Volume 43
Number 2 *Winter 2009*

*pp.*671-770

Winter 2009

Have You Seen My Inbox? Government Oversteps the Fourth Amendment Again: Goodbye Telephones, Hello E-Mail

Kimberly S. Cuccia

Notes

HAVE YOU SEEN MY INBOX? GOVERNMENT OVERSTEPS THE FOURTH AMENDMENT AGAIN: GOODBYE TELEPHONES, HELLO E-MAIL

I. INTRODUCTION

Its salient characteristics, particularly ease of use and informality, lead to the 'immortalizing' of information that normally would never be written down or distributed in an office memo.[1]

Happily married John Jones, a father of four and a self-employed contractor, conducts as many personal and business transactions as he can via the Internet to free up time for his family.[2] Along with managing his bank accounts, John pays the electric, water, credit card, health insurance, car payment, car insurance, and phone bills online via electronic mail ("e-mail"). John corresponds via e-mail with his doctor regarding his son's severe allergy condition and with his attorney regarding real estate investments, business practices, and general legal questions. John receives payment confirmations by e-mail for paid bills that he archives on his Internet server, Smalltown.net. Smalltown.net is a local company that serves a small town of approximately two thousand people.

Unbeknownst to John, a recent increase in fraudulent health insurance claims regarding steroids resulted in government investigation. Monthly, John makes claims on behalf of his son for a steroid medication used to treat his son's allergies. The government, having an interest in the Jones family health claims because of the steroidal prescription, obtained a warrant to seize John's e-mail based on knowledge that John receives his insurance statements electronically. The government faxed this warrant to Smalltown.net demanding all John Jones's e-mails for the past year that contained the keywords "health," "medication," or "steroids."

---

1 41 AM. JUR. 3D *Proof of Facts* § 1 (West 1997 & Supp. 2001).

2 The above hypothetical was inspired by Warshak v. United States (Warshak I), 490 F.3d 455 (6th Cir. 2007), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). This fact pattern was created by the author of this Note, and any similarities to real persons or facts are entirely coincidental.

Smalltown.net ran a term search and printed all of the hits. Two people handled the requested documents—a server technician and a nosy secretary, Betty Eyez, who bundled up the documents and packaged them for the government officials. Ninety percent of the e-mails in John Jones's account hit for one of the above terms, including credit card and bank statements, health insurance claims, and attorney correspondence. While waiting for the printing to finish, Betty Eyez glanced through some of John Jones's e-mails. Betty Eyez's two children attend the same middle school as the Jones children; later, Eyez's children spread rumors at school that John Jones is a drug addict who spends thousands of dollars on products from QVC, a large multimedia retailer, each year and has questionable business banking practices.

The breach of John Jones's privacy is an unconstitutional violation of the guarantees of trustworthiness provided by the Fourth Amendment to the United States Constitution.[3] In light of recent decisions by United States district courts, ancient electronic communications law, and the Stored Communications Act, the Smalltown.net scenario is certainly plausible. This Note discusses and analyzes the current law regarding governmental seizure of private e-mails that permits encroachment on constitutional guarantees of privacy.

The purpose of this Note is to demonstrate that current procedural provisions governing governmental entities that desire to obtain e-mails as evidence from third-party service providers under Title II of the Electronic Communications Privacy Act ("ECPA"), also known as the Stored Communications Act ("SCA"), are unconstitutional. These provisions violate the Fourth Amendment's privacy guarantees because the pro-government provisions severely outweigh the privacy guaranteed to e-mail account holders. Part II of this Note examines the history of the Fourth Amendment and discusses sections 2703, 2704, and 2705 of the SCA, which address disclosure of customer e-mail from

---

[3] *See* Ohio v. Roberts, 448 U.S. 56 (1980). Establishing that evidence against an accused must satisfy "particularized guarantees of trustworthiness." *Id.* at 66. The Court stated that it

> found no commentary suggesting that the Court has misidentified the basic interests to be accommodated. Nor has any commentator demonstrated that prevailing analysis is out of line with the intentions of the Framers of the Sixth Amendment. . . . [W]e reject the invitation to overrule a near-century of jurisprudence. Our reluctance to begin anew is heightened by the Court's implicit prior rejection of principal alternative proposals . . . .

Id. at 66 n.9.

service providers and aspects of delayed notice.[4] Part III analyzes the constitutional problems presented by sections 2703 and 2705 of the SCA, noting, specifically, the disparity in safeguards afforded to the government as compared to account holding individuals.[5] Part IV proposes amendments to the SCA that will more effectively protect the Fourth Amendment rights of citizens without jeopardizing the government's interest in preserving electronic evidence.[6] Finally, Part V analyzes the hypothetical introduced above under these proposed amendments to the SCA.[7]

II. BACKGROUND

> *The poorest man may in his cottage bid defiance to all the forces of the crown. It may be frail – its roof may shake – the wind may blow through it – the storm may enter – the rain may enter – but the King of England cannot enter! – all his force dares not cross the threshold of the ruined tenement!*[8]

The sanctity of privacy that William Pitt publicly announced regarding the Crown's ability to conduct searches and seizures in the eighteenth century governs e-mail today. Because general warrants violate natural expectations of privacy, our forefathers incorporated the Fourth Amendment into the Bill of Rights in order to enshrine powerful constitutional protection to a practice that had been gradually achieved in Great Britain.[9] Yet, new technologies have created new challenges for

---

4 *See infra* Part II (discussing Internet technology, the history of electronic communications law, and relatively recent applications of electronic communications law to e-mail and Internet searching).

5 *See infra* Part III (analyzing the overwhelming unconstitutional possibilities created by reading sections 2703, 2704, and 2705 together and the inconsistent judicial interpretations of these provisions).

6 *See infra* Part IV (proposing amendments to the current SCA provisions governing e-mail seizure to provide for more universal application, require police officer presence during seizures, and clarify objective terminology so that courts will have clear meaning).

7 *See infra* Part V.

8 William Pitt, The Elder, Earl of Chatham, Speech on the Excise Bill, Parliament (March 1763), *reprinted in* HENRY PETER BROUGHAM, 1 HISTORICAL SKETCHES OF STATESMEN WHO FLOURISHED IN THE TIME OF GEORGE III 42 (Richard Griffin & Company 1839).

9 U.S. CONST. amend. IV.

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

Id. But c.f. David E. Steinberg, *Self-Enhanced Searches and the Irrelevance of the Fourth Amendment*, 16 WM. & MARY BILL RTS. J. 465, 482–84 (2007) (suggesting that three specific

the historically cherished Anglo-American right to privacy.[10] Electronic communications statutes embody outdated technological theories and fail to protect privacy interests.[11] Part II.A provides a brief description of Internet Service Providers ("ISPs").[12] Part II.B then discusses the background of Fourth Amendment jurisprudence relevant to Title II of the SCA.[13] Finally, Part II.C introduces the procedural aspects of sections 2703, 2704, and 2705 of the SCA.[14]

A. What Is an Internet Service Provider?

ISPs allow individuals to access accounts from which they may send and receive e-mail.[15] The server itself may be local, or it may be wide,

---

controversies—the John Wilkes cases, the Paxton's case, and the Townshend Act—led to the adoption of the Fourth Amendment).

[10] David Snyder, *The NSA's "General Warrants": How the Founding Fathers Fought an 18th Century Version of the President's Illegal Domestic Spying*, ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/legal/cases/att/generalwarrantsmemo.pdf (last visited Jan. 31, 2008) [hereinafter "Snyder"] (posing the question as to whether America will follow the Framers' intent to step away from King George's "unfettered executive power"). *Id.* Snyder states that

> [w]e've now come full circle. The president has essentially updated this page from King George's playbook, engaging in dragnet surveillance of millions of Americans, regardless of whether they are suspected of a crime. The founders of this country took steps to limit precisely this sort of unfettered executive power. Will we?

Id.

[11] Robert A. Pikowsky, *An Argument for a Technology-Neutral Statute Governing Wiretapping and Interception of E-mail*, 47-OCT ADVOC 23 (2004) (stating that "[t]he outdated statutory scheme creates a needlessly complex set of rules that unduly focuses on the different technologies of communication rather than the underlying privacy interest, which remains constant regardless of the technology employed to convey the message[]").

[12] *See infra* Part II.A (explaining the basic functions of Internet Service Providers and e-mail).

[13] *See infra* Part II.B (setting forth the birth of electronic communications leading up to the governance of e-mail, and discussing false notions of privacy and the reasonableness of searches).

[14] *See infra* Part II.C (discussing procedural aspects of three sections of the SCA).

[15] E-mail is defined in the Senate Report for the ECPA as

> a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system.

such as the Internet.[16] The Internet is not a centralized system and can be thought of as a "crazy game of connect-the-dots."[17] ISPs give individuals

---

> Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.

S. REP. NO. 99-541, at 8 (1986). This definition of e-mail transmissions over telephone lines exemplifies the pace at which technology is progressing. Today, eighteen years later, the transmissions occur over telephone lines, digital subscriber lines ("DSLs"), and cable lines. This is not to say that the definition is not applicable. *See* MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 405 (11th ed. 2004). Compared to the Senate Report, Merriam-Webster's definition essentially gets the same point across but appears to assume that the reader is familiar with the concept of e-mail; Merriam-Webster defines e-mail as "a means or system for transmitting messages electronically (as between computers on a network)"; and "messages sent and received electronically through an e-mail system[.]" *Id*. *See also* MSN. Encarta, http://encarta.msn.com/encyclopedia_761566348/E-Mail.html (last visited Jan. 31, 2008). E-mail is defined as a "method of transmitting data, text files, digital photos, or audio and video files from one computer to another" over a condensed or broad network. *Id*. Since the 1990s, e-mail has greatly enhanced the communications of both businesses and individuals. *Id*.

[16] *See Glossary of Internet & Web Jargon*, UC BERKELEY—TEACHING LIBRARY INTERNET WORKSHOPS, http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Glossary.html #RSS (last visited Jan. 31, 2008). The "Internet" is defined as

> [t]he vast collection of interconnected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's. An "internet" (lower case i) is any computers connected to each other (a network), and are not part of the Internet unless the [sic] use TCP/IP protocols. An "intranet" is a private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use. An intranet may be on the Internet or may simply be a network.

Id. Further, a "server" may be defined as

> [a] computer running that software, assigned an IP address, and connected to the Internet so that it can provide documents via the World Wide Web. Also called HOST computer. Web servers are the closest equivalent to what in the print world is called the "publisher" of a print document. An important difference is that most print publishers carefully edit the content and quality of their publications in an effort to market them and future publications. This convention is not required in the Web world, where anyone can be a publisher; careful evaluation of Web pages is therefore mandatory. Also called a "Host."

Id. *See also* MSN. Encarta, *supra* note 15. Servers are computers that supply "services or data to other machines on a local area network (LAN) or a wide area network (WAN) such as the Internet." *Id*. Essentially, files, pictures, codes, and messages are transmitted back and forth between servers throughout the network. *Id.*

[17] Rob Kolstad, *Becoming an Internet Service Provider*, http://docs.rinet.ru/becomeISP/ (last visited Jan. 31, 2008). Kolstad notes that the Internet's connectivity aspects are "not organized like an army with a 'President' node at the top with 'General' nodes directly beneath it. The Internet is more like a hodge-podge of various interconnections that resemble more a crazy game of connect-the-dots than a cleverly designed backbone-with-branches." *Id.* Furthermore,

the means to send messages from individual computers via commercial e-mail programs or mail-user agents.[18] Essentially, ISPs provide account holders the ability to send, receive, and store opened and unopened e-mails associated with the ISPs' systems, which may also be thought of as the mail servers themselves.[19] The e-mails stored on ISP systems are available for different lengths of time depending on the server.[20] Having

---

> To connect to the Internet, one identifies an 'Internet Service Provider' (ISP) that is already connected to the Internet and negotiates a business agreement to join the Internet through them. The list of ISPs is large and includes tiny ISPs with a single computer and some dial-in lines and large ISPs with thousands of miles of fiber strung around the country. Different ISPs offer different strengths and different costs.

Id.

[18] MSN Encarta, *supra* note 15. Most commercial or mail-user programs have text editors for composing messages, and all the sender needs to provide is a destination address. *Id. See* R. Kayne, What is a Mail User Agent, http://www.wisegeek.com/what-is-a-mail-user-agent.htm (last visited Jan. 15, 2009). Wise Geek defines mail user agent as follows:

> A mail user agent (MUA) is an email program; software designed to collect and send electronic mail. It is also referred to as an email program, or email client. The term "mail user agent" is less familiar to the average person, but is used in email headers. The headers of the email supply information to the mail servers or computers that handle transferring messages across networks like the Internet.

Id. See KENNETH E. JOHNSON, THE LAWYER'S QUICK GUIDE TO E-MAIL 10 (1998). The actual communication process for e-mails takes place as follows:

> When you are ready to send or receive e-mail, you log on to the Internet through your ISP. Your e-mail program communicates with the mail server at the ISP through "protocols," which are simply definitions of how computers talk to one another. Standard protocols allow different computers and computers with different operating systems and software to communicate reliably, since they all speak the same "language."

Id.

[19] AMERICAN PROSECUTORS RESEARCH INSTITUTE (APRI), NATIONAL DISTRICT ATTORNEYS ASSOCIATION, THE ECPA, ISPS & OBTAINING E-MAIL: A PRIMER FOR LOCAL PROSECUTORS 10 (2005), http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf.

[20] *Id.* at 20. The APRI report addresses the problem of varying retention periods of ISPs:

> Retention periods for subscriber and transactional records and e-mail content records vary greatly among ISPs. Moreover, there are no statutorily mandated or industry guidelines regarding preservation of this information prior to request from law enforcement. Indeed, it is not unusual for ISPs to dispose of e-mail information and content after only days, even hours.

Id. See Jon Swartz & Kevin Johnson, *U.S. Asks Internet Firms to Save Data,* USA TODAY, June 1, 2006, *available at* http://www.usatoday.com/tech/news/internetprivacy/2006-05-31-internet-records_x.htm. On a similar note, top law enforcement officials have requested longer retention periods, than days or hours, of histories from Internet companies such as Google, Microsoft, AOL, Comcast, and Verizon. *Id.* Problems associated with this request

a basic understanding of how ISPs handle e-mail is essential to assessing how much invasive power the government should have. Fourth Amendment history and electronic communications case law is an appropriate place to begin the discussion of shielding individuals from the dangers of governmental privacy invasion.[21]

B. Fourth Amendment Jurisprudence Relevant To Title II of the Stored Communications Act

In England, in the 1760s, motivated by the reign of King George III, William Pitt declared certain individual rights fundamental, notoriously advocated for freedom of speech, and chastised general warrants granted by the King.[22] In the United States, the Fourth Amendment resulted because the former colonists of the states feared, and therefore disliked, warrants that would allow the police to search any and all persons—merely on the government's whim.[23] Contrary to these general warrants, the Fourth Amendment's text, which remains unchanged since its adoption in 1793, guarantees freedom from unreasonable searches and seizures.[24] In 1980, the United States Supreme Court held that

---

for longer retention periods are cost-based and Internet companies' concerns for violating operating policies. *Id.*

[21] *See infra* Part II.B.

[22] Wilkes v. Wood, Lofft 1, 98 Eng. Rep. 489, 498 (C.P. 1763). In *Wilkes*, the court eventually found forty-five general warrants invalid and declared general warrants "totally subversive of the liberty of the [warrant's] subject." *Id.* (alteration in original).

[23] *See* Snyder, *supra* note 10. Snyder notes that because a newspaper criticized the King of England, the King signed off on any general warrants applicable to printers or those taking part in publication. *Id.* The King's officers obtained power to rummage through all manuscripts and writings and cut through hundreds of locks. *Id.* Furthermore, the general warrants "spurred colonists toward revolution and directly motivated James Madison's crafting of the Fourth Amendment." *Id.* (footnote omitted).

[24] *See supra* note 9 (citing the text of the Fourth Amendment). *See also* Snyder, *supra* note 10. *See* MASS. CONST. of 1780, art. XIV. Snyder correctly notes that James Madison relied on the Massachusetts' Constitution when drafting the Fourth Amendment. Snyder, *supra* note 10. *See* MASS. CONST. of 1780, art. XIV. The Massachusetts Constitution provided as follows:

> Every subject has a right to be secure from all unreasonable searches, and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

Id.

"'indiscriminate searches and seizures conducted under the authority of "general warrants" were the immediate evils that motivated the framing and adoption of the Fourth Amendment.'"[25] Since the Amendment's incorporation into the Constitution, courts have struggled to determine exactly what types of searches are reasonable, especially in regard to recent electronic communications.[26] The relevant case law discussing reasonable searches begins with the governance of telephone calls in *Katz v. United States* and *Smith v. Maryland*.[27]

---

[25] Snyder, *supra* note 10 (quoting Payton v. New York, 445 U.S. 573, 583 (1980)). *See Payton*, 445 U.S. at 577. *Payton* explained why the "reasons for upholding warrantless arrests in a public place do not apply to warrantless invasions of the privacy of the home." *Id*.

> It is a "basic principle of Fourth Amendment law" that searches and seizures inside a home without a warrant are presumptively unreasonable. Yet is [sic] is also well settled that objects such as weapons or contraband found in a public place may be seized by the police without a warrant. The seizure of property in plain view involves no invasion of privacy and is presumptively reasonable, assuming that there is probable cause to associate the property with criminal activity.

Id. at 586–87 (footnote omitted). The Court turned to common law in order to analyze the fundamental importance of privacy in the home:

> It is obvious that the common-law rule on warrantless home arrests was not as clear as the rule on arrests in public places. Indeed, particularly considering the prominence of Lord Coke, the weight of authority as it appeared to the Framers was to the effect that a warrant was required, or at the minimum that there were substantial risks in proceeding without one. The common-law sources display a sensitivity to privacy interests that could not have been lost on the Framers. The zealous and frequent repetition of the adage that a "man's house is his castle," made it abundantly clear that both in England and in the Colonies "the freedom of one's house" was one of the most vital elements of English liberty.

Id. at 596–97 (footnote omitted).

[26] James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, PRACTICING LAW INST. NO. 11253, 407, 412 (2007). Dempsey stated that "[p]rivacy is an important constitutional value and a crucial component of the trust necessary for the flourishing of digital commerce and democracy. However, while technology has changed dramatically in the past twenty years, privacy law has not kept pace." *Id.*

[27] Smith v. Maryland, 442 U.S. 735 (1979); Katz v. United States, 389 U.S. 347 (1967).

1. *Katz* and *Smith* Establish Basic Standards for Evaluating Electronic Communications[28]

The United States Supreme Court found itself torn between the competing interests of privacy and security in the 1960s and 1970s when it decided *Katz* and *Smith*.[29] In analyzing the Fourth Amendment, these judicial opinions distinguished the *act* of making a phone call from the *content* of the call itself.[30] In *Katz*, the Plaintiff's telephone conversations were captured while he spoke in a telephone booth.[31] The Court noted that the Plaintiff "sought to exclude when he entered the booth . . . not the intruding eye . . . [but] the uninvited ear."[32] Relying on *Katz* and

---

[28] *Smith*, 442 U.S. at 735; *Katz*, 389 U.S. at 347. *Katz* and *Smith* set the stage as the relevant case law governing electronic communication of telephone calls. *See Smith*, 442 U.S. at 735; *Katz*, 389 U.S. at 347.

[29] *Katz*, 389 U.S. at 352. In *Katz*, the United States Supreme Court declared that surveillance of telephone conversations amounted to a search where the caller "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." *Id.* The Court held that because of this entitlement, Defendant Katz did not give up his privacy rights when he engaged in a telephone conversation. *Id. See* Snyder, *supra* note 10, at 6. Snyder stated that "[i]n recognizing that [sic] the principle that the Fourth Amendment prohibits indiscriminate searches regardless of the technology involved, the Court made it plain that advanced technology doesn't clear the government of the duty to establish probable cause, and to receive a warrant, before rummaging through the private lives of Americans." *Id*. *See* United States v. Miller, 425 U.S. 442 (1976). Further, in *Miller*, the Defendant filed a motion to suppress records relating to his accounts at two banks after alleging that the records had been illegally seized in violation of the Fourth Amendment. *Id*. The Court held that, "[o]n their face, the documents subpoenaed here [we]re not respondent's 'private papers[;]' . . . respondent c[ould] assert neither ownership nor possession. Instead, these [we]re the business records of the banks." *Id.* at 440.

[30] *Katz*, 389 U.S. at 360–361 (Harlan, J., concurring). Justice Harlan concurred, stating that *Katz* holds only

> (a) that an enclosed telephone booth is an area where, like a home, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.

Id.

[31] *Id.* at 352.

[32] *Id*. The Court further noted:

> He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to

Smith, courts have recognized that certain account information is expected to be available to police powers without warrants, such as a list of the numbers dialed from a phone, check information, and account registration information.[33] However, information that is not specifically content-oriented is expected to be private because people have a right to reasonably expect that private content will not be searched without a warrant.[34] In order to determine whether e-mail privacy is protected by the Fourth Amendment, further examination of Fourth Amendment jurisprudence is necessary. *Smith* set forth two requirements that are necessary to trigger Fourth Amendment protection: first, a reasonable expectation of privacy; and second, that the defendant's expectation of privacy is viewed as objectively reasonable by society.[35]

The first appropriate question raised in *Smith* is whether an individual has a reasonable expectation of privacy with regard to e-mail.[36] Particularly in the private sector, the "third-party doctrine"[37]

> ignore the vital role that the public telephone has come to play in private communication.

Id. (footnotes omitted).

[33] United States v. Phibbs, 999 F.2d 1053, 1078 (6th Cir. 1993). Phone and credit card records have been found to be "readily accessible to employees during the normal course of business[,]" and therefore Defendant may not claim a reasonable expectation of privacy. *Id.*; *see also Miller*, 425 U.S. at 442 (discussing that where banking information, such as checks and deposit slips, is available to employees during the normal course of business, there can be no expectation of privacy). *See Smith*, 442 U.S. at 741. Further, in *Smith*, phone number records recorded by a pen register are also banned from information of which an individual may expect privacy. *Id*. *See also* 18 U.S.C. § 2703(c)(2) (2006). Comparatively, in regard to e-mail, the SCA has explicitly stated that e-mail account holder information is not expected to be private and, therefore, may be obtained by police without notice being provided to the customer. *Id*. Specifically, name, address, local and long distance telephone records, length of service and type, any identifying numbers including assigned network address, and means and source of payment are not generally expected to be private information by individual account holders. *Id.*

[34] *See supra* note 29 (discussing the opinion in *Katz*, which found that words uttered into a mouthpiece are not expected to be broadcast to the world).

[35] *Smith*, 442 U.S. at 740 (1979). *Smith* held that the reasonable expectation of privacy

> embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy," whether, in the words of the *Katz* majority, the individual has shown that "he seeks to preserve [something] as private." The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable,'"—whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances.

Id. (alteration in original) (internal citations omitted).

[36] *Id. Smith* held that application of the Fourth Amendment is directly dependent on whether an individual has a "'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." *Id.* (citing Rakas v. Illinois, 439 U.S.

comes into play because many e-mail messages are designed to be sent to a third party or stored on an Internet company's remote server.[38] The third-party doctrine holds that once an individual voluntarily exposes information to another individual, the original party that disclosed the information no longer maintains a reasonable expectation of privacy

---

128, 143, 150, 151 (1978)); United States v. Chadwick, 433 U.S. 1, 7 (1977); *Miller*, 425 U.S. at 442; United States v. Dionisio, 410 U.S. 1, 14 (1973); Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Mancusi v. DeForte, 392 U.S. 364, 368 (1968); Terry v. Ohio, 392 U.S. 1, 9 (1968).

[37] "Third-party doctrine" is phraseology used by the author of this Note. *See Miller*, 425 U.S. at 443; *see also White*, 401 U.S. at 752; Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States 373 U.S. 427 (1963). The Court has consistently described the "third-party doctrine" as "information revealed to a third party and conveyed by him [the third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443. *See also White*, 401 U.S. at 752; *Hoffa*, 385 U.S. at 302; *Lopez*, 373 U.S. 427.

[38] Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 1, 22 (2007). Lawless stated:

> The messenger/recipient distinction is clearly exhibited in the context of e-mail. If one sends an e-mail "to" America Online (AOL) for account assistance, AOL would be the recipient of the message; on the other hand, where AOL merely transmits the message and stores it on its server, it is not the recipient of the communication but its messenger.

Id. See O'Connor v. Ortega, 480 U.S. 709, 717 (1987). The discussion in this Note is based on private sector e-mail. *See id.* Courts adapt their analysis for governmental workplace situations to use the "operational realities" test. *See id.* The Supreme Court acknowledged the operational realities test for the first time in *O'Connor*. *Id.* In *O'Connor*, the Court held:

> The operational realities of the workplace, however, may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of [sic] actual office practices and procedures, or by legitimate regulation. . . . The employee's expectation of privacy must be assessed in the context of the employment relation. An office is seldom a private enclave free from entry by supervisors, other employees, and business and personal invitees. Instead, in many cases offices are continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits. Simply put, it is the nature of government offices that others—such as fellow employees, supervisors, consensual visitors, and the general public—may have frequent access to an individual's office.

Id. The operational realities test has its own discrepancies which are not discussed in this Note, but for a general overview and examples especially regarding Internet searches, see Lawless, *supra* note 38, at 22 (suggesting that the Fourth Amendment is the proper remedial tool for suppression of Internet search records).

with regard to the information.[39] Package and letter carrier services are not third parties for purposes of this doctrine; instead, only the recipient who opens the package qualifies as a third party.[40] Comparably, if a sufficient privacy interest applies to e-mails, then the government must have probable cause to secure a warrant before seizing the e-mails.[41] On the contrary, if e-mails do not contain a sufficient privacy interest, then the government must meet only a reasonable standard before seizing the e-mails.[42]

Second, *Smith* advises that e-mail should be protected under the Fourth Amendment when the user's privacy interest is reasonable.[43] For example, in *Warshak v. United States* ("*Warshak I*"), the government seized the Plaintiff's e-mails directly from ISPs along with, as allowed by federal statute, the Plaintiff's account information.[44] The government

---

[39] United States v. Jacobsen, 466 U.S. 109 (1984). In *Jacobsen*, employees of Federal Express observed white powder that seemed to be concealed in four baggies within a tube that protruded from a box damaged by transport. *Id.* at 111. The Court held that defendants, addressees of package, had no expectation of privacy regarding the baggies due to the unsealed condition of the package and the insurance policy that Federal Express carried. *Id.* at 111, 119.

[40] United States v. Chadwick, 433 U.S. 1,10 (1977); United States v. Van Leeuwen, 397 U.S. 249, 251 (1970); *Ex parte* Jackson, 96 U.S. 727, 733 (1878). *See supra* note 37 (explaining how the Court has described the third-party doctrine, and showing how package and letter carrier services are not third parties for purposes of this doctrine).

[41] Warshak v. United States (Warshak I), 490 F.3d 455, 469 (6th Cir. 2007), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). The court compared *Phibbs* and *Miller* to *Katz* and *Smith*, where the issue in those cases was whether an individual has a reasonable expectation of privacy for information desired by the government. *Id.* at 470. "The distinction between *Katz* and *Miller* makes clear that the reasonable expectation of privacy inquiry in the context of shared communications must necessarily focus on two narrower questions than the general fact that the communication was shared with another." *Id.*

[42] *Id.*

[43] Smith v. Maryland, 442 U.S. 735 (1979). *See supra* note 35 and accompanying text.

[44] *Warshak I*, 490 F.3d at 460, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). The SCA distinguishes between account information, which the government is generally allowed to obtain, and content of e-mail messages. 18 U.S.C. § 2703 (2006); see also *infra* note 123 and accompanying text for the statutory list of general account information. The burden is much higher for content seizures than simply seizures of account information. *Id.* In *Warshak I*, the Magistrate Judge issued an order which

> Direct[ed] [the] internet service provider . . . to turn over to government agents information pertaining to Warshak's e-mail account with NuVox. The information to be disclosed included (1) customer account information, such as application information, "account identifiers," "[b]illing information to include bank account numbers," contact information, and "[any] other information

argued that the Plaintiff had only a reasonable expectation of privacy with regard to e-mail, similar to the expectation of privacy for a letter mailed by the United States Postal Service.[45] E-mails resemble paper letters because both typically have an addressed recipient.[46] Similarly, both electronic communications services and postal services carry items that are clearly less private than paper letters, such as blogs,[47] magazines,

---

> pertaining to the customer, including set up, synchronization, etc."; (2) "[*t*]*he contents of wire or electronic communications* (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled" by Warshak; and (3) "[a]ll Log files and backup tapes."

490 F.3d at 460, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III) (some alterations in original) (emphasis added).

[45] *Id.* Warshak argued that "the government could not get around the privacy interest attached to a private letter by simply subpoenaing the postal service with no showing of probable cause, because unlike in *Phibbs*, postal workers would not be expected to read the letter in the normal course of business." *Id.* at 471. Letters and packages have been protected under the Fourth Amendment for more than two hundred years. *See Ex parte Jackson*, 96 U.S. 727. The Court acknowledged this protection of privacy in 1878 when it decided in *Ex parte Jackson* that "[l]etters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." *Id.* at 733. And the Court observed further:

> No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment [sic] of the Constitution.

Id.

[46] *Warshak I*, 490 F.3d at 472, *vacated on other grounds en banc by* U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). E-mails "typically have a limited, select number of recipients." *Id.*

[47] As defined by *Merriam-Webster*, a blog is "a Web site that contains an online personal journal with reflections, comments, and often hyperlinks provided by the writer[.]" Http://www.m-w.com/ (search "blog"). *See also Glossary of Internet & Web Jargon,* UC BERKELEY—TEACHING LIBRARY INTERNET WORKSHOPS, http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Glossary.html#Internet (last visited Jan. 31, 2008). The Berkeley teaching library defines a blog as:

> A blog (short for "web log") is a type of web page that serves as a publicly accessible personal journal (or log) for an individual. Typically updated daily, blogs often reflect the personality of the author. Blog software usually has an archive of old blog postings. Many blogs can be searched for terms in the archive. Blogs have become a vibrant, fast-growing medium for communication in professional, poltical [sic], news, trendy, and other specialized web communities. Many blogs provide RSS feeds [Rich Site Summary], to

and leaflets and brochures addressed generically to "Resident."[48] Essentially, in the normal course of business, both ISPs and United States postal workers are expected to refrain from reading the contents of "sealed" items.[49]

Letters and e-mails, similar to phone calls, are not entitled to absolute protection under the Fourth Amendment because their contents may be disclosed by the recipient.[50] As the Supreme Court explained, "when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities[.]"[51] This may seem like common sense because, as most people learned in kindergarten, best friends do not always keep secrets.[52] Unfortunately, due to statutory exceptions for both law enforcement and emergencies, situations before the court are not always this simple.[53]

> which one can subscribe and receive alerts to new postings in selected blogs.

Id.

[48] *Ex Parte Jackson*, 96 U.S. at 733. The different levels of expectation of privacy simply draws attention to the fact that some mailings, whether electronic or snail, are less private than others. *Id.* The Court held in *Ex Parte Jackson* that:

> [A] distinction is to be made between different kinds of mail matter,-between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined.

Id. See Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001). Therefore, today, users of such electronic communication, such as Internet bulletin boards and blogs, "would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting." *Id.*

[49] *Warshak I*, 490 F.3d at 471, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). "Sealed" in the normal course of business refers to an item that is mailed with a specific addressee and that is packaged and addressed correctly. *Id.*

[50] *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) (stating 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[]"). Upon sending information to another individual, the sender loses his or her expectation of privacy because the receiver can distribute the information as the receiver sees fit. *Id.*

[51] *Id.*

[52] *See infra* note 55 (discussing an instance in which the third-party rule prevailed against a challenge to the Fourth Amendment because right to privacy does not extend to voluntary third parties).

[53] *Warshak I*, 490 F.3d. at 462, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). "Portions of the SCA that are not directly at stake here prohibit unauthorized access of electronic communications (§ 2701) and prohibit a service provider from divulging the

However, generally, the recipient of information that was disclosed via mail does not have the right to protect this information against governmental searches, and this is known as the third-party exception to individual expectations of privacy.[54] Therefore, the recipient may be subpoenaed to disclose the contents of a conversation, message, or letter, and in such instances, the sender may not raise a Fourth Amendment challenge.[55] Of course, e-mail complicates matters because the technological medium allows for inexpensive and indefinite storage capacity.[56] Still, similar to disclosure of information to a third-party in the context of mail, if lowered expectations of privacy are established with regard to e-mails, a Fourth Amendment challenge may be barred.[57] The next two cases address one specific judge's uneasiness with breaching e-mail privacy.[58]

2. Sister New York Cases—*Doe I* and *Doe II*: Lack of Notice

In both *Doe v. Ashcroft* ("*Doe I*") and *Doe v. Gonzales* ("*Doe II*"), Judge Marrero of the Southern District of New York declared unconstitutional statutorily issued gag orders for government officials who obtained electronic communications as evidence.[59] Both cases, although later partially overruled, discuss the importance of an individual's privacy as it relates to e-mail and Congress's competing interest of maintaining

---

contents of electronic communications that it is storing for a customer with certain exceptions pertaining to law enforcement needs (§ 2702)." *Id.*

54 SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 737 (1984). In *SEC v. Jerry T. O'Brien*, the Court declared that "when a person communicates information to a third party, even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities." *Id.* at 735–36.

55 *See* United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995). In *King*, the court stated that "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information . . . ." *Id.*

56 *See* Dempsey, *supra* note 26, at 418. Dempsey explained the changes in storage space and methods for storing since the enactment of the current laws, stating that

> [i]n the past, particularly at the time when current email privacy laws were written, email users accessed their email by downloading it onto their personal computers. That process often resulted in the deletion of the email from the computers of the service provider. Now, email--including email that has been read but which still has value to the user--often sits on a third party server accessible via the Web.

Id.

57 *See supra* Part II.B.1 (discussing expectations of privacy as established in *Katz*).

58 *See infra* Part II.B.3.

59 Doe v. Gonzalez (Doe II), 500 F. Supp. 2d 379 (S.D.N.Y. 2007), *overruled in part by* Doe, Inc. v. Mukasey, 549 F.3d 861 (2d. Cir. 2008); Doe v. Ashcroft (Doe I), 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *overruled in part by* Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008).

national security.[60] First, in *Doe I*, in 2004, the court held that National Security Letters ("NSLs")[61] used by the FBI were unconstitutional

---

[60] *Gonzalez* (*Doe II*), 500 F. Supp. 2d 379, *overruled in part by* Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008); *Ashcroft* (*Doe I*), 334 F. Supp. 2d 471, *overruled in part by* Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008). In 2008, the Second Circuit Court of Appeals took up the issue and overruled in part *Doe I* and *Doe II*, declaring:

> To recapitulate our conclusions, we (1) construe subsection 2709(c) to permit a nondisclosure requirement only when senior FBI officials certify that disclosure may result in an enumerated harm that is related to "an authorized investigation to protect against international terrorism or clandestine intelligence activities," (2) construe subsections 3511(b)(2) and (b)(3) to place on the Government the burden to show that a good reason exists to expect that disclosure of receipt of an NSL will risk an enumerated harm, (3) construe subsections 3511(b)(2) and (b)(3) to mean that the Government satisfies its burden when it makes an adequate demonstration as to why disclosure in a particular case may result in an enumerated harm, *(4) rule that subsections 2709(c) and 3511(b) are unconstitutional to the extent that they impose a nondisclosure requirement without placing on the Government the burden of initiating judicial review of that requirement, and (5) rule that subsections 3511(b)(2) and (b)(3) are unconstitutional to the extent that, upon such review, a governmental official's certification that disclosure may endanger the national security of the United States or interfere with diplomatic relations is treated as conclusive.*

Doe, Inc. v. Mukasey (Doe III), 549 F.3d 861, 883 (2d Cir. 2008) (emphasis added) (agreeing in holdings (4) and (5) that certain provisions of the ECPA are indeed unconstitutional). Where the district court invalidated the entire section of the Act, the Second Circuit Court instead only partially invalidated certain sections and instilled its own procedural safeguards:

> [W]e need not invalidate the entirety of the nondisclosure requirement of subsection 2709(c) or the judicial review provisions of subsection 3511(b). Although the conclusive presumption clause of subsections 3511(b)(2) and (b)(3) must be stricken, we invalidate subsection 2709(c) and the remainder of subsection 3511(b) only to the extent that they fail to provide for Government-initiated judicial review. The Government can respond to this partial invalidation ruling by using the suggested reciprocal notice procedure. With this procedure in place, subsections 2709(c) and 3511(b) would survive First Amendment challenge.

Id. at 884. After salvaging the statutory interpretations and partial invalidations, the Second Circuit remanded the case back to the district court to give the Government an opportunity to satisfy the newly outline constitutional standards for maintaining disclosure. *Id.* at 885. Therefore, this case, and accordingly the judicial interpretations of the statute are not yet over.

[61] *Ashcroft* (*Doe I*), 334 F. Supp. 2d at 475, *overruled in part by* Doe, Inc. v. Mukasey (Doe III), 549 F.3d 861 (2d Cir. 2008). NSLs "constitute a unique form of administrative subpoena cloaked in secrecy and pertaining to national security issues. The statute bars all NSL recipients from ever disclosing that the FBI has issued an NSL." *Id*. *See* Adam Liptak, *Judge Voids F.B.I. Tool Granted By Patriot Act*, N.Y. TIMES, Sept. 7, 2007, at A18. A columnist for the New York Times stated that the letters

because they demanded a wide variety of information, were too broad, and did not include a time limit for their sealed notice.[62] While the government appealed, Congress amended the pertinent statute—the USA Patriot Act—and the judgment was vacated pursuant to the Act.[63] Then, Plaintiff American Civil Liberties Union ("ACLU") brought another action in *Doe II*, claiming that the Patriot Act as amended was still unconstitutional.[64]

In *Doe I*, the Plaintiffs—Doe and the ACLU—challenged the Patriot Act's nondisclosure requirement.[65] In response, Judge Marrero stated

---

> allowed the F.B.I. not only to force communications companies, including telephone and Internet providers, to turn over the records without court authorization, but also to forbid the companies to tell the customers or anyone else what they had done. Under the law, enacted last year, the ability of the courts to review challenges to the ban on disclosures was quite limited.

Id.

[62] *Ashcroft* (*Doe I*), 334 F. Supp. 2d at 511, *overruled in part by* Doe, Inc. v. Mukasey (Doe III), 549 F.3d 861 (2d Cir. 2008).

> The Court holds only that such fundamental rights are certainly implicated in some cases in which the Government may employ § 2709 broadly to gather information, thus requiring that the process incorporate the safeguards of some judicial review to ensure that if an infringement of those rights is asserted, they are adequately protected through fair process in an independent neutral tribunal. Because the [safeguard provisions] are wholly absent here, the Court finds on this ground additional cause for invalidating § 2709 as applied.

Id. Furthermore, the court generally held that "compulsory, secret, and unreviewable production of information required by the FBI's application of 18 U.S.C. § 2709 violates the Fourth Amendment, and that the non-disclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment." *Id.* at 526–27.

[63] *Gonzalez* (*Doe II*), 500 F. Supp. 2d at 385–86, *overruled in part by* Doe, Inc. v. Mukasey (Doe III), 549 F.3d 861 (2d Cir. 2008) (giving a brief overview of the *Ashcroft* (*Doe I*) holding and the subsequent amendment of the USA Patriot Act).

[64] *Id.* at 395–96. The district court was concerned with nondisclosure orders and congressional violations, through the use of the statute, of fundamental principles of checks and balances. *Id.*

[65] *Ashcroft* (*Doe I*), 334 F. Supp. 2d at 474–75, *overruled in part by* Doe, Inc. v. Mukasey (Doe III), 549 F.3d 861 (2d Cir. 2008). The nondisclosure requirement

> authorizes the Federal Bureau of Investigation ("FBI") to compel communications firms, such as internet service providers ("ISPs") or telephone companies, to produce certain customer records whenever the FBI certifies that those records are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." The FBI's demands under § 2709 are issued in the form of national security letters ("NSL*s*"), which constitute a unique form of administrative subpoena cloaked in secrecy and pertaining to national security issues. The statute bars all NSL recipients from ever disclosing that the FBI has issued an NSL.

Id. (footnote omitted).

that "[t]he statute fail[ed] constitutional strict scrutiny[] . . . because it require[d] the court to blindly credit a finding that there 'may' be a reason—potentially any conceivable and not patently frivolous reason—for it to believe disclosure [would] result in a certain harm."[66] In *Doe II*, when the case came before the court again in 2007, Judge Marrero held for the second time that the use of the NSLs was unconstitutional because it lacked procedural safeguards.[67] Essentially, Judge Marrero's opinions reflected his discomfort about giving the FBI such broad discretion without ensuring sufficient safeguards.[68] The notion of e-mail privacy is described somewhat superficially by more recent cases that specifically address sections 2703 and 2705 of the SCA.[69]

3. Current E-Mail Jurisprudence: *Warshak I*, *Warshak II*, and *Allen*

Few cases analyze the constitutionality of, or even discuss, sections 2703 and 2705 of the SCA. One case that does, however, is *Warshak I*.[70] In *Warshak I*, the government obtained a court order directing Plaintiff Steven Warshak's ("Warshak") ISP to turn over both Warshak's e-mail account information and the contents of his e-mails.[71] The court issued the order under seal, which, for ninety days, prohibited the ISP from

---

66 *Gonzalez* (*Doe II*), 500 F. Supp. 2d at 418, *overruled in part by* Doe, Inc. v. Mukasey (Doe III), 549 F.3d 861 (2d Cir. 2008); *see also* http://news.findlaw.com/scripts/printer_friendly.pl?page=/andrews/bt/prv/20070925/20070925_doe.html. (last visited Jan. 31, 2008).

67 *Gonzalez* (*Doe II*), 500 F. Supp. 2d at 425, *overruled in part by* Doe, Inc. v. Mukasey (Doe III), 549 F.3d 861 (2d Cir. 2008) (holding that "§ 2709(c) is unconstitutional under the First Amendment because it functions as a licensing scheme that does not afford adequate procedural safeguards[] . . .").

68 *Ashcroft* (*Doe I*), 334 F. Supp. 2d at 475–76, *overruled in part by* Doe, Inc. v. Mukasey (Doe III), 549 F.3d 861 (2d Cir. 2008). Due to the fact that section 2709(c) prohibited recipients of the NSLs from giving notice to anyone and that there was no provision providing that the ban could be lifted, the section violated the Fourth Amendment because, as applied, it barred or deterred judicial challenge. *Id. See also Gonzalez* (*Doe II*), 500 F. Supp. 2d at 425, *overruled in part by* Doe, Inc. v. Mukasey (*Doe III*), 549 F.3d 861 (2d Cir. 2008).

69 *See infra* Part II.B.3.

70 United States v. Warshak, 490 F.3d 455 (6th Cir. 2007) (Warshak I), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). In *Warshak I*, the Defendant was suspected of mail fraud, wire fraud, money laundering, and other related federal offenses. *Id*. at 460.

71 *Id.* The e-mail content requested also included e-mails which had been deleted from storage for fewer than 181 days. *Id.* The government also requested copies of all log files and backup tapes which were not pertinent to the point discussed at that time. *Id.* Requesting e-mails that are more than 180 days old requires a lesser burden by the government than e-mails which are equal to or fewer than 180 days old. *See infra* note 126 and accompanying text (discussing e-mail storage time frame provisions under Section 2703).

notifying Warshak that the government had access to his records.[72] However, more than one year after the order was granted, Plaintiff Warshak still did not have notice of his e-mail seizure.[73] Government officials finally informed Warshak about the prior seizure one day after the order was unsealed.[74] The Court of Appeals for the Sixth Circuit then granted Warshak an injunction that barred the government from seeking additional e-mails without providing notice to Warshak.[75] Months later, the court vacated the injunction and scheduled an en banc hearing to determine whether government agents had acted in good faith when they requested the e-mails.[76] Because the government had

---

72 *Warshak I*, 490 F.3d at 460, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). This ninety-day seal is permitted under 18 U.S.C. § 2703(b)(1)(B). *Id.*

73 *Id.* In *Warshak I*, the government admitted it had violated section 2703, and it did not seek statutorily provided extensions for renewal of seal. *Id.* at 461 n.1.

74 *Id.* at 460–61.

75 *Id.* at 462.

76 Warshak v. United States, No. 06-4092, 2007 U.S.App. LEXIS 23741, 1 (6th Cir. Oct. 9, 2007) (en banc), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). Subsequently, in December 2007, the district court allowed the presentation of the Nuvox e-mails as evidence. United States v. Warshak, 2007 WL 4410237, *5 (S.D. OH Dec. 13, 2007) (Warshak II), *modified by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). As a result of Defendant's Omnibus Pretrial Motion in *Warshak II*, the court acknowledged that the government had the e-mails in its possession before the delayed notice provision expired. *Id.* During this hearing the court did not rule on the constitutionality of the SCA, and instead relied on the fact that the government held the questionable e-mails at the proper time. *Id.* In July 2008, the court, sitting en banc, ruled on *Warshak* for a third time. *Warshak v. United States (Warshak III)*, 532 F.3d 521 (6th Cir. 2008). The Sixth Circuit Court of Appeals vacated the injunction prohibiting future ex parte searches on the legal grounds that the issue was not ripe for adjudication. *Id.* at 526. The judges split on the issue 9-5 with Judge Martin Jr., who had ruled on the initial injunction in *Warshak I*, penning a stinging dissent. *Id.* at 534. Judge Martin Jr. accused the majority of sidestepping the issue instead of reaching the question of whether the delayed notice provision of the SCA is unconstitutional. *Id.* at 535 (Martin, J., dissenting). The dissent further states, "Despite the fact that a violation of one of the bedrock principles of the Bill of Rights has been alleged, today the majority has decided to treat the government more favorably than a private litigant would be treated in a similar preliminary injunction setting." *Id.* at 537. The dissent accuses the majority of not only tilting the law in favor of the government, but also disregarding mandatory precedent in the Sixth Circuit. *Id.* at 535. Finally, the dissent ends its discussion by chastising the government's investigatory strength:

> If it is free speech, freedom of religion, or the right to bear arms, we are quick to strike down laws that curtail those freedoms. But if we are discussing the Fourth Amendment's right to be free from unreasonable searches and seizures, *heaven forbid that we should intrude on the government's investigatory province and actually require it to abide by the mandates of the Bill of Rights*. I can only imagine what our founding fathers would think of this decision. If I were to tell James Otis and

obtained the challenged e-mails before the delayed notice expired, the court in *Warshak II* found that whether the SCA was constitutional remained unanswered because the judgment in *Warshak I* had been vacated.[77] *Warshak I* and *II* show the difficulties that one district court has had in deciding issues involving the SCA.

In addition, the court in *Warshak I* relied on *United States v. Miller* to explain that the "reasonable relevance" standard was appropriate.[78] Pursuant to this standard, government intrusion is less likely, and furthermore, if a party demonstrates that a legitimate expectation of privacy attaches to the seized records, the party has standing to dispute the subpoena on Fourth Amendment grounds.[79]

Ultimately, the court in *Warshak II* held that e-mail account holders have a reasonable expectation of privacy.[80] Privacy can be waived, but if it is not, e-mails are private and protected from government intrusion unless proper channels are used to demand access to them.[81] The court noted that the safeguards in place operate in the government's favor, namely the requirements of obtaining a warrant and notifying the

---

> John Adams that a citizen's private correspondence is now potentially subject to *ex parte* and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless.

Id. at 538 (first emphasis added).

77 *See supra* note 76 and accompanying text (discussing that the *Warshak II* court's vacation of the injunction against the e-mails was only due to the time issue). *See also Warshak II*, 2007 WL 4410237 at *5, *modified by* 532 F.3d 521 (6th Cir. 2008) (Warshak III) (noting that the defendant's reliance on *Warshak I* seems a bit misplaced due to the Sixth Circuit vacating *Warshak I*'s judgment in *Warshak II* when the fate of 2703(d) was in limbo). *See infra* Part III.C.3 (for a discussion of the delayed notice provision).

78 *Warshak I*, 490 F.3d at 468–69, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III) (citing Doe v. United States, 253 F.3d 256, 263–264 (6th Cir. 2001); United States v. Miller, 425 U.S. 435, 444 (1976)). The government argued that the court issued orders resembled subpoenas rather than pure searches, and thus, the government did not need to show probable cause. *Id.* at 468. If true, then the "reasonable relevance" standard suffices, and probable cause is not necessary. *Id.*; *see also* United States v. Valdicieso Rodriguez, 532 F. Supp. 2d. 332, 340 (D. Puerto Rico 2007) (supporting the proposition that "probable cause for [a] search warrant . . . need not be tantamount to proof beyond a reasonable doubt; probability is the touchstone[]").

79 *Warshak I*, 490 F.3d at 468–69, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III) (quoting *Doe*, 253 F.3d at 263–64; *Miller*, 425 U.S. at 444 (1976)).

80 *Id.* at 481–82.

81 *Id.* The court recognized the balancing of interests that needs to occur between those interests of the accused, the government, and the public. *Id.* at 481.

account holder that a warrant has been obtained.[82] Such constitutional safeguards protect individual interests and act as a roadblock and prevent the government from depriving of an essential constitutional right—the right to privacy.[83] Last, even if a warrant or subpoena is used to obtain e-mail records from an ISP, not all e-mails will fall within the request because the scope of the request must be narrowly tailored to the issue at hand.[84]

---

[82] *Id.* at 481. The government still has the option to seize e-mails by obtaining a warrant, notifying the account holder, or showing that the account holder has waived his expectation of privacy. *Id.* Furthermore, section 2703(f) of the SCA allows the government to require the ISP to preserve e-mails for evidentiary reasons, and the government may obtain the e-mails from the receiving or sending party. *Id.*; *see also* Lawless, *supra* note 38 (discussing what constitutes third party material in relation to sending and receiving e-mails). Additionally, the court does not rule out that some e-mail account holders may have lesser expectations of privacy due to heavy screening of e-mail. *Warshak I*, 490 F.3d at 478, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). The difference is computer generated screening and frequency:

> [I]t is entirely possible, if not likely, that this process occurs without ever having a human being read the content of subscribers' e-mails. Where total access is the norm, we hold that the government may show as much and then may compel disclosure through the ISP. Less in-depth screening, however, is insufficient to diminish the privacy interest in an e-mail account.

Id.

[83] *Warshak I*, 490 F.3d at 481, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III) (quoting Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973)). The *Warshak I* court further noted that "it is always in the public interest to prevent violation of a party's constitutional rights[.]" *Id.* at 481–82.

[84] *Warshak I*, 490 F.3d at 476 n.8, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). The court claimed the following:

> In neither instance is the government necessarily entitled to every e-mail stored with the ISP, many of which are likely to be entirely unrelated to its specific investigation. If the e-mails are seized pursuant to a warrant, the Fourth Amendment's particularity requirement would necessitate that the scope of the search somehow be designed to target e-mails that could reasonably be believed to have some connection to the alleged crime being investigated.

Id. And similarly, for subpoenas, "where a subpoena or an SCA order compels the disclosure of e-mails, the demand must be reasonable in scope and relevance." *Id.* (quoting *Doe*, 253 F.3d at 263. Both requirements are fact specific. *Id.* (quoting United States v. Logan, 250 F.3d 350, 365 (6th Cir. 2001)). The searches should be narrowed to the "sender, recipient, date, relevant attachments, or keywords[]" and should be applied on a case by case basis. *Id.*

Next, the United States Court of Appeals for the Armed Forces further contributed to section 2703 jurisprudence by finding, in *United States v. Allen*, that individuals hold no expectation of privacy in account information provided to ISPs, but do hold an expectation of privacy in the content of e-mails.[85] The court found no privacy interest in the information that the government had obtained from an Internet Access Provider ("IAP"),[86] Super Zippo, because the information consisted of data the defendant gave to employees, websites the defendant visited and no content from the defendant's e-mail.[87]

The procedural issue in *Allen* resulted because the IAP handed over the defendant's information without first receiving a warrant from the government as required by section 2703.[88] The government's agent had asked Super Zippo whether it required a warrant to obtain the requested information, and the general counsel for the IAP replied in the negative.[89] Therefore, because Super Zippo indicated that it did not require a warrant, the government did not obtain one.[90] The court in *Allen* found that the government acted in good faith in light of the agent's behavior, and noted that there appeared to be no reason why the evidence should not be admitted.[91] Because the IAP did not demand a warrant, no seizure existed; therefore, no constitutional violation occurred.[92] Thus, because the IAP willingly provided the requested

---

85 United States v. Allen, 53 M.J. 402 (C.A.A.F. 2000). In *Allen*, appellant's conviction consisted of anal sodomy, assault, conduct unbecoming of an officer, transporting and receiving child pornography, and soliciting his wife as a prostitute. *Id.* at 403–04. The United States Court of Appeals for the Armed Forces upheld the general court martial. *Id.* at 410. The court distinguishes itself from *Maxwell*, which prohibited access to contents of e-mails, by holding that *Allen* does not concern itself with communication at all and instead concerns itself with stored transactions that are recorded in a log format without accompanying text. *Id.* at 409.

86 *See supra* Part II.A (discussing the synonymy of IAPs and ISPs).

87 *Allen*, 53 M.J. at 409. Super Zippo, defendant's IAP, handed over a log to the government that "identif[ied] the date, time, user, and detailed internet [sic] address of sites accessed by appellant over several months." *Id.* at 409. The court reasoned that this information was covered by Title II of the ECPA because the list of websites did not constitute protected content as required under § 2703(c)(1)(A) in order to be protected. *Id.*

88 18 U.S.C. § 2703(c) (2006). Section 2703(c) regulates access to subscriber information. *Id.* In addition to a warrant, the government may obtain subscriber information by obtaining a court order, consent of the subscriber, or formal written request from a law enforcement agency concerning fraudulent allegations. *Id.*

89 *Allen*, 53 M.J. at 409.

90 *Id.*

91 *Id.* The court in *Allen* determined that if a warrant had been issued, the evidence would be admissible and, therefore, should be admitted because the government agent relied in good faith on the representation of Super Zippo's legal counsel. *Id.*

92 *Id.* at 409–10. Justice Sullivan in his concurrence noted that "the Electronic Communication Privacy Act does not require suppression for failure to comply with its

information, the court dismissed the section 2703 challenge in *Allen*, and the constitutionality question was once again avoided.[93]

4. False Notions of E-Mail Privacy

Applying this historical jurisprudence today, most courts, as in the cases discussed above, have held that most private-party e-mail

---

provisions, absent a violation of a constitutional right." *Id.* (Sullivan, J. concurring). *See* United States v. Ferguson, 508 F. Supp. 2d 7 (D.D.C. 2007). Additionally, a recent case from the D.C. District Court recognized § 2703 of the SCA as unconstitutional for its lack of an exclusionary provision. *Id.* In *Ferguson*, the Drug Enforcement Administration ("DEA") suspected that the defendant was involved in drug trafficking, and it launched an investigation. *Id.* at 8. The government submitted, and the magistrate approved, two ex parte applications that compelled MSN and Yahoo! to hand over to government officials the e-mails of the defendant that were more than 180 days old. *Id.* The defendant requested to suppress the evidence and alleged that the SCA was unconstitutional because it lacked a suppression remedy. *Id.* This judicial opinion is less than two pages long and is not clear in its reasoning, but suggests that *Warshak I* previously declared the SCA to be unconstitutional. *See id. See also Warshak I*, 490 F.3d 455, 476–77 (6th Cir. 2007), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). This interpretation is mistaken because *Warshak I* upheld the SCA and narrowly construed the injunction granted to exclude possible unconstitutional provisions regarding a facial challenge that had nothing to do with the lack of an exclusionary remedy. *See id*. *See also Ferguson*, 508 F. Supp. 2d at 9. In *Ferguson*, the court found that the government reasonably relied on the SCA because Acts of Congress are "entitled to a strong presumption of constitutionality[]" and because until 2006 in *Warshak I*, no court had ruled the SCA unconstitutional since its enactment in 1986. *Id.* Therefore, in 2003, when the government applied for SCA orders in this case, there was no indication that the statute was unconstitutional. *Id. B*ecause the government complied with SCA's standards, the court allowed the evidence. *Id*. Furthermore, the court held that "the Government's reliance on the SCA was objectively reasonable. Thus, the Court need not consider the constitutionality of the SCA." *Id.* Oddly enough, two short paragraphs later, the court cited *Smith*, one lonely case that stated that "'the Stored Communications Act does *not* provide an exclusion remedy. It allows for civil damages . . . and criminal punishment . . . but nothing more.'" *Id*. at 10 (quoting United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998)) (alteration in original). Thus, the question remains as to whether the lack of an exclusion remedy renders the entire SCA unconstitutional. *See id*.

[93] *Allen*, 53 M.J. at 409. In *Allen*, the court noted that suppression is not a remedy under the SCA, but that courts need to determine whether the accused (the individual whose account holder information was seized) had a reasonable expectation of privacy. *Id.* Also, the SCA "does not require suppression for failure to comply with its provisions, absent a violation of a constitutional right." *Id.* at 410 (Sullivan, J. concurring). This reasoning leads one to believe that courts recognize that suppression is guaranteed under the Fourth Amendment but not under the SCA unless there is a reasonable expectation of privacy. *See also* United States v. Maxwell, 45 M.J. 406, 422–23 (C.A.A.F. 1996) (barring electronic evidence that was illegally obtained and classified as fruit from the poisonous tree); Lawless, *supra* note 38, at 1 (stating that "[a]gainst the backdrop of this increased use of Internet search records used as criminal evidence, there is a corresponding void in privacy law: there is no applicable statutory suppression remedy[]").

correspondence is private, and thus constitutionally protected, because the user expects the content to be private.[94] Furthermore, e-mail is one of the most popular mediums for communication, similar to telephones and letters in the past.[95] ISPs house today's virtual mailboxes.[96] Even if an

---

[94] *Warshak I*, 490 F.3d at 473, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

[95] *Id.* The court analogized the constitutional protections given to telephone conversation content in *Katz* and found that those same protections should apply to e-mail. *Id.* In addition, the Senate Report acknowledged that computers are becoming the exclusive medium for communication and record keeping:

> The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. These services as well as the providers of electronic mail create electronic copies of private correspondence for later reference. This information is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity. For the person or business whose records are involved, the privacy or proprietary interest in that information should not change.

S. REP. NO. 99-541, at 3 (1986). The Report further acknowledged that the law prior to the ECPA would likely not protect the above mentioned records and that the purpose of the ECPA was to remedy this situation. *Id. See* Brief of Plaintiff-Appellee at 27, Warshak v. United States, No. 06-4092 (6th Cir. Jan. 11, 2007). Additionally, e-mail is granted the same privacy rights as sealed containers. *Id.* "In recent years, email has become the preferred medium of written communication for millions of Americans, revolutionizing the form in which individuals communicate to each other their thoughts, ideas, beliefs, hopes, dreams, and fears and becoming the backbone of the country's communication system." *Id.* Furthermore, "Emails are 'closed containers' which may not be searched without a warrant." *Id.* at 29. The Plaintiff-Appellee's Brief in *Warshak I* continued by explaining how e-mails are similar to closed containers. *Id.* at 30–31.

[96] Brief of Plaintiff-Appellee at 27, Warshak v. United States, No. 06-4092 (6th Cir. Jan. 11, 2007). In his final brief, Warshak argued as follows:

> Emails stored on an ISP's server are a form of closed container. The contents of an email are not visible to the naked eye; instead, several intrusive searches must occur before the contents may be read. One seeking to view the contents of an ISP-stored email must first gain access to that portion of the ISP's server that houses the subscriber's email; this is a search in and of itself. Even after one gains access to the a [sic] subscriber's virtual mailbox, the content of those emails remain [sic] shielded from public view, much like the content of letters sitting in a "real" mailbox. To view the contents of an email, another physically intrusive act is necessary: the email must be unsealed through the operation of a computer function such as clicking on the email using a mouse or using the computer's "open" function, an act doctrinally indistinguishable from the act of opening a sealed letter or

ISP contracts for a right to access a user's e-mail "in the ordinary course of business," this access does not waive a user's expectation of privacy.[97] Therefore, in light of Fourth Amendment jurisprudence, courts will likely continue to hold that individuals have an expectation of privacy regarding their e-mail.[98] Courts have discussed account holder expectations in more detail with regard to server policies.

5. Reasonable v. Unreasonable Expectations: Marking the Bounds

Two cases decided by the United States Courts of Appeals, regarding the impact of Fourth Amendment expectations of e-mail privacy in view of school or organizational server policies, merit brief

---

> package or unlocking a closed footlocker. [Therefore], ISP-stored emails are entitled to protection of the Fourth Amendment . . . .

Id. at *30–31 (internal citation omitted). *See* Dempsey, *supra* note 26, at 421. Dempsey also used the storage locker analogy: "[w]hen an individual stores personal property with a third party, the owner of the property retains a privacy interest in the stored items, meaning that a warrant would be required to search the storage space." *Id*. *See* Robert M. Goldstein & Martin G. Weinberg, *The Stored Communications Act and Private E-mail Communications*, CHAMPION, Aug. 2007, at 19–20. Finally, Warshak's attorneys authored an article discussing the SCA, and drew an interesting conclusion when comparing sealed containers, letters, and e-mails. *Id*. The authors described an e-mail as having more privacy aspects than a traditional letter because

> the owner of the e-mail can repossess a read-and-then-closed e-mail at any moment, without any notice or permission from the ISP. The owner of the e-mail can delete it from the mailbox, or do whatever he or she wants to do with the e-mail. It is, for all purposes, in that person's possession, dominion, and control at all times. Consequently, if there is any difference, the privacy interests should be greater in the context of e-mail than in the traditional carrier paradigm[] . . . .

Id.

[97] United States v. Miller, 425 U.S. 435, 442 (1976). *See supra* note 29 (discussing the facts of *Miller*). *See also* United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007). *Miller* requires that access to a user's e-mail must occur in the ordinary course of business and where university policies that provide for limited e-mail monitoring do not satisfy the ordinary course of business requirement. *See Miller*, 425 U.S. at 442; Heckenkamp, 482 F.3d at 1147. *See also Warshak I*, 490 F.3d at 473–74, *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III). Essentially, where user contracts for e-mail and ISP policies are in place, unless those contracts and policies allow greater than limited access and the government can prove that regular monitoring occurs, policies will be ineffective in proving that content is scanned by persons in the ordinary course of business. *Id*.

[98] *See* JOHNSON, *supra* note 18 (demonstrating that even lawyers recognize privacy of e-mail correspondence and how it can help in assisting clients). Johnson stated that, for practical purposes, "e-mail should be considered as secure as many other common means of communication, such as phone calls, faxes, the U.S. mail, and express delivery services." *Id*. at xvii.

attention.[99] Exemplifying the two extremes that mark the constitutional bounds for obtaining e-mails, *United States v. Simons* and *United States v. Heckenkamp*, discuss expected privacy interests of server users.[100]

In *Simons*, the Court of Appeals for the Fourth Circuit held that a Foreign Bureau of Information Services ("FBIS") engineer had no reasonable expectation of privacy on a work computer because the agency had a policy that allowed auditing of work computers and had notified the engineer of this policy.[101] The court determined that the policy eliminated the engineer's reasonable expectation of privacy.[102] According to the court, whether Plaintiff Mark Simons believed he was entitled to privacy was not relevant because the FBIS's policy objectively forewarned him that he was not.[103] The *Simons* court was one of the first

---

[99] *See* United States v. Simons, 206 F.3d 392 (4th Cir. 2000); *Heckenkamp*, 482 F.3d 1142.

[100] *Simons*, 206 F.3d 392; *Heckenkamp*, 482 F.3d 1142. *See* 41 AM. JUR. 3D *Proof of Facts*, *supra* note 1, § 13. An e-mail policy "should be clear, concise, and aimed at responsible use of e-mail, in order to gain acceptance throughout the company. The policy should be consistent with other company policies, such as access to and use of company facilities and property." *Id*.

[101] *Simons*, 206 F.3d at 398. The FBIS policy explained that FBIS would conduct electronic audits according to the following guidelines to ensure compliance with its internet usage policy:

> Audits. Electronic auditing shall be implemented within all FBIS unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall . . . be capable of recording:
>
> - Access to the system, including successful and failed login attempts, and logouts;
> - Inbound and outbound file transfers;
> - Terminal connections (telnet) to and from external systems;
> - Sent and received e-mail messages;
> - Web sites visited, including uniform resource locator (URL) of pages retrieved;
> - Date, Time, and user associated with each event.

Id. at 395–96. The policy also informed users that FBIS would periodically "audit, inspect, and/or monitor" user accounts when it deemed proper. *Id.* at 396. Defendant Simons's account fell under suspicion when a network manager noticed a number of hits for the word "sex" originating from Simons's computer. *Id.* Further investigation led FBIS to find that the websites that Simons visited contained nude pictures and that he had saved over one-thousand of such pictures and files on his computer. *Id.*

[102] *Id.* at 398. "We conclude that the remote searches of Simons' computer did not violate his Fourth Amendment rights because, in light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet." *Id.*

[103] *Id.* "[R]egardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use." *Id.* (citing Am. Postal Workers Union v. United States Postal Service, 871 F.2d 556, 560 (6th Cir. 1989)).

to examine employer e-mail privacy policies.[104] In contrast, the Ninth Circuit has ruled that organizational server policies do not negate an individual's reasonable expectation of privacy.[105]

In *Heckenkamp*, the Court of Appeals for the Ninth Circuit held that attaching one's computer to the University of Wisconsin's network did not waive a user's reasonable expectation of privacy.[106] Indeed, *Heckenkamp* illuminated the need for section 2703 of the SCA.[107] In *Heckenkamp*, immediately after the University of Wisconsin determined that a student had misused the computer she had attached to the school's network, school officials disconnected the student's computer from the network and confiscated it without a warrant.[108] The *Heckenkamp* court distinguished the facts in *Heckenkamp* from those in *Simons* because, in *Heckenkamp*, the University of Wisconsin did not have an announced screening or monitoring policy in effect, and, in fact, the server policy that was in place led users to believe that their accounts were private.[109] Therefore, as shown by the divergent outcomes in *Simons* and *Heckenkamp*, an organization's internet server policy may not effectively

---

[104] *Id.* at 392. *See* United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007). The other extreme is exhibited in the Ninth Circuit by *Heckenkamp*. *Id.*

[105] *Id.* at 1147. The court held that there is no single factor that establishes that a place is free from warrantless government intrusion. *Id.* at 1146. However, the court noted that people generally have a heightened expectation of privacy on their home computers and in their password protected files. *Id.*

> A person's reasonable expectation of privacy may be diminished in "transmissions over the Internet or e-mail that have [sic] already arrived at the recipient." However, the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer.

Id. at 1146–47 (quoting United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004)) (internal citations omitted).

[106] *Id.* at 1146.

[107] *Id.* In *Heckenkamp*, a University of Wisconsin student hacked into the main computer network and gained access to the university e-mail system. *Id.* at 1143. The student had been fired from the school's computer help desk for "similar unauthorized activity," which in turn justified the administrator's concern that Defendant Heckenkamp had the knowledge to actually cause harm. *Id.* at 1144. Since this happened during the period of final examinations, the university's computer network investigator noted that a disruption to the university would be "tremendous if e-mail was destroyed." *Id.*

[108] *Id.* at 1145.

[109] *Id.* at 1147. The school policy required that

> "[i]n general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to . . . protect the integrity of the University and the rights and property of the state."

Id. (alterations in original). The school's policy in *Heckenkamp*, therefore, actually gave the user a heightened expectation of privacy. *Id.*

eliminate the expectations of privacy that individuals have when accessing an organization's server.[110]

Laws governing electronic communications under the SCA specifically regulate e-mail evidentiary procedures with respect to third party ISPs.[111] This Note addresses the likely occurrence of an unconstitutional search and seizure pursuant to sections 2703, 2704, and 2705 of the SCA.

C. Sections 2703, 2704, and 2705 of the Stored Communications Act[112]

The SCA, which, as mentioned previously is also known as Title II of the ECPA, provides the government power with which it can access customer communication records from third-party service providers.[113] In 1986, Congress enacted the following Titles of the ECPA: Title I applies to "interception of communications and related matters";[114] Title II relates to "stored wire and electronic communications and transactional records access";[115] and Title III discusses "pen registers."[116]

---

[110] *Simons*, 206 F.3d at 398–99; *Heckenkamp*, 482 F.3d at 1147. The Court of Appeals for the Fourth Circuit explained in *Simons* that the FBIS's Internet policy diminished Simons's legitimate expectation of privacy. 206 F.3d at 398–99. Additionally, Simons never asserted that he was unaware of the Internet policy. *Id.* at 399 n.8. Conversely, in *Heckenkamp*, even though a policy existed and stated that certain users may access his account, University policies considered, in their entirety, did not diminish Heckenkamp's legitimate expectation of privacy. 482 F.3d at 1147.

[111] Electronic Communications Privacy Act, 18 U.S.C. §§ 1367, 2521, 2701–12, 3117, 3121–27 (2006).

[112] *See* The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors, APRI, July 2005, at 25, *available at* http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf. Two threshold questions when evaluating anything under the ECPA are as follows: one, "Does the provider offer e-mail services to the public?"; and two, "Is the law enforcement agency seeking e-mail content?" *Id.*

[113] *Id.* at 9. The ECPA does not define governmental entities and neither have courts. *Id.*

[114] H.R. 4952, 99th Cong. § 1 (1986). The purpose of the ECPA was to

> amend[] title III of the Omnibus Crime Control and Safe Streets Act of 1968—the Federal wiretap law—to protect against the unauthorized interception of electronic communications. The bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.

S. REP. NO. 99-541, at 1 (1986). *See also* THE CENTER FOR DEMOCRACY AND TECHNOLOGY, CURRENT LEGAL STANDARDS FOR ACCESS TO PAPERS, RECORDS, AND COMMUNICATIONS: WHAT INFORMATION CAN THE GOVERNMENT GET ABOUT YOU, AND HOW CAN THEY GET IT? (2006), http://www.cdt.org/privacy/govaccess/govaccesschart.pdf; http://www.cdt.org/wiretap/govaccess/govaccesschart-11x17.pdf (presenting more information about current legal standards, regarding access to papers, records, and communications, and presenting two charts mapping accessibility of documents, burdens, and levels of privacy protection).

[115] H.R. 4952.

This Note specifically addresses Title II, which attempts to balance the privacy interests of both citizens and law enforcement agencies.[117] The purpose of the SCA was to update existing wiretapping law to account for new forms of communications, such as e-mail.[118] Two sections of the SCA were recently subjects of litigation in district courts because of the provisions that address lack of notice and delayed notice when gathering the contents of e-mails.[119] Parts II.C.1–2 discuss these sections of the SCA.[120]

1. Section 2703: Required Disclosure of Customer Communications or Records[121]

Section 2703 of the SCA governs disclosure of customer communications and records.[122] Section 2703 provides that the government may obtain general account holder information[123] via

---

116 *Id.*

117 S. REP. NO. 99-541, at 1. *See* Robert S. Steere, *Keeping "Private E-mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 264–74 (1998) (Titles I and II of the ECPA should be clarified because of the very fine distinctions between stored communications and transit communications). *See also Pikowsky*, *supra* note 11. Another proposed solution arguing for clarification has been to address all communications—telephone, postal mail, e-mail—in one statute, and therefore provide consistency and incorporate emerging technologies at the same time. *Id.* (stating that "the statutes should be amended to provide the same protection against surreptitious access to stored communications, regardless of whether that communication is stored in a person's mailbox at an Internet Service Provider, in a personal computer located in a house, or in a file cabinet in an office[]").

118 132 CONG. REC. 4039 (1986).

119 *See* Warshak v. United States (Warshak I), 490 F.3d 455 (6th Cir. 2007), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III); United States v. Ferguson, 508 F. Supp. 2d 7 (D.D.C. 2007).

120 *See infra* Parts II.C.1–3 (discussing the sections of the SCA governing disclosure of e-mail by third party service providers, backup preservation, and delayed notice to account holders).

121 18 U.S.C. § 2703 (2006).

122 *Id.* (noting that section 2703 of the SCA is titled, "Required disclosure of customer communications or records").

123 *Id.* § 2703(c)(2). Such general account information held by remote electronic computing services that must be disclosed to a governmental entity includes

> (A) name;
> (B) address;
> (C) local and long distance telephone connection records, or records of session times and durations;
> (D) length of service (including start date) and types of service utilized;
> (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

warrant, court order, consent of the subscriber or customer, submission of a formal request by the governmental entity investigating, or administrative subpoena.[124] Furthermore, the government may obtain the actual content of e-mail communication with or without providing notice to the subscriber.[125] Section 2703 distinguishes between e-mails that are more than 180 days old and those that are equal to and less than 180 days old, the latter being harder to obtain.[126] The governmental

---

> (F) means and source of payment for such service (including any credit card or bank account number)[.]

Id.

[124] *Id.* § 2703(c)(1). The SCA specifically states that information may be obtained when the governmental entity

> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
> (B) obtains a court order for such disclosure under subsection (d) of this section;
> (C) has the consent of the subscriber or customer to such disclosure;
> (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
> (E) seeks information under paragraph (2).

Id. § 2703(c)(1). The information may be obtained under § 2703(c)(2) "of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena . . . ." *Id.* § 2703(c)(2). *See* H.R. 3156, 110th Cong. (2007); *infra* note 146. A bill is currently before Congress that will allow the governmental entity to obtain information while investigating the disappearance of a subscriber when the subscriber is either a minor, or if there is likely to be suffering and a guardian, spouse, or parent has consented. H.R. 3156, 110th Cong. (2007); *infra* note 146 (text of proposed bill).

[125] 18 U.S.C. § 2703(b).

[126] *Id.* § 2703(a)–(b). The statute reads:

> (a) Contents of Wire of Electronic Communications in Electronic Storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or 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 using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or 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.
> (b) Contents of Wire or Electronic Communications in a Remote Computing Service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

entity seeking the information may obtain the contents of wire or electronic communication without notice if it obtains a warrant.[127] Furthermore, the government may obtain information with prior notice by an administrative subpoena or court order.[128] Legal theorists and courts have questioned the constitutionality of administrative subpoenas and court orders, claiming that they do not satisfy the probable cause standard required by the Fourth Amendment.[129] Administrative subpoenas require only a reasonable relevance standard, whereas actual warrants require a showing of probable cause under the Fourth Amendment.[130] Although legal theorists and courts have exhausted this issue, this Note narrows its focus to the unconstitutional disparity of existing safeguards for e-mail privacy and the likelihood that Fourth Amendment violations will occur.[131]

> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
> (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

Id. It has been suggested that it "makes no sense" to distinguish between e-mails greater or less than 180 days old because all e-mails should be treated the same. Final Brief of Plaintiff-Appellee at 42 n.18, Warshak v. United States, No. 06-4092 (6th Cir. Jan. 11, 2007); *see also infra* notes 208–13 and accompanying text. Furthermore, Plaintiff Warshak argued:

> A year-old email is no less worthy of Fourth Amendment protection than is a day-old one, and permitting the seizure of a 181-day old email via §2703 orders or subpoenas but requiring a warrant based on probable cause for a 179-day old one is a distinction without constitutional foundation or principle.

Brief of Plaintiff-Appellee at 42 n.18, Warshak v. United States, No. 06-4092 (6th Cir. Jan. 11, 2007).

127 18 U.S.C. § 2703(a). *See* also FED. R. CRIM. P. 41. The warrant must be issued pursuant to Federal Rule of Criminal Procedure "by a court with jurisdiction over the offense under investigation or equivalent State warrant." 18 U.S.C. § 2703(a).

128 *See* 18 U.S.C. § 2703(b); *supra* note 126.

129 *See* Steinberg, *supra* note 9, at 478 (noting that court orders require "far less rigorous proof than the probable cause standard for a Fourth Amendment warrant[]"). *See also* U.S. CONST. amend. IV.

130 Doe v. United States, 253 F.3d 256, 263–64 (6th Cir. 2001); *see also supra* note 78 (discussing the reasonable relevance test).

131 *See* Warshak v. United States (Warshak I), 490 F.3d 455, 468 (6th Cir. 2007), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007),

2. Section 2704: Backup Preservation[132]

The SCA provides the government with a security blanket in section 2704 by requiring ISPs to backup user accounts when the government makes such a request.[133] This provides the government with an excellent opportunity to secure evidence because backup preservation pursuant to section 2703(b)(2) does not require the government to provide the user with immediate notice.[134] Therefore, the government may, without notifying the account holder, have the ISP backup the account until the

---

modified by 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III) (noting that the government typically argues that court orders issued under section 2703 of the SCA are akin to subpoenas, which require only a showing of reasonable relevance). *See also Doe*, 253 F.3d at 263–64. The reasonableness standard is applied to subpoenas, whereas actual warrants require a showing of probable cause under the Fourth Amendment. *Id*. A warrant can be distinguished from a subpoena by the level of intrusiveness of the seizure. *Id.* at 264. Whereas a warrant is classified to have immediate intrusiveness, an order or administrative subpoena may be contested in federal court through a motion to suppress, thereby being less intrusive. *Id. See also* Paul K. Ohm, *Parallel-Effect Statutes and E-mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1610–11 (2004). Ohm contended that there is a growing chasm between privacy and freedom. *Id.* at 1599. Furthermore, he predicted that lowering the standards the government has to meet to obtain a SCA warrant may simultaneously lower the standards for obtaining physical search warrants as well. *Id.* at 1613. Evidence suggests that Ohm's prediction is true in situations where warrants may be served via fax to the ISP, and then the ISP performs the search without supervision of a police officer. *Id.* at 1610–11. Ohm stated that these warrants granting unsupervised searches are not search warrants at all, and the problem arises where the accused does not even know that his inbox has been searched. *Id. See* 18 U.S.C. § 2704(a)(1). All the government needs to do is contact the ISP with the account information that it wants backed up and the ISP must comply with the government's request within two business days. *Id*. *See id*. § 2704(a)(4). Then, fourteen days after notice to the subscriber, the government may obtain access to the backed up copy if the subscriber has neither objected nor initiated proceedings against the government. *Id*. § 2704(a)(5). To satisfy its burden to justify e-mail back-up, the government must only demonstrate that it has a reason to believe that notification to the subscriber will result in destruction of e-mails; if it shows this, the backup preservation shall be authorized. *Id*. *See id*. § 2704(b)(1)–(5). The SCA grants proper remedies to subscribers in cases where subscribers may file a motion to vacate or quash subpoena. *Id*. Section 2704(b) of the SCA explicitly establishes procedures for challenging a backup and provides instructions for judges concerning when to grant and deny such motions. *Id*.

132 18 U.S.C. § 2704.

133 *Id.* "A governmental entity . . . may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications." *Id*. § 2704(a)(1).

134 *Id*. § 2704. "Without notifying the subscriber or customer . . . such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made." *Id*. § 2704(a)(1).

government can meet its burden to show cause for obtaining the contents.[135] Notice is provided to the account holder at the government's discretion because the delayed notice provision of section 2705 applies to backup preservation.[136] This Note examines delayed notice, one of the open-ended provisions of the SCA that can easily violate Fourth Amendment guarantees of privacy.[137]

3. Section 2705: Delayed Notice

Rules almost always come with exceptions, and section 2703 is not unique in this respect. Specifically, section 2703 states that when the government requests an account holder's information from an ISP, the government must notify the account holder of the request, but section 2703 also stipulates that this notice may be delayed for e-mail content gained by an administrative subpoena or court order.[138] This problematic exception is defined in section 2705, which provides that the government may elect to delay notification to the account holder for up to ninety days.[139] Furthermore, this delayed notice of ninety days may be continuously extended in ninety day increments if the government

---

135 *Id.*

136 *Id.* § 2704(a)(2). The government has three days to notify the subscriber after backup is confirmed by the ISP under section 2704. *Id.* However, the government can choose to use the delayed notice provision and then notice can be technically delayed for extended amounts of time. *Id.* § 2705. *See infra* note 140 (citing to the SCA provision extending delayed notice length—section 2705(a)).

137 *See infra* Part III.C.3.

138 *See supra* note 126 and accompanying text; *see also* 18 U.S.C. § 2703(b) (2006).

139 *See supra* note 126 (citing the text of 18 U.S.C. § 2703(b)). *See* 18 U.S.C. § 2705(a). Section 2703 provides as follows:

> (1) A governmental entity acting under section 2703(b) of this title may—
>
> (A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or
>
> (B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

Id.

submits the proper request for the court to grant such exception.[140] Therefore, theoretically, if continuous extensions are granted, the government may lawfully obtain the content of an individual's e-mail without any notification to that individual for an unlimited amount of time.[141] The drafters of section 2705 of the SCA claim that the only time this scenario could possibly take place is when an "adverse effect" is likely.[142] Consequently, this delay provision leaves open the possibility that individuals do not have the opportunity to refute seizures that may be unlawful before Fourth Amendment violations occur.[143] Congress has

---

[140] 18 U.S.C. § 2705(a)(4). This delayed notice exception specifically provides that "[e]xtensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section." *Id. See id*. 2705(a)(5). Upon expiration of the extension, the government must inform the subscriber of specific investigation details. *Id*. Section 2705(a)(5) specifically states:

> Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—
>
> (A) states with reasonable specificity the nature of the law enforcement inquiry; and
>
> (B) informs such customer or subscriber—
>
> (i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
>
> (ii) that notification of such customer or subscriber was delayed;
>
> (iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and
>
> (iv) which provision of this chapter allowed such delay.

Id.

[141] *Id*. § 2705(a)(4) (granting continuous extensions).

[142] *Id*. § 2705(a)(2). The SCA defines adverse effect as "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial." *Id*.

[143] Brief of Plaintiff-Appellee at 44, Warshak v. United States, No. 06-4092 (6th Cir. Jan. 11, 2007). *See infra* text accompanying note 172 (acknowledging the problem with delayed notice). Warshak's brief discussed

> [T]he unconstitutional synergy of §§2703(b)(1)(B)(ii), 2703(d), and 2705, which, in conjunction, allow the government to secretly seize and search the entirety of an individuals' private email correspondence and to affirmatively *prevent* the individual from learning of the intrusion at a point at which he could lodge a judicial challenge in advance of the seizure. In the administrative/grand jury subpoena context, while notice to the target of the subpoena may not be required by the Fourth Amendment, the fact remains that, where, as is often the case, the

proposed an amendment to the SCA; however, the proposed amendment attempts to "clarify [only] ongoing scope[s] . . . and warrants," but fails to address delayed notice or the lack of supervised seizures.[144]

4. Congress's Proposed Amendment

On July 24, 2007, just over one month after the Court of Appeals for the Sixth Circuit decided *Warshak I*, Congress proposed a bill intended to revamp section 2703 of the SCA.[145] Essentially, the important proposed changes include further defining the circumstances in which a governmental entity may require an ISP to divulge account information and clarifying the appropriate circumstances that lend themselves to requirements for a warrant and court order.[146] As discussed previously,

---

> target learns of the subpoena, he has the ability to move to quash it. In the §2703 context, however, notice to the account holder is *prohibited*, thus affirmatively denying him any chance to protect his rights in advance of disclosure.

Brief of Plaintiff-Appellee at 44.

144 H.R. 3156, 110th Cong. (2007).

145 *Id.* The bill proposed by Congress to amend the SCA is currently before the House subcommittee on Crime, Terrorism, and Homeland Security. *Id. See* Warshak v. United States (Warshak I), 490 F.3d 455, 462 (6th Cir. 2007), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III) (granting Plaintiff injunction barring government from seeking any further e-mails without notice to Plaintiff).

146 H.R. 3156, 110th Cong. (2007). The proposed bill reads:

> '(h)(1) In General- A court order under subsection (d) or a warrant under subsection (c)(1)(A) may require that records or other information (not including the contents of communications) be disclosed to a governmental entity on an ongoing basis.
>
> '(2) Standard- The court shall issue an order or warrant requiring such ongoing disclosure if--
>
> '(A) in the case of a court order under subsection (d), the court finds that the application contains specific and articulable facts showing that there are reasonable grounds to believe that the records or other information (not including the contents of communications) will be relevant and material to an ongoing criminal investigation; or
>
> '(B) in the case of a warrant under subsection (c)(1)(A), the court finds that probable cause supports issuing the warrant.
>
> '(3) Duration- An order or warrant requiring ongoing disclosure under this subsection may require ongoing disclosure for a period not to exceed 60 days. Extensions of such an order or warrant may be granted, but only upon an application for an extension under this subsection and upon the judicial finding required by paragraph (2). The period of extension shall be for a period not to exceed 60 days.

'(4) Nondisclosure- An order or warrant requiring ongoing disclosure under this subsection shall direct that--

'(A) the order or warrant be sealed until otherwise ordered by the court; and

'(B) the person or entity who is obligated by the order or warrant to disclose records or other information on an ongoing basis to the applicant shall not disclose the existence of the order or warrant or the existence of the investigation to any other person, unless or until otherwise ordered by the court.

'(5) Scope and Assistance-

'(A) IN GENERAL- An order or warrant requiring ongoing disclosure under this subsection, upon service of that order or warrant, shall apply to any person or entity providing wire or electronic communication service or remote computing service in the United States whose assistance may facilitate the execution of the order or warrant. Whenever such an order or warrant is served on any person or entity not specifically named in the order or warrant, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order or warrant shall provide written or electronic certification that the order or warrant applies to the person or entity being served.

'(B) INFORMATION PROVIDED- Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of an order or warrant requiring ongoing disclosure under this subsection, a provider of a wire or electronic communication service or a provider of remote computing services shall furnish such investigative or law enforcement officer all information, facilities, technical, and other assistance including execution of such warrant or order unobtrusively and with no more interference with the services that the person so ordered by the court accords the party with respect to whom the warrant or order pertains than is necessary to effect the disclosure required under the warrant or order, if such installation and assistance is directed by a court. Unless otherwise ordered by the court, records or other information disclosed under such warrant or order shall be furnished to the officer of a law enforcement agency designated in the court order, at reasonable intervals during regular business hours for the duration of the order. Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

'(6) Nonexclusivity- Nothing in this subsection shall preclude a governmental entity from requiring or receiving the production on an ongoing basis of records or other information (not including the contents of communications) with consent of the subscriber or user, or under any other lawful authority.'

courts have addressed the warrant/court order issue relating to whether the probable cause standard is met under the Fourth Amendment over and over, and Congress's proposed amendment could cure this problem.

Courts have not yet decided whether sections 2703 and 2705 of the SCA are unconstitutional in view of their provisions for renewed delayed notice and lessened evidentiary burdens compounded by section 2704's backup requirement. Keeping this in mind, Part III analyzes current safeguards in place for disclosure and backup as described in sections 2703 and 2704 to protect both the government and the subscribers, and Part IV suggests the proper approach for tailoring both these safeguards and section 2705 to achieve an outcome that complies with the Fourth Amendment.

III. ANALYSIS OF STORED COMMUNICATIONS ACT AS APPLIED TO GOVERNMENT REQUESTS FOR E-MAIL

The question is not what the statute *authorizes, but what the* Constitution *requires*.[147]

The United States Constitution requires lawmakers to pass statutes that fall within legitimate, constitutional parameters. The transition of stored data from home computers and filing cabinets to Internet databases, including ISPs, should not mitigate individuals' Fourth Amendment rights.[148] As one scholar pointed out,

> Over 200 years ago, the founders of our country took strong steps to permanently and finally end the authority of the government to conduct wholesale surveillance [on] the private communications and thoughts [of] ordinary Americans. The question for us today is whether we're going to give up on that

. . . .

H.R. 3156, 110th Cong. (2007) (setting forth proposed amendments to 18 U.S.C. § 2703).

147 Brief of Plaintiff-Appellee at 41, Warshak v. United States, No. 06-4092 (6th Cir. Jan. 11, 2007).

148 Jonathan Zittrain, *Search and Seizures in a Networked World*, 119 HARV. L. REV. FORUM 83, 90 (2005) (discussing the current trend to store data with "faraway third parties" and noting that this "should not entail a complete stripping of Fourth Amendment interests in having that data secure from unreasonable government intrusion[]").

> American ideal, or whether we're going to take the steps necessary to return to it.[149]

The decisions of *Katz* and *Smith* provide the foundation for evaluating electronic communications.[150] Because e-mail evidentiary issues are analogous to telephone calls and e-mails likely retain an even higher expectation of privacy than telephone communications because e-mails are more similar to written letters, heightened privacy protections guaranteed by the Fourth Amendment should apply to e-mails.[151]

Part III.A analyzes the constitutional problems presented by sections 2703, 2704, and 2705 by focusing on the overwhelming power granted to the government and the comparatively minimal protection against privacy invasion provided to e-mail account holders.[152] Next, Part III.B examines the current jurisprudential trend to veer away from interpreting the SCA, focusing on decisions by United States district courts that have interpreted the SCA in the context of e-mail seizure problems.[153] The fundamental question presented, then, is whether the SCA, including Congress's proposed amendment to the SCA, provides so much power to the government that individual account holders' Fourth Amendment rights to privacy are violated.

A. A Perfect Storm: Fourth Amendment Violations Presented by Sections 2703 and 2705

The expectation of privacy that individuals believe they have when typing an e-mail and saving it as a draft or sending it to a recipient may be easily violated, considering the overwhelming number of provisions in the SCA that allows the government to override an individual's right to privacy in e-mails.[154] E-mail has become the preferred medium of

---

149 *See Snyder*, *supra* note 10 ("[A]side from the technology, the government's ongoing violation of fundamental civil liberties would have been very familiar to the men who gathered in 1791 to adopt the Bill of Rights.").

150 *See supra* Part II.B.1 (discussing *Katz* and *Smith* and the initial reaction by the Supreme Court in respect to seizing electronic communications).

151 *See supra* Part II.B; *see also supra* note 35 and accompanying text (discussing the two questions presented in *Smith* for determining whether a reasonable expectation of privacy exists).

152 *See infra* Part III.A (analyzing the problematic interaction of the above mentioned SCA provisions).

153 *See infra* Part III.B (analyzing problems faced by the judiciary due to the confusing application of the SCA).

154 *See supra* Part II.C.; *c.f.* Steinberg, *supra* note 9, at 475. Steinberg notes that the battle line is drawn where some theorists favor judicial decisions over statutory regulations in regard to "sense-enhanced searches." *Id.* Steinberg further states that "[s]cholars favoring regulation through the Fourth Amendment emphasize the accessibility of Fourth

communication in today's world.[155] The first problem arises because section 2703 allows the government to obtain an account holder's account information without providing notice to the account holder.[156] The next issue arises because of the variety of methods that exist for obtaining e-mail contents without providing notice to account holders and delaying notice for lengthy periods of time.[157] ISP employees certainly have the potential to rummage through the private e-mail of individual account holders.[158] Last, the backup preservation option available to the government under section 2704 should be enough to permit the government to secure any desired evidence without using more intrusive options.[159] All of these conditions combined create great potential for Fourth Amendment violations.

The backup provision under the SCA is one of the government's greatest powers in providing insurance against evidence destruction.[160] As if this is not enough, the government also has the power to delay notice to account holders under the backup provision.[161] Therefore, even though a backup file of electronic evidence is created, if the government believes that notice to the subscriber could still result in the destruction of this evidence, it may extend the delay of notice for ninety day increments.[162] The original period of delayed notice appropriately gives the government ninety days to sort out its case, but a constitutional problem results when the renewals of the ninety day delays are granted.[163] In addition, problems have resulted where the government failed to renew its request for delayed notice, leading to periods as long

---

Amendment doctrine and the complexity of statutes. Scholars favoring regulation by statutes emphasize the specificity of statutory law and the vagueness of Fourth Amendment standards." *Id.*

155 *See supra* notes 95–96 and accompanying text (discussing how e-mail contains the same privacy expectations as letters and closed containers).

156 *See supra* notes 123–24 and accompanying text (discussing procedures the government must follow when obtaining account holder information).

157 *See supra* Part II.C.3 (discussing the delayed notice provision).

158 *See infra* notes 176–81 and accompanying text (analyzing the potential for privacy breaches during searches).

159 *See supra* note 132. *See infra* note 197 and accompanying text. As an additional evidential safeguard, the emerging hard disk recovery technology is also available. *Id.*

160 *See supra* Part II.C.2 (discussing statutory requirements that the government must meet before requesting to backup a user's e-mail).

161 18 U.S.C. § 2704(a)(2) (2006).

162 *See* Swartz & Johnson, *supra* note 20. The reasoning for this extension stems from the varying lengths of e-mail preservation by ISPs themselves. *Id. See supra* note 136 (discussing the applicability of the delayed notice provision to the backup provision).

163 *See supra* Part II.3 (discussing the delayed notice provision of section 2703 of the SCA).

as twelve months without governmental notification to the user regarding the seizure.[164]

Section 2705 addresses renewals for delay of notice.[165] The problematic aspect of delayed notice is that it applies to the most intrusive part of the SCA—government requests to obtain contents of e-mail as provided by section 2703.[166] Traditionally, governmental entities have provided notice of searches involving paper documents contemporaneously and not retroactively, and e-mail should be treated similarly due to its increasing role in displacing paper documents.[167] At first blush, the delayed notice provision seems to provide for only a ninety day extension.[168] However, closer observation reveals that the government may be granted extensions of up to ninety days in accordance with section 2705.[169] More specifically, the subsection of section 2705 that addresses preclusion of notice—the provision that allows the government to forego notifying account holders that it has seized the account holder's records—gives the government an opportunity to petition the court for a period of time that is "deemed appropriate" to refrain from notifying the account subscriber that the government is reading the subscriber's e-mail.[170] Theoretically, this could be for an infinite period of time.

Upon expiration of the delayed notice period, the government must inform the subscriber of the nature of government contact with the ISP, including information about the delayed notification and details of the court ordered delay.[171] The problem with delayed and precluded notice is that by the time the subscriber finds out about the seizure, it is too late

---

164 Warshak v. United States (Warshak I), 490 F.3d 455, 460–61 (6th Cir. 2007), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III).

165 *See supra* Part II.C.3 (discussing provisions of section 2705 of the SCA).

166 *See* Pikowsky, *supra* note 11, at 27–28 (discussing the problems with retrospective notice issues). Pikowsky confirmed that retrospective searches are less invasive than prospective searches. *Id.*

167 *Id.* at 29. Pikowsky observed:

> [W]here the police secretly copy files from a person's mailbox at his ISP or covertly break into a person's office to copy files from his personal computer, the privacy interest at stake is as great as a person's privacy interest in his telephone calls. Therefore, the protections of that privacy interest should be the same.

Id.

168 18 U.S.C. § 2705(a)(A) (2006).

169 *Id.* §§ 2705(a)(4), 2705(b).

170 *Id.* § 2705(b).

171 *See supra* note 140 (discussing procedures of notification upon expiration of sealed notice).

for the person to correct violations of his or her privacy.[172] The government can obtain important information from e-mails other than just the content of the message, such as date, time, sender, and receiver information.[173] This could result in additional leads and information that may be allowed as evidence which would never have been obtained but for the violation of the privacy interest a user has in his e-mail account.[174] The next problematic provision of the SCA that has the potential of violating an individual's Fourth Amendment rights involves the way that e-mail contents are obtained without official supervision.[175]

It is true that the Fourth Amendment does not require supervision of searches where civilian searches may be more reasonable than searches performed by police officers.[176] In fact, some situations, such as body cavity searches, present an example where privacy is greater outside the presence of an officer.[177] However, some people argue that an e-mail

---

172 *See supra* Part II.C.3 (discussing the SCA's delayed notice provision).

173 41 AM. JUR. 3D *Proof of Facts*, *supra* note 1, at § 1.

> Other aspects of the electronic information that are not considered part of the body or context of a message or file, but can be of immense importance, include date and time stamps reflecting the date of saving or transmission and the date of receipt, and a message's list of recipients.

Id. § 2. This article discussed that it is important for counsel to use electronic data to "become familiar with the forensics of the recovery and reconstruction of such data[]" when e-mails have been deleted from the system. *Id.* § 1. *See also* Dempsey, *supra* note 26, at 411 (noting that e-mails may contain private information). Dempsey stated:

> More and more of our lives are conducted online and more and more personal information is transmitted and stored electronically. Financial statements, medical data[,] and records of commercial transactions are computerized. Increasingly, book purchases, travel itineraries, and movie rentals are complied [sic] and stored online in "personal accounts." Most recently, storage has taken a new turn, as individuals use network capabilities to store draft documents, photos[,] and messages long since sent and retrieved--the kind of material once kept on paper and secure in a home or office.

Id. See also Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 139 (2005) (suggesting that it is surprising that this information can be accessed easier than a "search [of] our houses or even our cars[]"). *Id.*

174 *See* Slobogin, *supra* note 173, at 139.

175 *See* Steere, *supra* note 117, at 233 (stating that the ECPA "fails to provide enough protection to satisfy the true historical purpose of the Fourth Amendment[]").

176 United States v. Bach, 310 F.3d 1063, 1067 (8th Cir. 2002). *See* Zittrain, *supra* note 148 at 93 ("A lack of oversight or adversarial process for the kinds of searches that are about to become common threatens to have the exceptions dwarf the rule.")

177 *See* Rodriques v. Furtado, 575 N.E.2d 1124, 1126 (Mass. 1991). In *Rodriques*, police reasonably obtained a "warrant to search the plaintiff's vagina for narcotics" that included permission for that search "to be conducted by a licensed physician . . . ." *Id.* at 1126 (quotations omitted). The court held that although it was a troublesome outcome, the doctors were entitled to qualified immunity. *Id.* at 1130.

search, without officers present, drastically decreases the amount of privacy afforded to individuals.[178] One commentator called such unsupervised searches "sense-enhanced search[es,]" noting that these differ from the traditional "physical search."[179] To decide how much protection needs to be afforded during a search, courts consider the following factors: space available for physical presence, technical expertise of the person conducting the search, and location of the items seized.[180] Therefore, if the circumstances present themselves, it is likely that many seizures conducted without a police officer could violate Fourth Amendment rights because of the highly private correspondence that e-mails contain and the likelihood of exposure to ISP employees. In comparison, United States postal workers, similar to ISP employees, would not open mail without ensuring that a police officer supervises the search, even where a warrant has been obtained.[181]

Additionally, e-mail searches are not supposed to be an all-access pass for the government.[182] Decades ago, the great statesman Henry Stimson observed, "Gentlemen [and ladies] do not read each other's mail."[183] The Fourth Amendment was enacted to prevent the "hated

---

178 *Bach*, 310 F.3d at 1067.

179 *See* Steinberg, *supra* note 9, at 466 n.1 (Steinberg describes his use of the term "'sense-enhanced search' to describe police examination of a person or [his] property through the use of some method that provides information not available to unaided sensory perceptions[]" and the term "'physical search' to describe the traditional police search, which relies on unaided sensory perception[]").

180 *Bach*, 310 F.3d at 1067. In *Bach*, the court provided the following factors for evaluating the reasonableness of officer presence:

> (1) the actual physical presence of an officer would not have aided the search (in fact may have hindered it); (2) the technical expertise of Yahoo!'s technicians far outweighs that of the officers; (3) the items "seized" were located on Yahoo!'s property; (4) there was a warrant signed by a judge authorizing the search; and (5) the officers complied with the provisions of the Electronic Communications Privacy Act, 18 U.S.C. § 2701.

Id.

181 *See supra* note 45 (discussing a postal worker's lack of authority during a search and seizure of postal mail).

182 Theofel v. Farey-Jones, 359 F.3d 1066, 1071–72 (9th Cir. 2004). In *Theofel*, the court found an e-mail search under the SCA to be invalid where the government's subpoena was overbroad. *Id.* The subpoena was not narrowed and the government took all e-mails from the desired account. *Id.* at 1071. *See also* Robert M. Goldstein & Martin G. Weinberg, *The Stored Communications Act and Private E-Mail Communications*, CHAMPION, Aug. 2007, at 18 (concluding that the SCA provides the government with a "wholesale seizure" of its targets' e-mails).

183 *See* Steere, *supra* note 117, at 249 (quoting HENRY L. STIMSON, ON ACTIVE SERVICE IN PEACE AND WAR 7 (1948)) (alteration in original).

writs" that surfaced in the eighteenth century.[184] The idea is that government e-mail searches via warrant are narrowed by address, search terms, or time frames.[185] This narrowed search is supposed to protect account holder privacy, but often does not have the opportunity to be effective because the government typically seizes entire accounts without any narrowing guidelines.[186] Searches and seizures that are not narrowly tailored and that are open to ISP employee rummaging violate the Fourth Amendment.[187]

When combined, the SCA's provisions overwhelmingly cut in favor the government and deny meaningful protection to account-holding individuals.[188] The delayed notice provision can be stretched to such an extent that it can preclude notice entirely, despite other sufficient methods of preserving evidence such as file backups provided by the SCA.[189] Additionally, the lack of supervision of searches is problematic.[190] This is especially true in situations where notice has not been provided to an account holder and the search is performed unbeknownst to the account holder.[191] Despite the government's invasive power and lack of protection for individuals, courts have not provided consistent guidance when deciding cases involving sections 2703, 2704, and 2705 of the SCA.[192]

B. Jurisprudential Inconsistencies

Courts have been inconsistent when ruling on the constitutionality of the SCA, specifically sections 2703 and 2705.[193] Subjective and open-

---

184 *See* Snyder, *supra* note 10, at 1 (quoting Stanford v. Texas, 379 U.S. 476, 484 n.13 (1965)).

185 O'Grady v. Superior Ct., 139 Cal. App. 4th 1423, 1448 (Cal. App. 6th Dist. 2006). Seeking disclosure of records or information from an identified sender or receiver can be considered outside of the statutory authorization. *Id.*

186 *See supra* note 92 (discussing Yahoo! and the privacy breaches that occur when e-mail searches are not narrowed).

187 *See* Snyder, *supra* note 10, at 4. When general warrants were issued, "officials, broke down at least 20 doors and scores of trunks, and broke hundreds of locks." *Id.* Further, "the Fourth Amendment prohibits indiscriminate searches regardless of the technology involved[] . . . ." *Id.* at 6.

188 *See supra* Parts II.C.1–3 (discussing the interaction of sections 2703, 2704, and 2705 of the SCA).

189 *See supra* Part II.C.3 (outlining the delayed notice provision of the SCA).

190 *See supra* note 131 and accompanying text (discussing faxed warrants and seizures of entire accounts due to lack of official supervision).

191 *See supra* Part II.C.3 (discussing delayed notice provisions).

192 *See infra* Part III.B (describing jurisprudential inconsistencies).

193 Frederick M. Joyce & Andrew E. Bigart, *Liability for All, Privacy for None: the Conundrum of Protecting Privacy Rights in a Pervasive Electronic World*, 41 VAL. U. L. REV. 1481, 1482 (2007) (stating that "[c]onsequently, the current state of the law has left

ended terms in the Act leave room for much discretion and resemble the general warrants that the Fourth Amendment of the United States Constitution precludes.[194] Furthermore, the lack of procedural safeguards and lack of checks on government provide great potential for the government to violate the constitutional privacy rights afforded to e-mail account holders.[195]

To start, laws that govern ISPs must take into account that providers are not all the same: each provider has different requirements that governmental entities must meet when requesting account holder information, and a comprehensive law must account for these differences.[196] Research regarding how an ISP storage system operates could shed light on exactly how search engines can be effective in generating results from the term searches included in warrants and subpoenas.[197] Currently, general warrants are illegal and the term searches must be narrowed; however, currently term searches are often not narrowed.[198] Due to the reality of generalized searches, more

---

government, businesses, and private citizens without a clear sense of their legal rights, obligations, and liabilities[]"). *See also* Steinberg, *supra* note 9, at 466–71 (concluding that Supreme Court decisions, where "sense-enhanced searches[]" are at issue, are inconsistent, arbitrary, and fail to develop a coherent body of law). The statutory framework of the ECPA in general has been described as "notoriously confusing and unclear[,]" whereas "Fourth Amendment concepts tend to be relatively accessible." *Id.* at 475 (citing Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 747 (2005)).

194 *See supra* Part II.C.4 (describing that by proposing an amendment to the SCA, Congress acknowledged the reality of objective searches).

195 *See supra* Parts II.C.1–4 (outlining SCA sections 2703, 2704, and 2705).

196 *See supra* Part II.A (discussing specifics about ISPs and acknowledging the wide variety of capabilities among various ISPs).

197 *See supra* Part II.A. *See also* 41 AM. JUR. 3D *Proof of Facts*, *supra* note 1, at § 1 (stating that e-mail often provides "smoking gun" evidence, and noting that e-mail can be recovered and reconstructed from computer files).

> [C]omputer data is not safe from disclosure merely because it has been "deleted" from a system or is contained in a damaged disk or hard drive. "Using sophisticated computer programs, electronic mail messages or computer files thought to be deleted can be retrieved from the deep recesses of a computer data base long after they have disappeared from the screen." Given the potential value of such material, "[m]ore and more jilted employees, angry business rivals, and injured consumers are waging legal wars with floppy disks and hard drives."

Id. (second alteration in original) (footnote omitted).

198 *See supra* note 84 (suggesting specifics of how to narrow searches through fields and keywords).

supervision is necessary to ensure that government officials engage in appropriate ISP account searching.[199]

The lack of concern for the privacy of e-mail content is almost certainly due to the limited knowledge that account holders have about their privacy rights when it comes to their e-mail account.[200] This has to be a valid assumption due to judicial holdings and the opinions of legal theorists that e-mail is private and protected by the Fourth Amendment.[201] Conversely, the fact that e-mail is constitutionally protected should give account holders the assurance that nobody can subpoena or search their e-mail.[202]

Electronic communications law that began developing with *Katz* in the 1960s is applicable to e-mail.[203] As an account holder, knowledge of network policies and how they apply to usage can be extremely valuable.[204] Theoretically, network administrators may decide exactly how much privacy to give their account holders.[205] Furthermore, the *Smith* third-party approach is valid in conjunction with users' expectation of privacy.[206] Writing an e-mail from an Internet café with six friends huddled around as a joke would not likely result in a legitimate expectation of privacy. On the other hand, an individual who solely composes and sends an e-mail from the same Internet café while sitting in the corner would likely have legitimate privacy expectations.[207]

---

[199] *See supra* notes 131, 180 (discussing how implementing the requirement of a police officer's presence during searches provides more structure to the search and provides supervision, without which ISP employees become lazy and reveal full account content).

[200] *See supra* Part II.C.3 (discussion of delayed notice).

[201] *See supra* Part II.B (summarizing the development of electronic communications jurisprudence, first addressing seizures of letters and telephones and subsequently addressing e-mail seizures).

[202] *See supra* Part II.B (discussing the *Smith* third-party doctrine and server policies as avenues for the government to circumvent notice to the account holder); *see also* United States v. Rodriguez, 532 F. Supp. 2d 332, 340 (D. Puerto Rico 2007) (suggesting that the ECPA is "hardly a legislative determination that this expectation of privacy is one that rises to the level of 'reasonably objective' for Fourth Amendment purposes[]").

[203] *See supra* Part II.B.1 (discussing the development of electronic communications case law).

[204] *See supra* Part II.B.5 (discussing reasonable expectations and privacy policies and jurisprudence relating to both).

[205] *See supra* Part II.B.5 (analyzing the structure of privacy policies as related to reasonable expectations by users).

[206] *See supra* Part II.B.1; *c.f.* United States v. D'Andrea, 497 F. Supp. 2d 117, 118 (D. Mass. 2007) (suppressing evidence gained from a phone call to the Department of Social Services by a third party who provided an e-mail link and password for access to pictures that incriminated defendants). *D'Andrea* held that the third party doctrine trumps the expectation of privacy when information is conveyed to an outsider and that outsider conveys the information to the authorities. *Id.* at 123.

[207] *See supra* Part II.B.1 (discussing *Katz*'s requirements to protect communications).

E-mail has been distinguished by the SCA based on the length of time that it is stored.[208] The arbitrary length of time of 180 days is assigned to determine through which procedural channels the Government must navigate.[209] Coincidently, such an arbitrary time frame does not apply to searches of letters and sealed containers.[210] Likely, similar information will result from seizures of information from both time frames.[211] For example, the information from an account that sends payment reminders or confirmation messages to an individual's e-mail account is likely archived and will result in the same information retrieved whether the search is targeted at the last week or the last year.[212] The government should have to prove the desired time frame and the desired content for the search because an account holder's entire e-mail account is likely to have the same privacy expectations attached to it.[213] Additionally, account information is a source of evidence that the government can easily obtain along with third-party communication as an alternative source that is less invasive of privacy.[214] By giving the government direct access to e-mail content, the government circumvents long established privacy rights granted by the Fourth Amendment.[215]

The uniqueness of e-mail should make it easier for the government to preserve evidence while building a case. Unlike letters, packages, and telephone calls, e-mail inevitably leaves an electronic trail.[216] Section 2704 grants to the government the powerful tool of account preservation.[217] Given the knowledge of such capabilities, questions should be raised as to why unlimited and objective delayed notice procedures in Section 2705 are necessary.[218] The analogy drawn could be as follows: if the government has the power of a fully armed tank, such

---

208 *See supra* Part II.C.1; *supra* note 126 (discussing the 181-day storage length for e-mail where e-mails more than 180 days old are easier for the Government to seize).

209 *See supra* Part II.C.1; *see also supra* note 126 (discussing the Plaintiff-Appellee brief in *Warshak I*, which explains why the 180-day time frame seems arbitrary to the average subscriber).

210 *See infra* text accompanying note 233 (claiming that e-mails and paper letters should be treated similarly).

211 *See supra* note 126 (addressing the *Warshak I* brief's discussion of the arbitrary 180-day timeframe for e-mail storage).

212 *See supra* note 126 (addressing the *Warshak I* brief's discussion of the arbitrary 180-day timeframe for e-mail storage).

213 *See supra* notes 84, 182, 186 (discussing the narrowing of searches).

214 *See supra* note 123 (citing text of the account information provision of the SCA).

215 *See supra* Part II.B (discussing the background of electronic communications law that has strictly applied the Fourth Amendment).

216 *See supra* Part II.A (outlining technical ISP basics).

217 *See supra* Part II.C.2 (explaining the application of section 2704 of the SCA to e-mail account preservation).

218 *See supra* Part II.C.3 (explaining the delayed notice provision of the SCA).

as section 2704, then why does it need the musket-like power of section 2705? The simple answer is that it does not, and account holders are victims of an excessive and unconstitutional invasion of privacy.

E-mail serves as a communication highway and should be vehemently protected as private under the Fourth Amendment, just as letters and telephone calls have been in the past.[219] Because of the ease with which e-mail content is obtained from ISPs, the government has intruded upon the privacy that account holders believe guard their interests.[220] Arbitrary and objective provisions in sections 2703, 2704, and 2705 combined have left the judiciary ill-equipped to address today's e-mail issues, and the fifty-year-old doctrine of *Katz* has prevailed as the solution.[221]

Simple adjustments can be made to the above mentioned sections of the SCA that will enhance the way in which the sections interact and reduce invasive governmental actions concerning private e-mail. It is possible to protect individual privacy, give the government ample power to ensure national security, and bring the SCA back within the bounds of the Constitution by amending the SCA, as proposed next in Part IV, to cure its problematic sections.

IV. PROPOSED LEGISLATION

Reliance on protections such [as] individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is penetrable.[222]

---

[219] *See supra* Part II.B.4 (discussing notions of privacy attached to e-mail); *see also supra* Part II.B.1 (discussing initial judicial decisions involving electronic privacy issues such as *Katz* and *Smith*).

[220] *See supra* Part II.B.4 (discussing the presumed privacy that account holders believe attaches to e-mail).

[221] *See supra* note 94 (discussing the *Warshak I* court's analysis of the similarities between telephone content and e-mail content). *See* Smith v. Maryland, 442 U.S. 735, 739 (1979) (citing Katz v. United States, 389 U.S. 347, 351–53 (1967)). The *Smith* court explicitly "rejected the argument that a 'search' can occur only when there has been a 'physical intrusion' into a 'constitutionally protected area,' noting that the Fourth Amendment 'protects people, not places.'" *Id*. at 739 (citing *Katz*, 389 U.S. at 351–53).

[222] WAYNE R. LAFAVE, 1 SEARCH AND SEIZURE § 2.6 at 721 (4th ed. 2006) (citing Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995)). LaFave finds that e-mail has a justified expectation of privacy because it offers greater security than faxes, mail, shipping services and land-line conversations. *Id.* at 726. However, once the e-mail reaches a recipient, akin to a letter reaching its destination, the person who sent the item "has no valid Fourth Amendment complaint should the recipient turn the message over to the police or forward it on to others, or should the recipient turn out to be an undercover police officer." *Id.* at 727 (footnotes omitted).

Courts have not effectively addressed the issue of e-mail privacy because the SCA provisions became confusing and unclear as technology strayed from using simplistic locks and bolts to protect our personal items.[223] Furthermore, when courts apply the law, they are wary of Fourth Amendment conflicts that inevitably arise.[224] Too many governmental safeguards conflict with constitutional guarantees of privacy.[225] Some of the procedural aspects of the SCA must be downgraded to enhance notions of privacy.[226] Therefore, this Note suggests the following amendments to the sections of the SCA that are problematic—sections 2703, 2304, and 2705.[227] First, the 180 day time frame of e-mail preservations should be eliminated in 18 U.S.C. § 2703(a) to allow for a more even application in regard to e-mail seizures.[228] Next, 18 U.S.C. § 2703(g) must be modified to require police officer presence during searches of e-mail at electronic communications services or remote computing centers.[229] Last, 18 U.S.C. § 2705 must be amended to clarify the objective terminology in § 2705(a)(5) describing an "adverse result," heighten the standard for preclusion notice in § 2705(b), and explicitly grant injunctive relief when notice is not given at the expiration of delay periods for § 2705.[230]

A. Proposed Amendment to 18 U.S.C. § 2703(a)

Congress should amend 18 U.S.C. § 2703(a) as follows, with the normal font representing the current statutory language, the text with a line through it representing the text the author of this Note proposes to delete from the statute, and the italicized text representing the text the author of this Note proposes to add to the statute:

> **(a) 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 a wire or electronic communication, that is in electronic storage in

223 *See supra* Part III.B (analyzing issues courts deal with when interpreting conflicts between the SCA and the Fourth Amendment).
224 *See supra* Part II.B.2–3 (discussing *Warshak I*, *Allen*, *Ashcroft* (*Doe I*), and *Gonzalez* (*Doe II*)).
225 *See supra* Part III.A (analyzing sections 2703, 2704, and 2705 of the SCA).
226 *See supra* Part III.A (analyzing sections 2703, 2704, and 2705 of the SCA).
227 *See infra* Part IV.
228 *See infra* Part IV.A.
229 *See infra* Part IV.B.
230 *See infra* Parts IV.C–D.

> an electronic communications system ~~for one hundred and eighty days or less~~, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant~~. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days~~, *and* by the means available under subsection (b) of this section.

Commentary

This proposed amendment to section 2703(a) is one way courts, ISPs, and account holders can apply the SCA as a blanket when executing a search. Trying to figure out the time distinction as the statute currently states is a waste of valuable resources because in the end individual account holders subjectively regard all of their e-mail as having the same amount of privacy.[231] Furthermore, objectively, the public at large does not use time as a factor for distinguishing whether the correspondence is more or less private.[232] Last, e-mails are said to be given the same amount of privacy as sealed letters and telephone calls, which do not operate on a scaled, time frame basis. Therefore, just because it is easier to preserve e-mails on a server, than to preserve letters in a shoebox, e-mails should not be treated drastically different than letters in a shoebox.[233]

B. Proposed Amendment to 18 U.S.C. § 2703(g)

Congress should amend 18 U.S.C. § 2703(g) as follows, with the normal font representing the current statutory language and the text with a line through it representing the text the author of this Note proposes to delete from the statute.

> **(g) Presence of officer ~~not~~ required.**—~~Notwithstanding section 3105 of this title,~~*T*he presence of an officer shall ~~not~~ be required for service or execution of a search warrant issued in accordance with this chapter requiring

---

231 *See supra* note 126 (*Warshak I* court discussing the time limits placed by the SCA).
232 *See supra* note 126 (*Warshak I* court discussing the time limits placed by the SCA).
233 *See supra* note 95 (analogizing letters and sealed containers to e-mails).

> disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

Commentary

This proposed amendment to section 2703(g) is a means to the end of preserving privacy. Within the same title, under the current statutory language, section 3105 requires officer presence during the service and execution of the warrant; however, section 2703 is exempt from this requirement. This proposed amendment to the current language reins in the power of employees to haphazardly sift through e-mails, while, at the same time, adequately preserves the Fourth Amendment's guarantee of privacy.[234] Additionally, officer presence enhances the search and seizure of e-mails by adding authority to the process.[235] Like postal employees, who are not allowed to open letters even when a warrant is presented, ISP workers should not have that power either.[236] Therefore, this minor and important adjustment enhances the process in a variety of ways.

C. Proposed Amendment to 18 U.S.C. § 2705(a)(5)

Congress should amend 18 U.S.C. § 2705(a)(5) as follows, with the normal font representing the current statutory language and the italicized text representing the text the author of this Note proposes to add to the statute.

> (a)(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that—
>
> (A) states with reasonable specificity the nature of the law enforcement inquiry; and
>
> (B) informs such customer or subscriber—

---

[234] *See supra* notes 176–81 and accompanying text (analyzing the need for law enforcement officer presence during an e-mail search).

[235] *See supra* note 131 and accompanying text (discussing one theorist's view on police officer presence during e-mail searches).

[236] *See supra* note 45 (discussing *Ex parte* Jackson, 96 U.S. 727 (1878)).

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
(ii) that notification of such customer or subscriber was delayed;
(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and
(iv) which provision of this chapter allowed such delay.

If, upon expiration of the delay, notice is not served as dictated above to the account holder, then injunctive relief shall be granted barring all seized documents from evidence.

Commentary

Language describing an injunction must be added to the delayed notice provision as a restraint on government abuse. Currently, government actors do not provide notice to account holders whose circumstances have fallen under this provision, which results in a Fourth Amendment violation.[237] The SCA does not currently explicitly state that injunctive relief is proper.[238] This amendment to section 2705(a)(5) will provide much needed clarity for courts; it will be clear that any unauthorized e-mails obtained in violation of giving notice shall be excluded from evidence. Thus, this proposed change will save judicial resources and provide a constitutionally just result to the account holder.

D. Proposed Amendment to 18 U.S.C. § 2705(b)

Congress should amend 18 U.S.C. § 2705(b) as follows, with the normal font representing the current statutory language, the text with a line through it representing the text the author of this Note proposes to delete from the statute, and the italicized text representing the text the author of this Note proposes to add to the statute.

---

[237] *See supra* notes 84, 182, 186 (discussing the use of broad, not narrow, searches by ISPs to protect privacy).

[238] *See supra* note 92 (discussing suppression remedies and the Fourth Amendment).

> **(b) Preclusion of notice to subject of governmental access.—**A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for ~~such period as the court deems appropriate~~*ninety days*, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—
> (1) endangering the life or physical safety of an individual;
> (2) flight from prosecution;
> (3) destruction of or tampering with evidence;
> (4) intimidation of potential witnesses; or
> (5) otherwise seriously jeopardizing an investigation or unduly delaying trial.

Commentary

Delayed notice creates the biggest Fourth Amendment concern for subscribers.[239] By delaying notice that the government seized and examined the contents of private e-mail, section 2705 as it is currently drafted exceeds governmental limits as designated in the Constitution.[240] To curtail the effect of lack of notice, the unlimited preclusion for delay must be deleted from the SCA and a designated timeframe added, such as ninety days.[241] This proposed change enhances the SCA, brings it back within Fourth Amendment guarantees, and leaves open the opportunity to merge section 2705(b) with section 2705(a)(4), which provides a consistent approach for efficiency's sake. Additionally, section 2705(b)(5) should enumerate examples to lessen the objective nature of court decisions. Such objectivity can lead to entirely different

---

[239] *See supra* Part II.C.3 (discussing delayed notice); *see also supra* Part III.A (analyzing the same).

[240] *See supra* notes 138–43 and accompanying text (discussing constitutional problems with delayed notice).

[241] *See supra* text accompanying note 170 (discussing the potential infinite preclusion of notice).

outcomes and, when privacy is at issue, individual rights should not tolerate this inconsistency.[242] Finally, this proposed change restrains the SCA from violating privacy rights by still providing direction to the government and courts regarding how to search and seize e-mail from third party ISPs.

The above proposed amendments to the SCA together will reduce the likelihood of unconstitutional encroachment on account holders' privacy rights.[243] As demonstrated, the proposed changes are not drastic, and yet, effectively achieve the goals of the government and account holders, and assist courts in interpreting the SCA. By minimizing excessive governmental safeguards, the proposed amendments streamline the SCA to protect both the Government's interest in preserving evidence and the subscriber's interest in maintaining privacy.

V. CONCLUSION

Tolling for the aching ones whose wounds cannot be nursed
For the countless confused, accused, misused, strung-out ones an' worse
An' for every hung-up person in the whole wide universe
An' we gazed upon the chimes of freedom flashing.[244]

Freedom from search and seizure will soon be a flash before the eyes of many Americans as Fourth Amendment interests are trampled by the SCA. Too much time has passed without action to restore e-mail account holder privacy interests. If the amendments to the SCA proposed in Part IV of this Note are implemented, then embarrassment, like the embarrassment described in Part I suffered by John Jones's family, will be eliminated or certainly mitigated. Pursuant to the amendments proposed in Part IV, the government would not be allowed to search e-mail contents without a warrant, and the search would be supervised

---

[242] *See supra* note 92 (comparing United States v. Ferguson, 508 F. Supp. 2d 7 (D.D.C. 2007) and Warshak v. United States (Warshak I), 490 F.3d 455 (6th Cir. 2007), *vacated on other grounds en banc by* No. 06-4092, 2007 U.S.App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *modified by* 2007 WL 4410237 (S.D. OH Dec. 13, 2007) (Warshak II), *rev'd on other grounds by* 532 F.3d 521 (6th Cir. 2008) (Warshak III)).

[243] *See supra* Part II.C (comparing sections 2703, 2704, and 2705 of the SCA, and discussing the way all three sections interact together).

[244] BOB DYLAN, CHIMES OF FREEDOM (Legacy Recordings 1964). Released in 1964, just three years before the United States Supreme Court decided *Katz*, *Chimes of Freedom* may be analogized to today's invasion of e-mail privacy. *See id.* *See also* Mike Marqusee, CHIMES OF FREEDOM: THE POLITICS OF BOB DYLAN'S ART (2003). *Chimes of Freedom* represented a transition between Dylan's early protest style and his later poetic tendencies, and serves as a warning that the problems of yesterday are still faced today. *See* Marqusee, *supra*.

and narrowly tailored, thus discouraging Betty Eyez from her nosy habits. By applying the suggested changes as proposed, Congress will be able to rein in the government's unconstitutional behavior and still achieve the goal of preserving evidence.

E-mail is the communication of today's world. It is not limited to just today's children, but also yesterday's children, as parents and grandparents increasingly log on to their computers to see what awaits them in their e-mail inboxes. As the variety of transactions from our home computers increases exponentially, account holders' privacy interests become all the more precious. The SCA is currently written in such a way that leaves too many standards open-ended. Courts have inconsistently interpreted the SCA, leaving many questions remaining about how to apply sections 2703, 2704, and 2705 of the SCA, while not offending the Fourth Amendment rights of individuals. Congress should revise the SCA according to the amendments proposed in Part IV and ensure the privacy guarantees on which our Founders established this country. As Justice Stewart so eloquently stated thirty years ago, "[privacy] considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, *he is entitled to know* that he will remain free from unreasonable searches and seizures."[245]

Kimberly S. Cuccia[*]

---

[245] Katz v. United States, 389 U.S. 347, 358 (1967) (emphasis added).

[*] J.D. Candidate 2009, Valparaiso University School of Law; B.A., Business Administration, University of Florida, 2005. Special thanks to my Mom, Tom, Abby, Charlie, Nana, and the rest of my wonderful family for their unconditional love and encouragement, not only through law school, but through all of my journeys. Also, thanks to my friends, Julia for being the best friend anyone could ask for, and to all of the people I have met over the past three years at Valpo Law. One journey ends and another begins. Thank you all for adding vibrant colors to the crayon box of life. Also, very special thanks to Professor Rosalie Berger Levinson for her invaluable help during the notewriting process and her dedication to teaching the law, and also to Professor Derrick Carter for his endless ideas and ever open door.