive all three of these as essentially the same activity. However, the ECPA affords different levels of Fourth Amendment protection to these three recipients.

B. *The ECPA*

This Section will first explain the background of the ECPA, which is a Congressional attempt at applying third-party doctrine to electronic communications in storage with third parties. It will then provide a thorough analysis of the ECPA’s provisions allowing the government to compel disclosure of electronic communications in storage for longer than 180 days without a warrant. This Section will conclude by applying the ECPA to several scenarios that highlight the legal differences that arise for activities many would consider essentially identical.

In the absence of statutes, courts would have to determine the application of third-party doctrine to electronic communications through case law.⁷¹ However, courts would then have to make difficult judgments that would invariably lead to inconsistencies.⁷² Accordingly, Congress statutorily defined the circumstances under which an individual has a reasonable expectation of privacy with respect to electronic communications in the Electronics Communications Privacy Act of 1986.⁷³ Because Congress is in a better position than the courts to conduct fact-finding inquiries, courts, in deference to Congress, will typically avoid unnecessary determinations of constitutional questions where Congress has drafted an expansive statutory scheme regulating some aspect of constitutional rights.⁷⁴ The ECPA is one such

⁷¹ See *In re Askin*, 47 F.3d 100, 105-06 (4th Cir. 1995).

⁷² *Id.*

⁷³ 18 U.S.C. § 2510 (2000); *In re Askin*, 47 F.3d at 104.

⁷⁴ *Adams v. City of Battle Creek*, 250 F.3d 980, 986 (6th Cir. 2001); Ian Walden & Anne Flanagan, *Honeypots: A Sticky Legal Landscape?*, 29 RUTGERS COMPUTER & TECH. L.J. 317, 342 n.139 (2003) (“[S]ome courts have held that where a detailed federal statutory scheme is intended by Congress as the primary vehicle for enforcing constitutional rights, separate analysis is obviated, unnecessary and to be discouraged.” (citing *Adams*, 250 F.3d at 986)). *But see id.* (citing *Bohach v. City of Reno*, 932 F. Supp. 1232, 124-36 (D. Nev. 1996)) (explaining that some courts do conduct separate analyses).

statutory scheme,⁷⁵ and therefore, courts are often deferential to Congress in determining Fourth Amendment protection for electronic communications.⁷⁶ However, it is ultimately the Supreme Court's responsibility to determine constitutionality,⁷⁷ and within the context of the ECPA, one may argue that the Court should update its interpretations of this Act because of advances in technology since its adoption in 1986.

Congress enacted the ECPA to keep federal surveillance law and privacy safeguards in pace with developing technologies.⁷⁸ As the legislative history indicates, "Senator Leahy said . . . the existing law '[was] hopelessly out of date.'"⁷⁹ A 1985 study concluded that "current legal protections for electronic mail [were] 'weak, ambiguous, or non-existent,' and that 'electronic mail remain[ed] legally as well as technically vulnerable to unauthorized surveillance.'"⁸⁰ The House Committee members saw the urgency for updating legal protections for e-mail when an expert testified it was "reasonable to assume that during the 1990's electronic mail will become a regular and important part of the communications mix that a substantial number of Americans use."⁸¹ The ECPA aimed to clear the fog of uncertainty that shrouded Fourth Amendment protection for "developing area[s] of communication."⁸²

To provide some context, when the ECPA was enacted in 1986, Ronald Reagan was president, *Top Gun* was the top grossing film of the year,⁸³ the first web page was still four years away from being developed,⁸⁴ and the first

⁷⁵ See *Adams*, 250 F.3d at 986 ("The Electronic Communications Privacy Act is part of detailed legislative scheme under Title III of the Omnibus Crime and Control Act of 1986."); *Askin*, 47 F.3d at 105 ("The general presumption of constitutionality afforded to duly enacted legislation has heightened significance with regard to Title III.").

⁷⁶ *Adams*, 250 F.3d at 986 (deferring to the EPCA to determine the scope of a plaintiff's Fourth Amendment privacy right with respect to wiretapping).

⁷⁷ *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 177 (1803).

⁷⁸ 18 U.S.C. § 2510 (2000) (effective Oct. 21, 1986); Katherine A. Oyama, *E-Mail Privacy After United States v. Councilman: Legislative Options for Amending ECPA*, 21 BERKELEY TECH. L.J. 499, 499 (2006).

⁷⁹ S. REP. NO. 99-541, at 2 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3556.

⁸⁰ *Id.* at 4 (quoting U.S. CONG., OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 29 (1985)).

⁸¹ *ECPA Hearings*, *supra* note 7, at 20 (testimony of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association, accompanied by Michael F. Cavanagh, Executive Director, Electronic Mail Association).

⁸² S. REP. NO. 99-541, at 4.

⁸³ Top Grossing Movies for 1986 in the USA, <http://www.imdb.com/Sections/Years/1986/top-grossing> (last visited Aug. 11, 2008).

⁸⁴ Tim Berners-Lee, Frequently Asked Questions by the Press, <http://www.w3.org/People/Berners-Lee/FAQ.html#Examples> (last visited Mar. 8, 2008) (describing the first web page which debuted in 1990).

graphical web browser was over seven years away.⁸⁵ Moreover, an industry expert estimated that less than 0.5% of Americans had e-mail access.⁸⁶ It is within this context that Congress passed a statute dealing with privacy protection for emerging technologies. Therefore, it is not surprising that some portions of the Act are now dated. The following Section will explain one such portion.

1. The ECPA's 180-Day Distinction

Chapter 18 U.S.C. § 2703 describes when and how the government may compel “a provider of electronic communication service” to disclose “the contents of an electronic communication, that is in electronic storage.”⁸⁷ Subsection (a) sets forth a warrant requirement – requiring probable cause – to compel disclosure of communications that are in electronic storage of an electronic communication service for 180 days or less.⁸⁸ Subsection (b) describes means for compelling disclosure of communications that are in storage longer than 180 days.⁸⁹ The government may compel disclosure of e-mails in this latter category without notice to the subscriber if the government obtains a warrant.⁹⁰ Alternatively, under 18 U.S.C. § 2703(b)(1)(B), the government may compel disclosure of these e-mails *without a warrant* if the government gives the subscriber prior notice and obtains either an administrative subpoena or a court order.⁹¹ The standard for the court order is

⁸⁵ Mosaic Web Browser History, http://www.livinginternet.com/w/wi_mosaic.htm (last visited Apr. 21, 2008) (“Mosaic was the first popular Web browser [It was] released as version 0.5 on January 23, 1993 [It] provided support for graphics, sound, and video clips.”).

⁸⁶ This percentage is based on an estimate given at the ECPA Hearings of the number of electronic mailboxes in the United States in 1986 divided by the Census population data from 1990. See *ECPA Hearings*, *supra* note 7, at 475 (memorandum from ACLU Project Staff) (estimating “one million electronic ‘mailboxes’ in the United States” by the end of 1986); U.S. CENSUS BUREAU, SUMMARY, POPULATION, HOUSING UNITS, AREA MEASUREMENTS, AND DENSITY: 1790 TO 1990, at 2 tbl.2 (1990), available at <http://www.census.gov/population/censusdata/table-2.pdf> (stating that the United States population on April 1, 1990 was 248,709,873).

⁸⁷ 18 U.S.C. § 2703(a) (2000).

⁸⁸ *Id.* For the exact language of § 2703(a), see *supra* note 2.

⁸⁹ 18 U.S.C. § 2703(b) (2000).

⁹⁰ 18 U.S.C. § 2703(b)(1)(A) (2000). This section of the statute reads:

A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication [in electronic storage for more than one hundred and eighty days] . . . without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant

Id.

⁹¹ 18 U.S.C. § 2703(b)(1)(B) (2000). This section of the statute reads:

A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication [in electronic storage for more than one

“specific and articulable facts showing that there are reasonable grounds to believe,”⁹² which is a lower standard than probable cause.⁹³ However, the statute also includes a provision explaining that the government may delay notice to the subscriber for up to ninety days.⁹⁴ Delayed notice is an option where notification of “the court order may have an adverse result.”⁹⁵ Examples of an adverse result are: “endangering the life or physical safety of an individual,” “flight from prosecution,” “destruction of or tampering with evidence,” “intimidation of potential witnesses,” or “otherwise seriously jeopardizing an investigation or unduly delaying a trial.”⁹⁶

To summarize, the ECPA sets two levels of Fourth Amendment protection for e-mails stored on third-party servers. The government must afford e-mails stored on a server for 180 days or less full Fourth Amendment protection at a probable cause standard. However, the government may compel disclosure, without prior notice, of e-mails stored on a server for more than 180 days at a mere subpoena standard. In other words, under the ECPA, when an e-mail sitting on a third-party server ages from 180 days to 181 days, a user no longer has a reasonable expectation of privacy in its contents.

2. The Content/Envelope Distinction Applied to E-mail

It is important to understand what portion of e-mail communications § 2703(a) and (b) govern. Recall that Fourth Amendment protection extends to the content of a communication, not the envelope.⁹⁷ Within the context of e-mail communication, the message body is analogous to the content.⁹⁸ The other fields, which help the e-mail transfer from the sender’s computer to the recipient’s computer, are more like envelope information.⁹⁹ Examples of these attributes are the “to” address, the “from” address, the sender’s and receiver’s IP addresses, and the time and date stamp.¹⁰⁰ The Fourth Amendment does not

hundred and eighty days] . . . with prior notice from the governmental entity to the subscriber or customer if the governmental entity . . . uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or . . . obtains a court order for such disclosure under subsection (d) of this section

Id.

⁹² 18 U.S.C. § 2703(d) (2000).

⁹³ *Warshak v. United States*, 490 F.3d 455, 462 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

⁹⁴ 18 U.S.C. § 2703(b)(1)(B) (2000); 18 U.S.C. § 2705(a)(1)(A) (2000).

⁹⁵ 18 U.S.C. § 2705(a)(1)(A) (2000).

⁹⁶ 18 U.S.C. § 2705(a)(2) (2000).

⁹⁷ *See supra* Part I.C.

⁹⁸ *See* PETERSON & DAVIE, *supra* note 56, at 647-48 (describing the SMTP commands for extracting the header information that “form[s] an *envelope* for the message” and the commands for sending content information).

⁹⁹ *Id.*

¹⁰⁰ *Id.*; Kerr, *supra* note 41, at 615.

protect these envelope fields.¹⁰¹ Accordingly, § 2703(c) of the ECPA allows the government to compel the disclosure of envelope information without a warrant, regardless of the age of the e-mail; the 180-day distinction of § 2703(a) and (b) only apply to e-mail message bodies.¹⁰²

The content/envelope distinction within the e-mail context was the central issue of *United States v. Forrester*.¹⁰³ In *Forrester*, co-defendant Alba was convicted of operating an ecstasy-manufacturing laboratory.¹⁰⁴ Part of the evidence used against Alba was obtained by monitoring the “to” and “from” addresses of his e-mail correspondence without a warrant.¹⁰⁵ Alba appealed the conviction arguing that the monitoring violated his Fourth Amendment rights.¹⁰⁶ The Ninth Circuit upheld the conviction, likening the monitoring of “to” and “from” addresses to the warrantless monitoring of phone calls through a pen register.¹⁰⁷ The court explained:

[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.¹⁰⁸

Moreover, the court reasoned that “e-mail to/from addresses and IP

¹⁰¹ *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); Kerr, *supra* note 41, at 628 (“[A]n Internet user cannot enjoy a reasonable expectation of privacy in non-content information sent to an ISP because the user has disclosed the information to the ISP.” (citing *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001))); *see also* Kaiser, *supra* note 45, at 676 (“Non-content based communications are not thought to implicate the Fourth Amendment.”); Lawless, *supra* note 20, at 8-9 (“[The ‘content/envelope’] distinction enables courts to recognize that while a third party may have physical control over an individual’s information, such control does not make all expectations of privacy unreasonable. Rather, only information that the third party sees . . . is unprotected, while information that is hidden from the third party . . . is covered by the Constitution.”); *supra* text accompanying note 45 (explaining that content information is protected by the Fourth Amendment but envelope information is not).

¹⁰² 18 U.S.C. § 2703(a)-(b) (2000) (setting forth the 180-day distinction for compelling disclosure of the *content* of electronic communications); 18 U.S.C. § 2703(c)(1)(B) (2000) (“A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications . . .) to a governmental entity only when the governmental entity . . . obtains a court order for such disclosure under subsection (d) of this section . . .”); 18 U.S.C. § 2703(d) (2000) (describing the requirements for a court order).

¹⁰³ 512 F.3d 500, 510 (9th Cir. 2008).

¹⁰⁴ *Id.* at 505-06.

¹⁰⁵ *Id.* at 505.

¹⁰⁶ *Id.* at 509.

¹⁰⁷ *Id.* at 511.

¹⁰⁸ *Id.* at 510.

addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers.”¹⁰⁹ Furthermore, as far back as the nineteenth century, “the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties.”¹¹⁰ Accordingly, because the government sought only the envelope and not the content, the government appropriately compelled disclosure without a warrant.

3. Application of the ECPA to Three Hypothetical Recipients

Applying the ECPA to the three hypothetical recipients discussed above leads to interesting results.¹¹¹ Recall that Alice and Bob both use Outlook to access their e-mails from their university’s e-mail server.¹¹² However, because they use different Outlook settings, Alice’s e-mails are transferred to her computer and deleted from the university server when she views them, whereas Bob’s remain on the university server and are not deleted. Charlie accesses his e-mail using Gmail. Therefore, his e-mails remain on Google’s server even after Charlie views them.¹¹³

For this exercise, suppose that the government suspects Alice, Bob, and Charlie of drug trafficking and wants to read their e-mails; however, the government lacks probable cause. Imagine exactly 180 days have passed since Alice, Bob, and Charlie, and received their e-mails from Tommy. At this point, Alice’s e-mail is no longer located on the third-party server because it was deleted after being transferred to her home computer.¹¹⁴ Chapter 18 U.S.C. § 2703(a) applies only to “disclosure by a *provider of electronic communication service*,” so it cannot reach Alice’s e-mail.¹¹⁵ Accordingly,

¹⁰⁹ *Id.* The court explained the similarity between e-mail to/from addresses and phone numbers, stating: “[w]hen the government obtains the to/from addresses of a person’s e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed.” *Id.* Instead, the government “make[s] educated guesses” as to the content of the message or webpage based on its knowledge of the e-mail and IP addresses involved. *Id.* This is similar to making an educated guess as to the contents of a phone call based on the “identity of the person . . . dialed.” *Id.* “Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms.” *Id.*

¹¹⁰ *Id.* at 511.

¹¹¹ See *supra* Part II.A (discussing hypothetical scenarios of an e-mail user named Tommy Trafficker sending e-mails to recipients named Alice, Bob, and Charlie).

¹¹² See *supra* Part II.A.

¹¹³ See *supra* Part II.A.

¹¹⁴ See *supra* Part II.A.1.

¹¹⁵ See 18 U.S.C. § 2703(a) (2000) (emphasis added).

Alice's e-mail receives full Fourth Amendment protection at a probable cause standard.¹¹⁶ Bob used a different Outlook setting than Alice, so his e-mail remained on his third-party server, which belongs to his university.¹¹⁷ Likewise, Charlie's e-mail remained on his third-party server belonging to Google.¹¹⁸ Under § 2703(a), e-mails stored on third-party servers for 180 days or less require a warrant to compel disclosure.¹¹⁹ Accordingly, Tommy's e-mails to Alice, Bob, and Charlie are all protected by full Fourth Amendment protection at the 180-day mark and can only be compelled for disclosure by a warrant. Therefore, because the government lacks probable cause, all three of these e-mail communications remain private.

Imagine one more day passes. Now 181 days have elapsed since Tommy sent his e-mail to Alice, Bob, and Charlie. The government still lacks probable cause. As before, Alice's e-mail is on her home computer rather than a third-party server, so it is outside the reach of § 2703(a) and can only be seized through a warrant.¹²⁰ Bob and Charlie each have their e-mails from Tommy sitting on a third-party server, a university server and Google, respectively.¹²¹ These e-mails fall under § 2703(b) because they have been residing on the third-party server for longer than 180 days.¹²² Of most relevance is that under §§ 2703(b)(1)(B) and 2705(a)(1)(A), the government may compel the university and Google to disclose Tommy's e-mails – without prior notice to either Bob or Charlie – at a mere subpoena standard if the court determines that prior notice would lead to an “adverse result.”¹²³

In other words, 181 days after receiving an e-mail, a recipient using an e-mail client set to POP will have full Fourth Amendment protection while a

¹¹⁶ When e-mails are located on an individual's home computer and not with an electronic service provider, the government must show probable cause to obtain a warrant allowing for the seizure of the computer. *See, e.g.*, *United States v. Himmelreich*, No. 06-5186, 2008 WL 410117, at *2 (3d Cir. Feb. 15, 2008) (detailing a search warrant that “allowed law enforcement to search and seize any computers” or “e-mails” at the defendant's residence); *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006) (holding that the government had “acted properly in searching [the defendant's] computer and seizing . . . emails” pursuant to a warrant to search the defendant's home); *Russell v. Harms*, 397 F.3d 458, 461 (7th Cir. 2005) (discussing a warrant that authorized the government to “search [the suspect's] home and seize . . . [e]mail records relating to E-bay auctions”).

¹¹⁷ *See supra* Part II.A.2 (explaining that IMAP uses the third-party server as the storage location for e-mails).

¹¹⁸ *See supra* Part II.A.3 (explaining that Charlie views his e-mail on the web and that his e-mails remain on Google's server even after he views them).

¹¹⁹ 18 U.S.C. § 2703(a) (2000).

¹²⁰ *See id.*; *supra* note 116 and accompanying text (discussing cases in which the government obtained a warrant before searching e-mails).

¹²¹ *See supra* Part II.A.2-3.

¹²² 18 U.S.C. § 2703(b) (2000).

¹²³ 18 U.S.C. §§ 2703(b)(1)(B), 2705(a)(1)(A) (2000).

recipient using either an e-mail client set to IMAP or a web-based client will not.¹²⁴ A summary of the different results from applying § 2703 at 180 days and at 181 days is described below in Table 1.

¹²⁴ A possible basis for why the drafters of the ECPA included the 180-day distinction may be discerned through the committee hearing transcript. The transcript makes clear that the drafters did not envision an Internet where users would have broadband access and would want to store data permanently on third-party servers. An expert describing to the committee how e-mail worked explained: “the way these electronic mail systems are operated[,] the user first of all will access the computer over some form of a dedicated channel, [like a] dial-up telephone line.” *ECPA Hearings, supra* note 7, at 24 (testimony of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association). Moreover, the Deputy Assistant Attorney General, James Knapp, described an e-mail on a third-party server as “[d]ata [t]emporarily [s]tored in a [d]ata [b]ank” that is similar to a “first class piece of mail” waiting in a mailbox for the recipient to pick up. *Id.* at 234 (memorandum from James Knapp, Deputy Assistant Attorney General). This underscores how the drafters of the ECPA did not foresee that e-mail users would permanently store e-mails on a third-party server, but instead likened the server to temporary storage. *See, e.g.,* *Steve Jackson Games, Inc. v. U.S. Secret Service*, 816 F. Supp. 432, 434-39 (W.D. Tex. 1993) (describing a 1990 electronic bulletin board system (“BBS”) where users dial into the BBS and download e-mails to their home computer).

In fact, when Congressman Robert Kastenmeier, Jr. asked Knapp whether he would “make a distinction [of] before and after delivery, in terms of third-party repository of ‘E’ mail,” Knapp responded that he would, because “[b]efore delivery it is still in the process of transmission, it is still a message, it is still a communication, and the search warrant requirement should apply.” *ECPA Hearings, supra* note 7, at 251 (testimony of James Knapp, Deputy Assistant Attorney General). A memorandum from the ACLU bolstered Knapp’s testimony. *See id.* at 469, 474-79 (memorandum from ACLU Project Staff). In answering what e-mail is, the ACLU explained that after the “message arrives at the electronic mail company,” it is “stored in the addressee’s mailbox until the addressee . . . calls up this databank and retrieves his or her mail.” *Id.* at 474.

Further, in explaining what would be anachronistic today, the ACLU memorandum stated that “[i]f the addressee does not subscribe to the service, the electronic mail company converts the correspondence into hardcopy and deposits the communication in the first class or priority mail stream to the addressee’s house or office.” *Id.* Based on these testimonies before the committee hearings, it is reasonable to infer that the drafters of the ECPA believed that an e-mail service provider only stored e-mails temporarily on their servers, and therefore, if an e-mail user were to leave an e-mail communication on such a server for over six months, the user had abandoned it to the service provider.

<i>E-mail Technology</i>	<i>Server Retention</i>	<i>Warrant Requirement on Day 180?</i>	<i>Warrant Requirement on Day 181?</i>
POP	No	Yes	Yes
IMAP	Yes	Yes	No
Web client	Yes	Yes	No

Table 1. *Summary of protection required by the ECPA for different types of e-mail technologies.*

4. The ECPA Case Study

One example of the government successfully applying §§ 2703 and 2705 of the ECPA is *United States v. Ferguson*.¹²⁵ The Drug Enforcement Administration (“DEA”) was investigating Ferguson for drug trafficking.¹²⁶ During the investigation, the DEA discovered that Ferguson maintained accounts with both Yahoo! Mail and MSN Hotmail.¹²⁷ The government submitted a request to a magistrate to compel both services to produce all e-mails in storage for over 180 days.¹²⁸ The magistrate granted the request,¹²⁹ and Yahoo! subsequently handed over 137 e-mails.¹³⁰

Any e-mail that Ferguson had on his Yahoo! account that was over 180-days old was turned over to the government without a warrant because of the ECPA.¹³¹ However, had Ferguson instead used an application like Microsoft Outlook set to POP, the e-mails would have been residing on his own computer instead of Yahoo!’s server. They would therefore be unreachable by the ECPA, and accordingly, would not have been turned over to the government without a warrant.¹³²

III. SIXTH CIRCUIT PANEL HELD 180-DAY DISTINCTION UNCONSTITUTIONAL

In a now vacated ruling, a Sixth Circuit panel held in *Warshak v. United States*¹³³ that “individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP.”¹³⁴

¹²⁵ 508 F. Supp. 2d 7 (D.D.C. 2007).

¹²⁶ *Id.* at 8.

¹²⁷ *Id.* Microsoft has since rebranded “MSN Hotmail” as “Windows Live Hotmail.” Davis D. Janowski, *Windows Live Hotmail (beta)*, PC MAGAZINE, Mar. 26, 2007, <http://www.pcmag.com/article2/0,2817,2107839,00.asp>.

¹²⁸ *Ferguson*, 508 F. Supp. 2d at 8.

¹²⁹ *Id.*

¹³⁰ *Id.* MSN Hotmail did not comply with the request. *Id.*

¹³¹ *Id.*

¹³² *See supra* note 116.

¹³³ 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

¹³⁴ *Id.* at 471; *see* Rebecca Porter, *Account Holder Has Right to E-Mail Privacy*, *Sixth*

Specifically, the panel court upheld a preliminary injunction enjoining the government from “seizing the contents of a personal e-mail account” under 18 U.S.C. § 2703(d) unless the government provides prior notice to the e-mail user or shows that the e-mail user had no reasonable expectation of privacy vis-à-vis the e-mail service provider.¹³⁵ In effect, the court held by its injunction that portions of the ECPA were unconstitutional.¹³⁶ This Part will examine the factual background of *Warshak*, the district court holding, the Sixth Circuit panel holding, and the en banc opinion vacating the panel judgment.

A. *Warshak v. United States: Factual Background and District Court Ruling*

The government suspected Steven Warshak and his company, Berkeley Premium Nutraceuticals, of mail and wire fraud and money laundering.¹³⁷ The government obtained a court order issued under 18 U.S.C. § 2703 from a magistrate compelling Warshak’s ISP, NuVox, and Warshak’s e-mail service provider, Yahoo!, to disclose any of Warshak’s e-mails residing on their servers for longer than 180 days.¹³⁸ Furthermore, the order was sealed, so neither NuVox nor Yahoo! was allowed to notify Warshak of the disclosure until the government authorized them to do so.¹³⁹ The government notified Warshak of the orders one year after the magistrate granted them.¹⁴⁰ Warshak immediately filed suit against the government and sought “declaratory and injunctive relief, and alleg[ed] that the *compelled disclosure of his e-mails without a warrant* violat[ed] the Fourth Amendment.”¹⁴¹ Warshak also requested assurance from the government that it would not seek additional orders compelling disclosure of e-mails under § 2703(d).¹⁴² The government declined to make any such assurances, and Warshak subsequently “moved for a temporary restraining order and/or a preliminary injunction prohibiting such

Circuit Rules, 43 TRIAL 71, 71 (2007) (“The Sixth Circuit has become the first federal appeals court to rule that e-mail users have a reasonable expectation of privacy regarding messages they send and store with commercial Internet service providers . . .”); Erin E. Wright, *The Right to Privacy in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of Warshak v. United States*, 3 I/S: J.L. & POL’Y FOR INFO. SOC’Y 531, 544 (2008) (“In June 2007, the United States Court of Appeals for the Sixth Circuit single-handedly rewrote the law of Internet privacy by relaxing the third party doctrine when it handed down *Warshak v. United States*.” (footnotes omitted)).

¹³⁵ *Warshak*, 490 F.3d at 482.

¹³⁶ *See id.*

¹³⁷ *Id.* at 460.

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.* at 460-61 & n.1 (“The government has conceded that it violated the statute by waiting for over a year without providing notice of the e-mail seizures to Warshak or seeking extensions of the delayed notification period . . .”).

¹⁴¹ *Id.* at 461 (emphasis added).

¹⁴² *Id.*

future searches.”¹⁴³

The district court was unwilling to agree with Warshak’s argument that § 2703 violated the Fourth Amendment solely because it allowed the seizure of e-mails “without a warrant and on a showing less than probable cause.”¹⁴⁴ However, the court found it distasteful that the government did not give Warshak “the opportunity to present his case.”¹⁴⁵ Therefore, the court found the statute unconstitutional because it required only the “government’s *ex parte* representations” to compel disclosure on a standard of less than probable cause.¹⁴⁶ Accordingly, the district court “deemed the constitutional flaws of the statute ‘facial in nature,’ and agreed to preliminarily enjoin additional seizures of e-mails from an ISP account of any resident of the Southern District of Ohio without notice to the account holder and an opportunity for a hearing.”¹⁴⁷ The government appealed this decision to the Sixth Circuit.¹⁴⁸

B. *The Sixth Circuit Panel Ruling*

On appeal, a Sixth Circuit panel held that the injunctive relief granted by the district court was “largely appropriate,” but required modification.¹⁴⁹ At the outset, the government argued that the court order issued under § 2703 was not a search but rather a compelled disclosure.¹⁵⁰ Therefore, the government argued, the appropriate standard was a “showing of reasonable relevance,” and not “the more stringent showing of probable cause” that is required by the Fourth Amendment.¹⁵¹ This “begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-à-vis the party who is subject to compelled disclosure – in this instance, [the e-mail service provider or ISP].”¹⁵² If an e-mail user does not maintain a reasonable expectation of privacy, then “the government must meet only the reasonableness standard applicable to compelled disclosures to obtain the material.”¹⁵³ However, if an e-mail user does maintain a reasonable expectation of privacy, “then the Fourth Amendment’s probable cause standard controls the e-mail seizure.”¹⁵⁴

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Warshak v. United States*, No. 1:06-cv-357, 2006 WL 5230332, at *8 (S.D. Ohio July 21, 2006), *aff’d as modified*, 490 F.3d 455 (6th Cir. 2007), and *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

¹⁴⁶ *Id.*; *Warshak*, 490 F.3d at 461.

¹⁴⁷ *Warshak*, 490 F.3d at 461.

¹⁴⁸ *Id.* at 462.

¹⁴⁹ *Id.* at 482.

¹⁵⁰ *Id.* at 468.

¹⁵¹ *Id.*

¹⁵² *Id.*

¹⁵³ *Id.*

¹⁵⁴ *Id.*

In determining whether the e-mail user, Warshak, maintained a reasonable expectation of privacy in the content of e-mails stored on his ISP, the court focused on two narrow inquiries rather than on the general fact that the user shared a communication.¹⁵⁵ The court first assessed with whom the “communication was shared” and then determined which information was “conveyed to the party” from whom disclosure was sought.¹⁵⁶

For the first inquiry courts must “specifically identify the party with whom the communication [was] shared, as well as the parties from whom disclosure [was] shielded.”¹⁵⁷ In determining this, the panel court looked toward *Katz* and *United States v. Miller*.¹⁵⁸ The guidance from *Katz* provides that the user’s expectation of privacy does not entirely dissipate solely because the communication was shared with another person; otherwise the government would have free range to eavesdrop.¹⁵⁹ Moreover, *Miller* provides that by sharing the communication with the third party, the user assumes the risk that the third party may reveal the communication to the government or disclose it through a subpoena.¹⁶⁰

The second inquiry “pertains to the precise information actually conveyed to the party through whom disclosure is sought or obtained.”¹⁶¹ Two guideposts here are *Katz* and *Smith*.¹⁶² In *Katz*, the conversation the defendant made over the phone – content information – was held private,¹⁶³ whereas in *Smith*, the phone numbers of the calls the defendant made – envelope information – were not held as private.¹⁶⁴ This harkens back to the envelope/content distinction, in which the content of a communication has Fourth Amendment protection while the envelope information does not.¹⁶⁵ As the *Warshak* court put it, “[l]ike telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.”¹⁶⁶ In *Warshak*, the government did not prove that the ISP regularly accessed the

¹⁵⁵ *Id.* at 470.

¹⁵⁶ *Id.* at 470-71.

¹⁵⁷ *Id.* at 470.

¹⁵⁸ *Id.* (citing *Katz v. United States*, 389 U.S. 347 (1967), and *United States v. Miller*, 425 U.S. 435 (1976)); see *supra* Part I.A for additional discussion of *Katz* and *Miller*.

¹⁵⁹ *Warshak*, 490 F.3d at 470; see *supra* note 21 and accompanying text (discussing the requirements needed for Fourth Amendment Protection: (1) a subjective expectation of privacy; and (2) an expectation society considers reasonable).

¹⁶⁰ *Warshak*, 490 F.3d at 470; see *supra* note 25 and accompanying text.

¹⁶¹ *Warshak*, 490 F.3d at 470.

¹⁶² *Id.*

¹⁶³ *Katz*, 389 U.S. at 352.

¹⁶⁴ *Smith v. Maryland*, 422 U.S. 735, 745-46 (1979); *Warshak*, 490 F.3d at 470.

¹⁶⁵ See *supra* Part I.C.

¹⁶⁶ *Warshak*, 490 F.3d at 471.

contents of its users' e-mails.¹⁶⁷ Accordingly, its users "privacy expectation in the content [of their e-mails was] not diminished."¹⁶⁸ Moreover, the court rejected the government's argument that a user's expectation of privacy would be unreasonable where the ISP scans e-mails for viruses, spam, and child pornography.¹⁶⁹ The court rejected this argument because the ISP used software search algorithms to search for this content instead of human review, and therefore, the user would not believe the contents of his e-mails were disclosed to anyone but the recipient.¹⁷⁰ Accordingly, the court disagreed with the government's compelled disclosure argument because the defendant maintained a reasonable expectation of privacy with respect to his e-mails stored on the third-party servers.¹⁷¹

Therefore, the panel upheld the district court injunction, but modified it to eliminate protection where the user does not maintain an expectation of privacy vis-à-vis the ISP:

[T]he preliminary injunction should be modified to prohibit the United States from seizing the contents of a personal e-mail account maintained by an ISP in the name of any resident of the Southern District of Ohio, pursuant to a court order issued under 18 U.S.C. § 2703(d), without either (1) providing the relevant account holder or subscriber prior notice and an opportunity to be heard, or (2) making a fact-specific showing that the account holder maintained no expectation of privacy with respect to the ISP, in which case only the ISP need be provided prior notice and an opportunity to be heard.¹⁷²

C. *Sixth Circuit Exception for ISP Waiver of Privacy Expectation Through Auditing*

Warshak suggested that "e-mail users maintain a reasonable expectation of privacy in the content of their e-mails" *except* where "a fact-specific showing [is made] that the account holder maintained no expectation of privacy with respect to the ISP."¹⁷³ In fleshing out the rule, the *Warshak* court stated that "[w]here a user agreement calls for regular auditing, inspection, or monitoring of e-mails, the expectation [of privacy] may well be [unreasonable], as the potential for an administrator to read the content of e-mails in the account should be apparent to the user."¹⁷⁴ The court pointed to a case from the Fourth

¹⁶⁷ *Id.* at 474.

¹⁶⁸ *Id.* at 471.

¹⁶⁹ *Id.* at 474.

¹⁷⁰ *Id.*

¹⁷¹ *Id.* at 475.

¹⁷² *Id.* at 482.

¹⁷³ *Id.*

¹⁷⁴ *Id.* at 473.

Circuit, *United States v. Simons*,¹⁷⁵ for an example of an agreement that would meet their “regular auditing” criteria.¹⁷⁶ The agreement in *Simons* stated that the defendant’s employer “would conduct electronic audits to ensure compliance” with their requirements.¹⁷⁷ Moreover, the agreement stated that the audits would include archiving copies of all “[s]ent and received e-mail messages.”¹⁷⁸ The employer hired an agency to manage and monitor their computer network.¹⁷⁹ An employee of the hired firm did a search on the keyword “sex” – without a warrant – which led him and an FBI agent to discover that one of the employees had a collection of child pornography on his computer.¹⁸⁰ The court held that the warrantless search did not violate the defendant’s Fourth Amendment rights because the agreement included an “auditing” provision where the employer actively managed and monitored network traffic.¹⁸¹

D. *En Banc Rehearing and Implications of Warshak*

In an en banc decision, the Sixth Circuit recently vacated the panel’s preliminary injunction and “remand[ed] the case to the district court to dismiss Warshak’s constitutional claim.”¹⁸² In the meantime, Warshak was “convicted on federal fraud charges” and “forfeit[ed] \$33 million in assets.”¹⁸³ Moreover, the en banc court stressed the need for “a concrete factual context”¹⁸⁴ that was absent to test “[t]he underlying merits [at] issue in the case.”¹⁸⁵ The facts were held insufficient because “the expectation of privacy that computer users have in their e-mails . . . shifts from internet-service agreement to internet-service agreement and . . . requires considerable [concrete] knowledge” that was not available in *Warshak*’s record based on hypothetical future seizures.¹⁸⁶

¹⁷⁵ 206 F.3d 392 (4th Cir. 2000).

¹⁷⁶ *Id.* at 398.

¹⁷⁷ *Id.* at 395-96.

¹⁷⁸ *Id.*

¹⁷⁹ *Id.* at 396.

¹⁸⁰ *Id.* at 396.

¹⁸¹ *Id.* at 398.

¹⁸² *Warshak v. United States*, 532 F.3d 521, 534 (6th Cir. 2008) (en banc).

¹⁸³ *Steven Warshak, Other Berkeley Nutraceuticals Officials to Forfeit \$33M*, BUS. COURIER OF CINCINNATI, Feb. 27, 2008, <http://www.bizjournals.com/cincinnati/stories/2008/02/25/daily29.html>; *see also Warshak*, 532 F.3d at 525.

¹⁸⁴ *Warshak*, 532 F.3d at 526-27 (quoting *Ammex, Inc. v. Cox*, 351 F.3d 697, 706 (6th Cir. 2003)).

¹⁸⁵ *Id.* at 526.

¹⁸⁶ *Id.* at 526-27. *But see id.* at 536-37 (Martin, J., dissenting) (“The original panel opinion sufficiently addressed th[e] issue, analyzing the relevant facts, and pertinent Supreme Court opinions, as well as the most recent precedents of our sister circuits. . . . Rather than address the facts and law cited by the panel’s opinion, the majority fails to cite one case dealing with electronic communications in the privacy context, instead relying on a

Accordingly, the en banc court did not reach the issue of whether “§ 2703(d) [is] consistent with the Fourth Amendment, which generally requires ‘probable cause’ and a warrant in the context of searches of individuals, homes and . . . posted mail.”¹⁸⁷ This Note advocates that the principle underlying the vacated *Warshak* holding is correct and that § 2703(d) is unconstitutional.¹⁸⁸ Because courts are “especially reluctant to invalidate statutes on their face under the Fourth Amendment,”¹⁸⁹ the best remedy is for Congress to amend the ECPA.

IV. PROPOSAL TO AMEND THE ECPA

A. *Proposed Amendment*

As this Note has explained, portions of § 2703 of the ECPA are unconstitutional. An e-mail user has a reasonable expectation of privacy in the e-mails she has stored on her e-mail service provider’s server, assuming the service provider does not monitor or audit her e-mails. While § 2703 applies full Fourth Amendment protection at a probable cause standard to e-mails in storage on a third-party server for 180 days or less, it denies them this protection once they age over 180 days. Therefore, if this issue were to reach the Supreme Court, it ought to strike down the less-than-probable-cause

single professor’s law review article.”); *id.* at 537 (“The factual record necessary to support a preliminary injunction does not have to be complete.”).

¹⁸⁷ *Id.* at 526 (majority opinion).

¹⁸⁸ As evidence of the desire to bring privacy rights in line with modern technologies, some courts have quickly adopted aspects of the Sixth Circuit panel’s reasoning in *Warshak*. For example, a district court case in Massachusetts applied the holding of *Warshak*, ruling that a cell phone user has a reasonable expectation of privacy in his location because even though the cell phone company (the third party) may have his location information, they would not normally use that to identify the location of a customer. *In re Applications of the United States of America for Orders Pursuant To Title 18, United States Code, Section 2703(d) To Disclose Subscriber Information and Historical Cell Site Information for Mobile Identification Numbers: (XXX) XXX-AAAA, (XXX) XXX-BBBB, AND (XXX) XXX-CCCC*, 509 F. Supp. 2d 64, 74 n.6 (D. Mass. 2007), *rev’d*, 509 F. Supp. 2d 76 (D. Mass. 2007).

Additionally, a case from the Eastern District of New York looked toward *Warshak* in holding that a telephone user has a reasonable expectation of privacy in the digits she dials after getting connected to a callee because *those* digits are not normally used by the telephone company. *In re United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices*, 515 F. Supp. 2d 325, 337-38 (E.D.N.Y. 2007) (“[*Warshak*] holds that only when an institution ‘actually relies on and utilizes . . . access [to information] in the normal course of business’ does the supplier of that information forfeit his reasonable expectation of privacy.”). These cases help show the eagerness of courts to adopt the reasoning of *Warshak*: that a user has a reasonable expectation of privacy in electronic communications stored on a third-party server.

¹⁸⁹ *Warshak*, 532 F.3d at 529.

standard for e-mails in electronic storage longer than 180 days, as described in § 2703.¹⁹⁰

However, as discussed in Part II.B, since Congress enacted the ECPA as “part of a detailed legislative scheme,” any privacy concerns with the ECPA are best addressed toward that body and not the federal courts.¹⁹¹ Accordingly, this Note proposes that Congress amend the ECPA to bring it up-to-date with modern e-mail technology.¹⁹²

Specifically, § 2703(a) provides a warrant requirement for e-mail communications stored on third-party servers for 180 days or less, but it provides other means for the authorities to obtain e-mails stored longer than 180 days under subsection (b) at a standard less than probable cause.¹⁹³ This Section details a proposed amendment that would overcome this constitutional deficiency.

First, this proposed amendment would remove the 180-day distinction of the first sentence of § 2703(a) and delete the second sentence of subsection (a). Subsection (a) currently reads in its entirety:

¹⁹⁰ See *Ayotte v. Planned Parenthood of N. New England*, 546 U.S. 320, 328-29 (2006) (“Generally speaking, when confronting a constitutional flaw in a statute, we try to limit the solution to the problem. We prefer, for example, to enjoin only the unconstitutional applications of a statute while leaving other applications in force or to sever its problematic portions while leaving the remainder intact.”(citations omitted)).

¹⁹¹ *Adams v. City of Battle Creek*, 250 F.3d 980, 986 (6th Cir. 2001). See Wright, *supra* note 134, at 551 (explaining that scholars such as “Professor Orin Kerr argue that the legislature, not the courts, should determine privacy rights in the face of rapidly changing technology.” (citing Kerr, *Fourth Amendment and New Technologies*, *supra* note 17)). But see *id.* at 549 (“[P]roponents such as Professor Peter Swire argue that the courts should determine the outer limits of government surveillance.” (citing Peter P. Swire, *Katz Is Dead. Long Live Katz.*, 102 MICH. L. REV. 904, 922 (2004))).

¹⁹² Congress has proposed legislation to amend § 2703 as recently as July 24, 2007; however, the proposed legislation does not address the 180-day distinction that is the topic of this Note. See H.R. 3156, 110th Cong. § 131 (2007). Other advocates of amending the ECPA suggest that Congress should broaden the definition of “transit” so that an e-mail is in “transit” until the recipient actually receives the e-mail, rather than the e-mail being in “transit” until it arrives on the third-party server, at which point it enters electronic storage. Robert S. Steere, *Keeping “Private E-mail” Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 274 (1998). This would apply Fourth Amendment protection to e-mails until they are received by the user. *Id.* However, this does not solve the problem of users that elect to permanently store their e-mails on third-party servers. *Id.* at 270 (describing how the two possible scenarios are either (1) the user elects to *store backup* copies of e-mails on the third-party server, which are not protected by the Fourth Amendment; or (2) the user elects to *download* the user’s e-mails to his personal computer and delete the e-mails from his third-party server). This oversight is most likely due to the rapid recent growth of web-based e-mail. For example, Microsoft only began offering free web based e-mail starting in 1998. *Microsoft Acquires Hotmail, An E-mail Service Provider*, N.Y. TIMES, Jan. 1, 1998, at D4.

¹⁹³ 18 U.S.C. § 2703(a) (2000).

CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE. – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.¹⁹⁴

By deleting the 180-day distinction within the first sentence of subsection (a) and by deleting the second sentence, § 2703(a) would then accord all e-mails in electronic storage – regardless of the length of time in storage – full Fourth Amendment protection by requiring a warrant under a probable cause standard.

However, as the Sixth Circuit panel discussed in *Warshak*, there may be circumstances under which an e-mail user does not maintain a reasonable expectation of privacy vis-à-vis her e-mail service provider.¹⁹⁵ Therefore, it would be too far reaching for the amended statute to grant a reasonable expectation of privacy to e-mails in storage with *any* e-mail service provider. Accordingly, the proposed amendment includes an exception to the warrant requirement of § 2703(a) when there is “a fact-specific showing that the account holder maintained no expectation of privacy with respect to the [provider of electronic communication service], in which case only the [service provider] need be provided prior notice and an opportunity to be heard.”¹⁹⁶

This Note’s proposed amendment would have § 2703(a) read in its entirety:

CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE. – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant, except where there is a fact-specific showing that the account holder maintained no expectation of privacy with respect to the provider of electronic communication service, in which case only the service provider need be provided prior notice and an opportunity to be heard.

The proposed amendment would bring § 2703 in line with modern e-mail technology. By eliminating the 180-day distinction, the amended ECPA would

¹⁹⁴ *Id.*

¹⁹⁵ *Warshak v. United States*, 490 F.3d 455, 482 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

¹⁹⁶ *See id.*

afford full Fourth Amendment protection to all e-mails in electronic storage where the user maintains an expectation of privacy vis-à-vis the service provider. This amendment would afford all e-mail users the same Fourth Amendment protection regardless of what technology they use to access their e-mail.

B. *Proposed Amendment Applied to Three Hypothetical Recipients*

Recall the three hypothetical e-mail recipients discussed earlier – Alice, Bob, and Charlie, who all received e-mails from Tommy Trafficker.¹⁹⁷ In each scenario, a third-party server received Tommy’s e-mail.¹⁹⁸ Based on their Outlook e-mail settings, Alice’s e-mail was transferred to her home computer while Bob’s e-mail remained on his university’s server and Charlie’s e-mail remained on Google’s server.¹⁹⁹ To most, the activities of these three e-mail users are essentially indistinguishable. Currently, however, the ECPA provides only the first category – e-mails downloaded from the server – full Fourth Amendment protection at a probable cause standard after 180 days have elapsed.²⁰⁰ This Note’s proposed amendment would remedy this absurd result.

Under the proposed amendment, there is no longer a 180-day distinction. Alice’s e-mail, which her home computer downloaded through Outlook, is outside the reach of the ECPA because her e-mail is stored in her home and the government may only seize her computer through a warrant.²⁰¹ Bob and Charlie’s e-mails remain on third-party servers even after 180 days have passed. Under the proposed amendment, because Bob and Charlie maintain an expectation of privacy with respect to their service providers – the university and Google – their e-mails in storage over 180 days are afforded full Fourth Amendment protection and the government can only force their disclosure through a warrant. This is the level of privacy that Alice, Bob, and Charlie would expect to have. Their Fourth Amendment protection no longer turns on their choice of e-mail clients. A summary of how the proposed amendment would affect different e-mail technologies is described below in Table 2.

¹⁹⁷ See *supra* Part II.A.

¹⁹⁸ See *supra* Part II.A.

¹⁹⁹ See *supra* Part II.A.1-3.

²⁰⁰ See *supra* Part II.B.3.

²⁰¹ See *supra* note 116 and accompanying text.

<i>E-mail Technology</i>	<i>Server Retention</i>	<i>Warrant Required After 180 Days?</i>	
		<i>Current ECPA</i>	<i>Amended ECPA</i>
POP	No	Yes	Yes
IMAP	Yes	No	Yes
Web client	Yes	No	Yes

Table 2. *Comparison of warrant requirements afforded through the current ECPA and that afforded through this Note's proposed amendment.*

CONCLUSION

The Supreme Court established through *Katz* that the “Fourth Amendment protects people, not places” in holding that an individual has a reasonable expectation of privacy in the content of her phone calls.²⁰² Through *Smith*, the Court refined this rule by holding that while an individual has a reasonable expectation of privacy in the content of her phone call, she does not have a reasonable expectation of privacy in the numbers she dials.²⁰³ These holdings define the content/envelope distinction of third-party doctrine.²⁰⁴

Congress passed the ECPA in 1986 to draw clear lines as to where Fourth Amendment protection extends with emerging technologies.²⁰⁵ In 1986, e-mail technology was still very new. Most e-mail users dialed-up to their e-mail servers using a modem and downloaded their communications to a home computer, with the server acting only as a medium for temporary storage.²⁰⁶ Using this rationale, the ECPA draws a distinction between e-mails in electronic storage on third-party servers for 180 days or less and those in electronic storage longer than 180 days.²⁰⁷ E-mails in storage for 180 days or less are afforded full Fourth Amendment protection at a probable cause standard while those in storage for longer than 180 days may be compelled for disclosure at a mere subpoena standard.²⁰⁸ This distinction reflects how twenty years ago, if a user did not download an e-mail communication to her home computer within 180 days, she had essentially abandoned it to the service provider and no longer had a reasonable expectation of privacy within its contents.²⁰⁹

²⁰² *Katz v. United States*, 389 U.S. 347, 351 (1967).

²⁰³ *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979).

²⁰⁴ *See supra* Part I.C.

²⁰⁵ *Oyama*, *supra* note 78, at 499.

²⁰⁶ *ECPA Hearings*, *supra* note 7, at 24 (testimony of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association).

²⁰⁷ 18 U.S.C. § 2703(a) (2000).

²⁰⁸ 18 U.S.C. §§ 2703(a), (b)(1)(B), 2705(a)(1)(A) (2000).

²⁰⁹ *See supra* note 124.

Today, technology has greatly changed how people access their e-mail. While some users employ applications like Microsoft Outlook, which download e-mails to their home computers, many other users use web-based e-mail clients, like Gmail, which store e-mail communications permanently on third-party servers. Under current laws, users of the latter are afforded less Fourth Amendment protection than users of the former for essentially doing the same activity after 180 days pass. This distinction is unconstitutional.

The Sixth Circuit was the first circuit court to properly address this issue, and its panel decision held that e-mail users have a reasonable expectation of privacy with their e-mails stored on third-party servers so long as the service provider does not maintain a policy that they would actively audit the users' communications. The Sixth Circuit vacated the panel opinion en banc for lack of ripeness and did not reach the underlying constitutional issues.

This Note recommends that Congress amend the ECPA to bring it in line with current e-mail communication technology.²¹⁰ Congress should update the ECPA by eliminating the 180-day distinction of § 2703(a). By doing so, Congress will statutorily extend Fourth Amendment protection to communications that e-mail users today reasonably expect to have protected.

²¹⁰ See *supra* Part IV.