3-1-2011

U.S. v. Warshak: Will Fourth Amendment Protection Be Delivered to Your Inbox

Casey Perry

Follow this and additional works at: http://scholarship.law.unc.edu/ncjolt

Part of the Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncjolt/vol12/iss2/5

This Notes is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of Law & Technology by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
The Warshak decision is a long-overdue federal case extending Fourth Amendment protection to electronic communications stored with third parties. In holding that citizens have a “reasonable expectation of privacy” for stored e-mail messages, the Sixth Circuit decision represents a shift towards a stricter interpretation of the Fourth Amendment as it applies to modern forms of communication. Applauded by civil liberties and privacy protection groups, Warshak may pave the way for communication over other digital means (e.g., cloud computing, Facebook, LinkedIn) to obtain Fourth Amendment protection, through application of a two-prong test to determine the existence of a reasonable expectation of privacy. Warshak also highlights blatant loopholes in the current federal statutory scheme, underscoring the need for revision of the Stored Communications Act in order to bring the law in line with modern technology.

I. INTRODUCTION

There are few concepts as deeply entrenched in American law as individual privacy. The fervent reverence afforded to privacy as a fundamental human right is reflected in our Constitution, particularly in the Bill of Rights. One of the most important

* J.D./M.B.A. Candidate, University of North Carolina School of Law, 2012.
1 Though the U.S. Constitution contains no explicit right to privacy, many of the first ten amendments protect particular aspects of individual privacy. For example, the Third Amendment safeguard against the nonconsensual quartering of soldiers is often interpreted as the Founders’ expression of protecting privacy, as are the individual liberties enumerated in the First Amendment. See Doug Linder, The Right of Privacy, EXPLORING CONSTITUTIONAL LAW, http://www.law.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html (last visited Feb. 23, 2011) (maintaining that the Bill of Rights reflects the Framers’ concern for the protection of individual’s privacy rights).
safeguards of individual privacy is found in the Fourth Amendment right of the people to be secure “in their persons, houses, papers, and effects, against unreasonable searches and seizures,” requiring that warrants be issued only upon a showing of probable cause and specifying “the place to be searched, and the persons or things to be seized.” While the language of the Fourth Amendment makes it clear that the Founders intended to limit the use of searches and seizures to those that are reasonable, what constitutes a “reasonable” search and seizure has been extensively debated.

2 U.S. CONST. amend. IV. While some “highly cherished freedoms, such as those relating to speech, religion, press and trial by jury were lumped in together with others,” the prohibition against unreasonable searches and seizures was considered important enough to constitute a single amendment. Charles A. Reynard, Freedom from Unreasonable Search and Seizure—A Second Class Constitutional Right?, 25 IND. L.J. 259, 273 (1950).

3 See Thomas Y. Davies, Recovering the Original Fourth Amendment, 98 MICH. L. REV. 547, 551 (1999) (discussing the Founders’ intent to limit searches and seizures and condemn the use of general warrants).

4 Compare Dorothy K. Kagehiro, Ralph B. Taylor & Alan T. Harland, Reasonable Expectation of Privacy and Third-Party Consent Searches, 15 LAW & HUM. BEHAV. 121, 122 (1999) (stating that the Fourth Amendment indicates that searches are only “reasonable” if they are conducted under a warrant representing judicial determination of probable cause or, alternatively, if they fall under an exception to the warrant requirement made by the United States Supreme Court over the years), and Reynard, supra note 2, at 276 (contending that the Fourth Amendment offers dual guarantees, both that warrants shall be issued with probable cause and particularity and that no unreasonable searches or seizures shall be made, even with a warrant), with Davies, supra note 3, at 551 (opining that the Founders did not consider the application of “unreasonable” to unwarranted searches at all, but meant for the standard to apply to the “inherent illegality of any searches or seizures . . . under general warrants.”), David A. Sklansky, The Fourth Amendment and Common Law, 100 COLUM. L. REV. 1739, 1740 (2000) (arguing that modern courts determine whether a search or seizure is “unreasonable” based on “the realities of modern law enforcement rather than the eighteenth-century origins of the Fourth Amendment”), and Tracey Maclin, The Central Meaning of the Fourth Amendment, 55 WM. & MARY L. REV. 197, 201 (1993) (arguing in support of the theory that the Fourth Amendment “merely requires rational police behavior . . .”). But see Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 MINN. L. REV. 349, 395 (1974) (stating succinctly that “its language is no
Today, the “reasonable expectation of privacy” test is used to determine whether a search meets the reasonableness requirement, and to define when law enforcement’s finding and taking of property is a “seizure” protected by the Fourth Amendment. As Justice Harlan explained in *Katz v. United States,* the expectation of privacy test that has emerged is twofold, requiring first, that a person “have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” Applying this test, courts have found that certain mediums of communication, including the telephone and postal mail, are protected by a reasonable expectation of privacy. These decisions require law enforcement to obtain a valid warrant based on probable cause before seizing such communications.

Today, as people increasingly turn to digital means of communication in both their private and professional lives, many have called for the expansion of Fourth Amendment protection to incorporate a modern interpretation of an individual’s “papers and effects.” Despite this push for the Fourth Amendment to keep help and neither is its history” and that we can glean a better understanding of “reasonableness” from the origin of the Fourth Amendment).

5 “I join the opinion of the Court, which I read to hold only (a) that . . . 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.” *Katz v. United States,* 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

6 *Id.* at 361 (Harlan, J., concurring).

7 *See id.* at 352–59 (holding that the practice of wiretapping telephone calls is subject to the Fourth Amendment, because of the “vital role that the public telephone has come to play in private communication”); *United States v. Jacobsen,* 466 U.S. 109, 114 (1984) (“Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy . . . .”)

8 *See, e.g., Jacobsen,* 466 U.S. at 114 (“[W]arrantless searches of [the general class of effects in which the public at large has a legitimate expectation of privacy] are presumptively unreasonable.”).

9 *See, e.g., Andrew William Bagley,* *Don’t Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects,* 21
pace with evolving technology, there has been little direction from the federal courts regarding the reasonable expectation of privacy for digital communication, including emails. However, on December 14, 2010, the Sixth Circuit of Appeals took a critical first step towards defining these issues, addressing the applicability of the Fourth Amendment protection to emails stored with internet service providers ("ISPs") in the landmark case of United States v. Warshak.

In Warshak, the Sixth Circuit held that the reasonable expectation of privacy for communication via telephone and postal mail extends to emails stored with third parties, bringing stored emails within the protection of the Fourth Amendment. As the only federal appellate decision to rule on the privacy of stored emails, Warshak prompts a series of questions, not only about the

ALB. L.J. SCI. & TECH. 153 (2011) (urging an update of the Fourth Amendment to reflect the reality that papers and effects are now often digital in nature).

10 "To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." Kyllo v. United States, 533 U.S. 27, 34 (2001).

11 Susan Freiwald, Susan Freiwald on United States v. Warshak: Sixth Circuit Brings Fourth Amendment Protection to Stored Email, At Last, CONCURRING OPINIONS BLOG, posted by Danielle Citron (Dec. 17, 2010, 3:15 PM), http://www.concurringopinions.com/archives/2010/12/susan-freiwald-on-united-states-v-warshak-sixth-circuit-brings-fourth-amendment-protection-to-stored-email-at-last.html [hereinafter Freiwald, Susan Freiwald on United States v. Warshak]. The Stored Communications Act, a federal law addressing stored wire and electronic communications, is discussed infra Part II. Internet Service Providers ("ISPs") are businesses or organizations that offer Internet access, often in the form of broadband or dial-up Internet access. What is an Internet Service Provider (ISP)?, INDIANA UNIVERSITY KNOWLEDGE BASE, http://kb.iu.edu/data/ahoz.html (last visited Feb. 25, 2011).

12 631 F.3d 266 (6th Cir. 2010).


future of privacy in electronic communications, but also about the efficiency and effectiveness of current federal privacy laws relating to the government’s ability to search and seize stored electronic communications.\footnote{See id. (advocating for Congress to revise the Stored Communications Act to clearly require warrants to obtain emails from ISPs in light of the \textit{Warshak} ruling).}

In order to fully understand the \textit{Warshak} decision and its implications, Part II of this Recent Development will provide a brief explanation of the Stored Communications Act,\footnote{The Stored Communications Act is codified at 18 U.S.C. §§ 2701–12 (2006) and discussed \textit{infra} Part II.} a federal statute addressing electronic communication privacy critical to the \textit{Warshak} opinion. Part III will then introduce the \textit{Warshak}\footnote{631 F.3d 266.} decision itself, including the prior history of the case. Part IV discusses the potential need for Congressional reform of the Stored Communications Act, based on loopholes highlighted by the \textit{Warshak} investigation. Finally, Part V will look towards the future of the \textit{Warshak} decision and its implications for the rest of the country, followed by a brief conclusion.

\section*{II. THE STORED COMMUNICATIONS ACT}

Supplementing the Fourth Amendment, there are three primary federal statutes that serve to protect individuals’ privacy in a network environment, collectively known as the Electronic Communications Privacy Act (“ECPA”).\footnote{See Orin S. Kerr, \textit{Computer Crime Law} 456 (2d ed. 2006).} The Stored Communications Act, the Wiretap Act, and the Pen Register statute regulate criminal investigators’ access to both in-transit electronic communications and stored content, including emails stored with ISPs.\footnote{\textit{Id.} at 456. The Wiretap Act, 18 U.S.C. §§ 2510–22, “regulates efforts to collect evidence by intercepting the contents of Internet communications in real time.” Kerr, \textit{supra} note 18, at 256. The Pen Register statute, 18 U.S.C. §§ 3121–27, regulates “collecting evidence by obtaining non-content information in real time.” \textit{Id.} at 456. The Wiretap Act and the Pen Register statute were not referenced in the \textit{Warshak} opinion and are thus outside the scope of this Article.} The Stored Communications Act, regulating
access to stored content, was particularly relevant to the Warshak case and thus requires a brief explanation.

A. The Structure of the Stored Communications Act

Passed in 1986 as part of the Electronic Communications Privacy Act of 1986, the Stored Communications Act ("SCA") is a federal statute that regulates access to stored electronic communications. The SCA regulates retrospective surveillance, specifically content that is in storage with an ISP. Two of the principal provisions of the SCA are found in sections 2702 and 2703, which regulate voluntary disclosures and compelled disclosures, respectively. In section 2703, the SCA imposes strict scope of this Recent Development. For more on these statutes, see id. at 461–97 (on the Wiretap Act) and 497–510 (on the Pen Register statute).

20 The Electronic Communications Privacy Act of 1986 was created to fill gaps in existing privacy law created by changing technologies, specifically computer network technologies, amounting to "a statutory version of the Fourth Amendment for computer networks." Id. at 458–59.


22 Kerr describes retrospective surveillance as "access to stored communications that may be kept in the ordinary course of business by a third-party provider" and gives the following example:

[I]f an FBI agent issues a subpoena ordering an ISP to disclose basic subscriber information about a particular Internet account, that access is a type of retrospective surveillance. The ISP will have generated that record at some time in the past in the ordinary course of its business; the subpoena seeks the disclosure of a stored record that already has been created.

KERR, supra note 18, at 459. In contrast, prospective surveillance refers to "obtaining communications still in the course of transmission." Id. The Wiretap Act and the Pen Register statute both deal with prospective surveillance. Id.

23 Id. at 510. The SCA does not apply to communication that is in transit. See, e.g., Dorothy Higdon Murphy, United States v. Councilman and the Scope of the Wiretap Act: Do Old Laws Cover New Technologies?, 6 N.C. J.L. & TECH. 437, 459 (2005) ("The SCA, however, does not apply to messages that are still in transmission. Electronic messages that are in transmission are covered by the Wiretap Act.").

24 KERR, supra note 18, at 511. Other important sections include § 2705, the delayed notice provision, § 2708, the remedies limitation, and § 2711, which includes definitions. Id.
rules on when the government may compel service providers to disclose information they are storing on their subscribers.\textsuperscript{25} The SCA creates similar limits on voluntary disclosures to the government by ISPs in section 2702, heightening the protection provided by the private search doctrine of the Fourth Amendment.\textsuperscript{26} According to the United States Department of Justice, the SCA serves “to protect and regulate the privacy interests of network users with respect to government . . . and the world at large,”\textsuperscript{27} yet courts have had a difficult time interpreting and applying the statute, due in no small part to its density and complexity.\textsuperscript{28}

B. Government Access under the SCA

In regulating government access to emails, the SCA offers various levels of protection based on the length of time the email has been stored electronically and the type of service in which the

\textsuperscript{25} \textit{Id.} “Although the Fourth Amendment may require no more than a subpoena to obtain e-mails, the statute confers greater privacy protection.” \textit{Id.}

\textsuperscript{26} \textit{Id.}


\textsuperscript{28} See, e.g., Kerr, supra note 21, at 1208 (“But courts, legislators, and even legal scholars have had a very hard time understanding the method behind the madness of the SCA. The statute is dense and confusing, and that confusion has made it difficult for legislators to legislate in the field, reporters to report about it, and scholars to write scholarship in this very important area”); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (quoting Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994)) (referring to the provisions of the ECPA as “famous (if not infamous) for [their] lack of clarity” and the “complex, often convoluted” intersection of the SCA and the Wiretap Act); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (describing the statutory framework as “ill-suited to address modern forms of communication” like a secure website); Lieutenant Colonel LeEllen Coacher, Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See, 46 A.F. L. REV. 155, 171 (1999) (commenting that the intent of Congress to cover email transmissions via the ECPA was obscured by the complexity of the statutory language).
email is held.29 For example, emails stored with an electronic communication service for less than 180 days may be acquired "only pursuant to a warrant."30 Emails stored with a remote computing service and those stored with an electronic communication service for more than 180 days require the government to either obtain a search warrant, an administrative subpoena, or a court order.31 Though probable cause is required to obtain a search warrant, the SCA allows subpoenas and court orders to be issued under much lower standards than those of the Fourth Amendment, requiring only that the government entity offer "specific and articulable facts" showing "reasonable grounds" to believe that the contents of the communication "are relevant and material to an ongoing criminal investigation."32

III. UNITED STATES V. WARSHAK

The Warshak case was not one, but a series of cases, both criminal and civil. The Sixth Circuit case at issue stems from

---

29 United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010). Emails may be held with either an electronic communication service or a remote computing service. Id. The U.S. Code defines an electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). A remote computing service is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). If these definitions seem less than clear, you are not alone. See supra text accompanying note 28.

31 Warshak, 631 F.3d at 283. The court in In re Grand Jury Subpoenas Dated Dec. 10, 1987 distinguished subpoenas from search warrants:
Subpoenas are not search warrants. They involve different levels of intrusion on a person's privacy. A search warrant allows the officer to enter the person's premises, and to examine for himself the person's belongings. The officer, pursuant to the warrant, determines what is seized. . . . Service of a forthwith subpoena does not authorize an entry into a private residence. Furthermore, the person served determines whether he will surrender the items identified in the subpoena or challenge the validity of the subpoena prior to compliance. 926 F.2d 847, 854 (9th Cir. 1991).
Warshak’s appeal from his May 2008 conviction by the U.S. District Court for the Southern District of Ohio.33

A. The Controversial Seizure of Warshak’s Emails

The Warshak case arose out of a criminal investigation involving Stephen Warshak, his mother Harriet,34 and the management of his mail-order nutritional supplements business, Berkeley Premium Nutraceuticals, Inc. (“Berkeley”).35 From all accounts, Warshak ran a shady business centered around the sale of its flagship product, the infamous Enzyte male enhancement supplement.36 In addition to the now infamous “Smilin’ Bob” commercials,37 Berkeley’s advertising techniques for Enzyte included a bogus independent customer study,38 a spurious customer satisfaction rating,39 and the lauding of impressive but

34 Warshak’s company employed “approximately 12 to 15 people, nearly all of whom were Warshak’s friends and family.” Warshak, 631 F.3d at 276. Harriet was Warshak’s mother as well as an employee of the business, in which capacity she processed credit card payments. Id. Warshak also employed his sister, who worked in Customer Care, and his brother-in-law, who served as President of the company. Id.
35 Warshak did not own just one, but “a handful” of companies. Id. One, TCI Media, Inc., sold advertisements in sporting venues, while other assorted “nutraceuticals” companies operating under various names were later aggregated to form Berkeley. Id. In addition to herbal supplements, the companies also sold a product marketed to mask drug traces in urine tests, called Keflex. Id. at 276 n.1.
36 Id. at 276–77. Enzyte, purported to “increase the size of a man’s erection,” pushed Berkeley’s annual sales to nearly $250 million in 2004. Id. at 276.
37 “Smilin’ Bob” was a character featured in Enzyte commercials characterized by an “exaggerated smile . . . presumably the result of Enzyte’s efficacy.” Id. at 277. A clip of Smilin’ Bob is still available on the Enzyte website. ENZYTE, http://www.enzyte.com (last visited Mar. 13, 2011).
38 The study, published in a number of men’s interest magazines and referenced in radio advertisements and on the company website, claimed that “over a three-month period, 100 English-speaking men who took Enzyte experienced a 12 to 31% increase in the size of their penises.” Warshak, 631 F.3d at 277. A Berkeley employee, James Teegarden, later testified that Warshak instructed him to fabricate the survey with numbers he “plucked . . . out of the air.” Id.
39 Though Berkeley boasted a 96% satisfaction rating for Enzyte, Teegarden testified that this, too, was bogus. Id. Warshak had his employee “harvest 500
fictitious doctors that supposedly developed the drug. Berkeley employed the use of a continuity or negative-option auto-ship program to distribute their products, but customers were neither given notification of their enrollment nor required to authorize the additional charges. Customers that attempted to obtain a refund were forced to deal with Berkeley’s refund policy to “make it as difficult as possible.” Additionally, Berkeley scammed their credit-card processors and the merchant banks from which they

40 Dr. Fredrick Thomkins, “a physician with a biology degree from Stanford,” and Dr. Michael Moore, “a leading urologist from Harvard,” were credited in print and radio advertisements for the development of Enzyte. Id. Unfortunately for Berkeley, investigators who contacted the alleged doctors’ alma maters found that neither man existed. Id.

41 After a customer ordered a free trial of a product, he would continue to receive shipments—and credit card charges—until he opted out. Id. at 277–78. “The shipments and charges would continue until the customer decided to withdraw from the program, which required the customer to notify the company.” Id.

42 After over 1,500 complaints to the Better Business Bureau, Berkeley claimed to have added disclosure language into their sales scripts and changed their notification policies, but the evidence suggests these measures were superficial at best. Id. at 278–79. In some instances, customers were enrolled in the auto-ship program after explicitly declining:

For example, in November 2003, Berkeley hired a company called West to handle “sales calls that were from . . . Avlimil or Enzyte advertisements.” During the calls, West’s representatives asked customers if they wanted to be enrolled in the auto-ship program, and over 80% of customers declined. When Warshak learned what was happening, he issued instructions to “take those customers, even if they decline[d], even if they said no to the Auto-Ship program, go ahead and put them on the Auto-Ship program.” A subsequent email between Berkeley employees indicated that “all [West] customers, whether they know it or not, are going on [auto-ship].” As a result, numerous telephone orders resulted in unauthorized continuity shipments. Id. at 279.

43 Id. at 280 n.10. Some customers were even told they would have to present a notarized statement indicating that they had seen “no size increase,” based on the “admittedly ingenious idea” that customers would be too embarrassed to obtain such a notarization. Id.
obtained their lines of credit by falsifying applications and using elaborate ploys to keep Berkeley’s chargeback ratio artificially low. Eventually, these questionable practices led to the September 2006 grand jury indictment of Warshak, Harriet, and others on a combined 112 counts, including conspiracy to commit mail, wire, and bank fraud; mail fraud; bank fraud; making false statements to banks; money laundering; misbranding; and conspiracy to obstruct a Federal Trade Commission (“FTC”) proceeding.

In the process of obtaining evidence to support these charges, government agents became interested in emails stored with Warshak’s ISP, NuVox. In October 2004, operating under section 2703(f) of the SCA, the government formally requested

After having an account terminated with the Bank of Kentucky, Warshak often used his mother to apply for merchant accounts at other banks, falsely listing her as CEO and 100% owner of Berkeley. Id. at 280. Other times, Warshak would falsify applications by claiming he had never been previously terminated from a merchant account. Id.

A chargeback, occurring when a customer contacts the credit card company and successfully disputes a charge, is undesirable for merchant banks, representing increased financial risk from the merchant company. Id. at 279–80. Typically, if chargebacks result from more than 1% of a merchant company’s transactions, their account will be terminated. Id. at 280. Berkeley used a strategy called “double-dinging,” in which they split up a single transaction into multiple charges, in order to inflate the denominator (the number of transactions) of their chargeback ratio. Id. at 280. Other times, they would charge and then refund randomly selected customers, blaming a “computer glitch” if anyone complained. Id. at 281.

The 112 charges were spread amongst the three defendants in this case (Steven Warshak, owner and operator of Berkeley, Harriet Warshak, the mother of Steven and an employee of Berkeley, and TCI Media, Inc., another company owned by Steven), as well as “several others with various crimes related to Berkeley’s business.” Id.

18 U.S.C. § 2703(f) (2006). Section 2703 regulates compelled disclosures of stored communications. Specifically, § 2703(f) lists the requirements to preserve evidence:

(1) In general.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

Id.
that NuVox preserve all of Warshak’s future incoming and outgoing emails. In subsequent months, NuVox preserved copies of approximately 27,000 of Warshak’s emails without his knowledge or permission, pursuant to the government’s directive.

After obtaining a subpoena under the SCA in January 2005, the government compelled NuVox to turn over the emails it had begun preserving in October 2004, as well as any additional emails in Warshak’s account, a total of approximately 27,000 emails. Warshak did not receive notice of the subpoena or of the corresponding preservation of his emails until May 2006.

Warshak’s subsequent motion to exclude the emails obtained from NuVox from being used as evidence was denied, freeing the government to use them at trial. The contents of the emails turned over to the government contained “sensitive and sometimes damning substance” which was used to convict the defendants on the majority of the 112 charges, including mail fraud, bank fraud, and money laundering. Warshak was sentenced to twenty-five years imprisonment and ordered to pay $459,450,000 in proceeds-money-judgment forfeiture, $44,876,781.68 in money-laundering-

---

49 Warshak, 631 F.3d at 283. Warshak accessed his emails using Post Office Protocol ("POP"), in which emails are generally deleted from the ISP server when they are downloaded to the subscriber’s personal computer. Id. at 283 n.14.

50 Id.

51 These “additional emails” were obtained pursuant to an ex parte court order under § 2703(d) of the SCA. See 18 U.S.C. § 2703(d).

52 Warshak, 631 F.3d at 283.

53 Id.

54 Id. at 281.

55 Id. at 284.

56 Id. at 281. Warshak was acquitted of fifteen of these charges, including making false statements to banks and misbranding offenses. Warshak’s mother, Harriet, was also acquitted of making false statements to banks. Id.
The defendants appealed the district court ruling to the Sixth Circuit. 58

57 Id. at 281–82. Harriet was held jointly and severally liable for both of the forfeiture judgments, sentenced to twenty-four months in prison, and made to pay an $800 special assessment. TCI was put on probation for five years and fined $160,000 with a special assessment of $6,400. Id.

58 While the 112-count indictment was awaiting trial, Warshak brought a civil suit against the government for the warrantless seizure of his emails in June 2006, seeking declaratory and injunctive relief. See Warshak v. United States, 490 F.3d 455 (6th Cir. 2007) [hereinafter Warshak I]; Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (rehearing en banc granted, opinion vacated, Oct. 9, 2007) [hereinafter Warshak II]. At trial, the United States District Court for the Southern District of Ohio granted Warshak’s request for injunctive relief, preventing the government from conducting unwarranted searches until final disposition of the case. Warshak I at 461. Following the government’s appeal of the injunction, the Sixth Circuit Court of Appeals heard the Warshak civil case. Finding the arguments advanced by amici curiae briefs convincing, the Sixth Circuit acknowledged the analogy between the recognized privacy interests in telephone conversations and those in the content of emails. Warshak I at 469–70. Like phone conversations and postal mail, the court reasoned that the content of email is a form of private communication that the user seeks to preserve as private, thus warranting constitutional protection:

Turning to the instant case, we have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user “seeks to preserve as private,” and therefore “may be constitutionally protected.” It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past. Warshak I at 473 (citing Katz v. United States, 389 U.S. 347 (1967)). The court ruled that Warshak did have a valid privacy interest in the contents of his stored emails, an interest protected by the Fourth Amendment. See Warshak, 631 F.3d at 282 n.12; see also Bankston, supra note 14 (“There the 6th Circuit agreed with [the] EFF that email users have a Fourth Amendment-protected expectation of privacy in the email they store with their email providers. . . .”). A rehearing en banc, however, vacated that decision due to lack of ripeness. Warshak II at 523.
B. Warshak's Criminal Conviction Appeal to the Sixth Circuit Court of Appeals

On appeal, Warshak argued—among other things—that the ex parte seizure of his emails without a warrant was a violation of his Fourth Amendment rights. In response, the government claimed that any Fourth Amendment violations that did occur were "harmless." Additionally, the government claimed that the search and seizure of Warshak's emails was protected through its good faith reliance on the SCA.

In a decision applauded by many civil liberties groups, the Sixth Circuit held that Warshak's Fourth Amendment rights had been violated by the government's warrantless seizure of his email. By compelling NuVox to turn over the contents of Warshak's emails and taking possession thereof, the government violated what the court found to be a reasonable expectation of privacy in stored emails.

The court analogized stored emails to other forms of communication already protected. Referring to Katz v. United States and United States v. Jacobsen, the Sixth Circuit considered the "expectation of privacy" analysis the Supreme Court previously used to apply Fourth Amendment protections to traditional forms of communication. In Katz, the Court found that telephone users were "surely entitled to assume that the words . . . uttered into the mouthpiece would not be broadcast to the world," leading to a holding that has brought telephone

---

59 Warshak, 631 F.3d at 282.
60 Id.
61 Id.
62 See, e.g., Bankston, supra note 14.
63 Warshak, 631 F.3d at 282.
64 Id. at 285.
67 Warshak, 631 F.3d at 284.
conversations fully under the shelter of the Fourth Amendment.\footnote{Warshak, 631 F.3d at 285 (citing Smith v. Maryland, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting)).} Extending this doctrine, the Jacobsen court found that “[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy,”\footnote{United States v. Jacobsen, 466 U.S. 109, 114 (1984).} based on the premise that a search arises any time the government “infringes upon ‘an expectation of privacy that society is prepared to consider reasonable.’”\footnote{Warshak, 631 F.3d at 284 (citing Jacobsen, 466 U.S. at 109).}

The existence of a reasonable expectation of privacy for emails thus rests on two questions, requiring the court to analyze both the Warshak fact pattern and the relationship between society and email communication.\footnote{Freiwald, supra note 11 (summarizing the subjective and objective expectations of privacy analysis undertaken by the Sixth Circuit).} In other words: (1) did Warshak, as the subject of the search in question, manifest a subjective expectation of privacy; and (2) was this expectation of privacy one that society at large would recognize as reasonable?\footnote{See Warshak, 631 F.3d at 284; Katz 389 U.S. at 361 (Harlan, J., concurring).}

Looking first at Warshak’s subjective expectation of privacy regarding his email account, the court succinctly found that it was “highly unlikely” that he expected his email would be made public due to its content, described as “often sensitive and highly damning.”\footnote{Warshak, 631 F.3d at 284.} Turning to the question of society’s acceptance of such an expectation of privacy as reasonable, the court first recognized that “[m]uch hinges . . . on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber’s emails without triggering the . . . Fourth Amendment[,]” given that access to an individual’s email account would give the government “the ability to peer deeply into his activities.”\footnote{Id.} Quoting an article by Professors Susan Freiwald and Patricia L. Bellia, the court concluded that “[g]iven the fundamental similarities between email and traditional forms of
communication, it would defy common sense to afford emails lesser Fourth Amendment protection.  

Highly influential to this conclusion was the indispensable role of email in American society today, requiring that it be joined with other “essential” forms of private communication under the protection of the Fourth Amendment.

Despite finding that government agents had invaded Warshak’s reasonable expectation of privacy and violated his Fourth Amendment rights, his appeal for an exclusionary remedy was denied. Following previous decisions involving the SCA and Fourth Amendment challenges, reversal was found “unwarranted” on the grounds that the “agents relied on the SCA in good faith” believing it to be within the bounds of the Constitution, and thus the exclusionary rule did not apply.

---

76 Id. at 285–86 (citing Patricia L. Bellia & Susan Freiwald, Fourth Amendment Protection for Stored E-mail, 2008 U. CHI. LEGAL F. 121, 135 (2008) (urging an elimination of unreasonable differences between the treatment of email and other protected forms of communication)). The court did not elaborate on what these “fundamental similarities” between email and traditional forms of communication might be, though they did go on to say that “[e]mail is the technological scion of tangible mail.” Warshak, 631 F.3d at 285–86.

77 Warshak, 631 F.3d at 286.

78 Id. at 288–89. Petitions for rehearing en banc of the Warshak case were denied by the Sixth Circuit upon a finding that “the issues raised in the petitions were fully considered upon the original submission and decision of the cases.” U.S. v. Warshak, Nos. 08-3997/4085/4087/4212/4229/09-3176, 2011 U.S. App. LEXIS 5007, at *1-2 (6th Cir. Mar. 7, 2011).

79 Warshak, 631 F.3d at 282. Good faith reliance is used as an exception to the exclusionary rule where an agent acts in “objectively reasonable reliance upon a statute that is later found unconstitutional,” based on the idea that penalizing the agent for a legislative error does not serve the exclusionary rule’s goal of deterring Fourth Amendment violations. Id. at 333–34 (Keith, J., concurring) (citing Illinois v. Krull, 480 U.S. 340, 350 (1987)).

80 Id. Warshak’s convictions as well as those of his company were affirmed, as were the forfeiture judgments against him. All of Harriet’s convictions were affirmed except for conspiracy to commit money laundering and money laundering, which were reversed. The proceeds-money forfeiture judgment against Harriet was affirmed, but her money-laundering forfeiture judgment was reversed. The sentences of Warshak and Harriet were vacated and remanded for resentencing. Id. at 333.
IV. DOES WARSHAK UNDERSCORE THE NEED FOR CONGRESSIONAL REVISION OF THE SCA?

A. Misuse of the SCA in the Warshak Investigation

One of the more contested issues in the Warshak search was the government’s use of the SCA to request that NuVox prospectively preserve emails.\(^81\) The SCA is considered by many to regulate only retrospective surveillance of communications,\(^82\) leaving the Wiretap Act and the Pen Register statute to regulate prospective communication.\(^83\) Section 2703(f) of the SCA, on which the government agents relied to request preservation of Warshak’s emails, explicitly states that a service provider shall take “all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.”\(^84\) By its plain language, section 2703(f) permits only the preservation of emails in the possession of the service provider when the request is made, not the prospective preservation of future emails used in the Warshak investigation.\(^85\) Government agents wishing to compel such prospective surveillance should “comply with the [Wiretap Act and the Pen/Trap statute].”\(^86\)

As NuVox was, by definition, a remote computing service,\(^87\) any emails stored with them could have been obtained via warrant, an administrative subpoena, or a court order.\(^88\) However, the emails retrieved by the government under the SCA, via their May

\(^{81}\) Id. at 283.

\(^{82}\) KERR, supra note 18, at 256 (“[T]he SCA deals with retrospective surveillance instead of prospective surveillance.”) (emphasis added). But see Warshak, 631 F.3d at 290, note 21 (stating that “some courts and commentators have suggested that § 2703(f) applies only retroactively . . . . However, the language of the statute, on its face, does not compel this reading.”).

\(^{83}\) See supra text accompanying note 19 on the Wiretap Act and the Pen Register statute.


\(^{85}\) Warshak, 631 F.3d at 335 (Keith, J., concurring).

\(^{86}\) Id. at 335, citing U.S. Dept. of Justice, supra note 27, at 139.


\(^{88}\) Id. See also supra text accompanying note 29.
2005 _ex parte_ court order, were actually _copies_ of Warshak’s emails made by NuVox as a direct result of the October 2004 formal request for prospective preservation; in other words, these emails would have been deleted from the NuVox server, and thus would not have been in storage for the requisite 180 days, had the preservation order to maintain all prospective emails not been made by the agents.89

This has led some to believe that the SCA was, at best, misinterpreted or, at worst, abused. In an amicus brief, the Electronic Frontier Foundation (“EFF”) argued that:

[The government] blatantly exceeded the scope of the SCA and violated the Wiretap Act, . . . by secretly compelling NuVox to prospectively “preserve” Warshak’s emails, emails that the government later obtained improperly and without a probable cause warrant using the SCA’s procedures. Put simply, the government misused the SCA to conduct a “back door wiretap” of Warshak’s emails and bypass the Wiretap Act’s strict requirements, including its requirement of probable cause.90

In a concurring opinion, agreeing with both the results and the application of the good faith exception to the exclusionary rule, Judge Keith expressed similar concerns to the methods used:

In practice, the government used the statute as a means to monitor Warshak after the investigation started without his knowledge and without a warrant. Such a practice is no more than back-door wiretapping. I doubt that such actions, if contested directly in court, would withstand the muster of the Fourth Amendment . . . . To interpret § 2703(f) as having both a retroactive and prospective effect would be contrary to the purpose of the statute as a whole . . . . [A] policy whereby the government requests emails prospectively without a warrant deeply concerns me. I am furthermore troubled by the

---

89 Warshak, 631 F.3d at 335 (observing that “the provider would have destroyed Warshak’s old emails but for the government’s request that they maintain all current and prospective emails for almost a year”). See also _supra_ text accompanying note 49 (explaining that the emails would have been deleted from the ISP server once Warshak downloaded them to his personal computer, thus, had no copies been made pursuant to the prospective preservation order, the emails would not have been available on the NuVox server).

90 Bankston, _supra_ note 14. Presumably, as the Wiretap Act prohibits “real-time interception of . . . computer communications,” it would prevent government agents from simply intercepting Warshak’s emails as they were received by NuVox. _Kerr, supra_ note 18, at 461.
majority’s willingness to disregard the current reading of § 2703(f) without concern for future analysis of this statute.91

The belief that the government has been able to conduct secret, warrantless seizures of email has led many to call for the SCA to be reevaluated and updated to reflect the holding of the Sixth Circuit in *Warshak*, requiring warrants for the seizure of stored emails.92 Civil rights groups such as the Digital Due Process Coalition93 and the Electronic Frontier Foundation94 have used the *Warshak* investigation as a rallying cry, supplying Congress with suggested reforms and submitting *amicus curiae* briefs to the Sixth Circuit in support of Fourth Amendment protection.95

B. Twenty Four Years of Changing Technology: The Need for Congressional Reform

Though the SCA currently has strong restrictions and requirements for interception, the *Warshak* case brings to light a glaring loophole. Government agents’ use of the SCA to command preservation of emails not yet created is not only violative of the Act’s overarching mission96 but would likely fail under Fourth Amendment scrutiny if directly contested.97 As noted

---

91 *Warshak*, 631 F.3d at 335 (Keith, J., concurring). Judge Keith further explains that he agrees with the majority’s holding that the evidence should not be excluded, as it fell within the good faith exception to the exclusionary rule. *Id.* at 336.

92 *Id.* at 288.


94 See generally *Our Work*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/work (last visited Mar. 28, 2011) (“EFF is the leading civil liberties group defending your rights in the digital world.”).

95 See, e.g., Bankston, supra note 14; Freiwald, supra note 11 (calling for Congressional reform of the “unconstitutional Stored Communications Act”).

96 *Warshak*, 631 F.3d at 335 (Keith, J., concurring) (stating that the purpose of the Stored Communications Act is to “maintain the boundaries between a citizen’s reasonable expectation of privacy and crime prevention in light of quickly advancing technology”).

97 *Id.* “I doubt that such actions, if contested directly in court, would withstand the muster of the Fourth Amendment.” *Id.* Though the majority
by Judge Keith in his concurring opinion, the practice was “no more than back-door wiretapping,” as the statute was used to monitor the defendant’s email without his knowledge and without a warrant. 98

If the purpose of the SCA is, as Judge Keith stated, “to maintain the boundaries between a citizen’s reasonable expectation of privacy and crime prevention in light of quickly advancing technology,” then *Warshak* is a clear example of the need for modification and fortification of the protective restrictions of the statute. 99 The SCA is limited, in its body, to requiring service providers “to preserve records and other evidence in its possession pending the issuance of a court order or other process.” 100 Nothing in the statute permits prospective email interception without a proper warrant, a conclusion supported by the *Warshak* court. Thus, an essential first step in mending the loopholes of the statute would involve expressly forbidding the practice of prospective preservation, through Congressional amendment to the SCA. The constitutional boundaries need to be clearly laid out, putting an end to the “good faith” reliance loophole around the exclusionary rule, used by the Sixth Circuit in *Warshak*. 101

The prospective reforms need not end there. The Digital Due Process Coalition has put together proposals for Congressional review of the federal surveillance statutes, spurred by the need for greater transparency, better notice requirements, and more serious

acknowledges the existence of a potential statutory violation, noting the preclusion of the SCA to prospective preservation in the Department of Justice’s own computer-surveillance manual, they state that “this statutory violation, whether it occurred or not, is irrelevant to the issue of good faith reliance.” 102

98 *Id.* at 335.
99 *Id.*
101 Although the good faith exception was applied in *Warshak*, the majority noted that the loophole is effectively closed after their decision, stating “[o]f course, after today’s decision, the good-faith calculus has changed, and a reasonable officer may no longer assume that the Constitution permits warrantless searches of private emails.” *Warshak*, 631 F.3d at 289 n.17.
Though the warrant requirement now applies to email in the Sixth Circuit, a congressional amendment could quickly bring the rest of the nation up to speed, saving judicial resources and expediting the process of patching a statute now found to be, at least in part, unconstitutional.103

It is no surprise that the SCA is in dire need of updating. In 1986, when the statute was passed, computer networking was "in its infancy."104 Enacted before the "advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994," the SCA "is best understood by considering its operation and purpose in light of the technology that existed in 1986."105 Though the SCA remains, overall, good law, its application to modern computing will involve "extracting operating principles from a tangled legal framework."106 Over twenty-four years of technological advances suggest that a statute intended to address cutting age technology in 1986 is just not going to cut it today.

V. WHERE TO GO FROM HERE: THE APPLICATION OF WARSHAK OUTSIDE THE SIXTH CIRCUIT

The Warshak decision is a monumental victory for constitutional privacy advocates and a crucial first step towards federal protection of stored email. However, it is essential to note that, at this time, the decision is only binding within the four states

102 Freiwald, supra note 11 (calling for greater reforms such as "greater transparency, notice to users, and meaningful remedies").
103 "[T]o the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." Warshak, 631 F.3d at 288.
105 Id. at 971 n.15. See also Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (stating that "the difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web").
106 Robison, supra note 104, at 1204–05.
comprising the Sixth Circuit. With no cases on point in other circuits and the likelihood of an impending appeal, it remains unclear how the rest of the nation will treat the *Warshak* decision. Will other circuits follow *Warshak*'s rejection of the SCA as “inconsistent with the Fourth Amendment?”

One of the most efficient ways to broaden Fourth Amendment protection to the rest of the nation would be for the Supreme Court to grant certiorari. Should the Supreme Court uphold the Sixth Circuit and find a protection, it would ensure that the same protections would be applied in all jurisdictions, guaranteeing vital uniformity. Alternatively, the issue could be addressed by each of the remaining eleven circuit courts. Though this could lead to standardized results, individual circuit opinions risk the occurrence of a circuit split, with different standards and tests arising in each circuit. Additionally, the good faith exception would continue to exist in each circuit until a similar case is heard and decided, creating the potential for future “backdoor wiretapping.” The potential lack of uniformity would undoubtedly cause confusion in an area of law that already has a high potential for misunderstanding, making a more uniform approach highly favored. Thus, Congressional amendment of the SCA or Supreme Court review appears to be, for now, the most favorable scenarios for extending *Warshak* nationwide.

---

108 Freiwald, *supra* note 11 (acknowledging the uncertainty of both an appeal and the result of a prospective appeal).
110 Of course, there is also the possibility that the Supreme Court would reverse *Warshak*, similar to the possibility of a reversal upon a rehearing en banc.
112 See *supra* note 28 (discussing the complexity of the ECPA).
VI. CONCLUSION

In his *Olmstead v. United States*\textsuperscript{113} dissent, Justice Brandeis made one of the most frequently quoted comments\textsuperscript{114} on privacy:

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment . . . . Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.\textsuperscript{115}

Although email was not one of the sanctities the Supreme Court might have considered in 1928, Justice Brandeis's comment recognizes that future “privacies of life” would become important as society advanced, necessitating continued expansion of Fourth Amendment protection as new types of “sanctities” and new methods of communication arose.

The *Warshak* decision underscores the importance of keeping the Fourth Amendment in pace with our progressive technology. In a world of cloud computing and Google, the concept of an individual’s “papers and effects” is rapidly evolving.\textsuperscript{116} The question of whether the law can keep up remains to be seen.\textsuperscript{117} “If courts are still struggling with electronic mail, how will they


\textsuperscript{114} Linder, supra note 1 (stating “[t]he most frequently quoted statement by a Supreme Court justice on the subject of privacy comes in Justice Brandeis’s dissent in *Olmstead v. U.S.*”).

\textsuperscript{115} *Olmstead*, 277 U.S. at 478–79 (Brandeis, J., dissenting).

\textsuperscript{116} Bagley, supra note 9, at 153.

\textsuperscript{117} Shockley, supra note 109.
address the challenges presented by mobile devices, ubiquitous internet access and cloud computing?"118

The most effective approach will likely be for the courts to tackle these issues one by one as they prove to be problematic, resolving each question in a way that provides both useful guidance and necessary flexibility for resolving future technological legal dilemmas. For now, privacy advocates will have to await the final word on the expectation of privacy with stored emails, in order to determine if the Fourth Amendment will one day apply to everyone’s inbox.

118 Id.