I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

ERIN E. WRIGHT*

The Right to Privacy in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of *Warshak v. United States*

Abstract: This note examines the Fourth Amendment and statutory protections accorded to private electronic communications. While the Fourth Amendment provides some protection for these actions, its scope is largely undefined as technological and societal expectations of privacy change. Due to this uncertainty, Congress enacted the Electronic Communications Privacy Act to fill the constitutional "gap" left by the Fourth Amendment's protection. In 2007, the Fourth Amendment and the ECPA were at the forefront of news and debate. A seminal United States Court of Appeals for the Sixth Circuit decision, *Warshak v. United States*, squarely examines both protections and evinces perhaps a new era with regard to private electronic communications.

* Erin E. Wright is a Juris Doctor candidate at The Ohio State University Moritz College of Law, Class of 2008. She earned a Bachelor of Arts degree, *magna cum laude with Honors* in political science and a minor in psychology from The Ohio State University.

I. INTRODUCTION

The Fourth Amendment to the United States Constitution guarantees "[t]he right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[1] Memorialized by the United States Supreme Court as the "right to be let alone," Americans widely consider the Fourth Amendment to be both comprehensive and highly valued.[2] This Amendment reflects the Framers' recognition that certain aspects of an individual's life should be free from government intrusion.[3] While a person's home and personal belongings are traditionally protected, whether an individual's private electronic communications are entitled to Fourth Amendment protection remains relatively undefined. Electronic communications most notably include e-mail, but they can also include other forms such as text messaging.[4] For Fourth Amendment purposes, electronic communications can be considered modern-day "papers and effects."[5]

Recent government searches and seizures of privately held electronic communications and files have made national headlines and have spawned international debate. Notably, as the War Against Terror progressed, the Bush Administration sought to protect the United States from future terrorist attacks when it authorized the Terrorist Surveillance Program ("TSP").[6] This National Security Agency ("NSA") program monitored telephone calls and Internet communications between the United States and other countries without

---

[1] U.S. CONST. amend. IV.

[2] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[3] Oliver v. United States, 466 U.S. 170, 178 (1984).

[4] *See* Quon v. Arch Wireless Operating Co., Inc., 309 F. Supp. 2d 1204, 1209 (C.D. Cal. 2004).

[5] Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1586 (2004); *see* Am. Civil Liberties Union v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd* 521 U.S. 884 (1997).

[6] Letter from Alberto Gonzales, Att'y Gen., to Patrick Leahy, Chairman, S. Judiciary Comm., (Jan. 17, 2007), *available at* http://news.findlaw.com/ cnn/docs/doj/ag11707fisaltr.html [hereinafter *Letter from Alberto Gonzales*].

obtaining search warrants; the United States believed its policy was both right and justified because someone on either side of the phone was believed to be linked to al Qaeda.[7]

However, in August 2006, a federal district court in Michigan held that the TSP violated the Fourth Amendment and was, therefore, unconstitutional.[8] Five months later, in January 2007, then-Attorney General Alberto Gonzales announced that the warrantless TSP had been placed under the review of the Foreign Intelligence Surveillance Court ("FISC"), a court that specializes in wiretap requests.[9] Under this new jurisdiction, the government is able to target international communications after a FISC judge issues an order based on the finding that "there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization."[10]

Fourth Amendment issues arose in 2007 in popular American sports culture as the government engaged in arguably warrantless searches of private electronic files. Federal authorities investigated the use of performance-enhancing drugs by Major League Baseball ("MLB") players, which began shortly after team owners called for confidential testing following congressional hearings whereby several high-profile MLB players denied such use.[11] The existence of the test results enabled federal investigators to obtain a search warrant to search the files of ten named players at the participating drug testing laboratories. During the search, federal agents seized paper and electronic data related to those ten players subject to the warrant, but also obtained intermingled incriminating data of 104 other MLB

---

[7] Dan Eggen, *Court Will Oversee Wiretap Program*, WASH. POST, Jan. 18, 2007, at A1, *available at* http://www.washingtonpost.com/wpdyn/content/article/2007/01/17/AR2007011701256.html.

[8] Am. Civil Liberties Union v. Nat'l Sec. Agency, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006); *see also* United States v. U.S. Dist. Ct. for the E. Dist. of Mich., 407 U.S. 297 (1972) (holding that prior judicial approval was required for certain types of domestic security electronic surveillance).

[9] *See Letter from Alberto Gonzales*, *supra* note 6; *see also* Eggen, *supra* note 7.

[10] *Letter from Alberto Gonzales*, *supra* note 6.

[11] Adam Thompson, *Is Baseball Drugs Ruling a Fourth-Amendment Foul?*, WALL ST. J., Jan. 16, 2007, http://online.wsj.com/public/article_print/SB116891199049077225-9a1pzT2nNQfzm_dX9Jr3KIfn8s0_20070214.html.

players not specified in the warrant.[12] The data seized included the results from 1,438 tests from 2003, as well as medical records of participants in "13 other 'major sports organizations,' three unaffiliated businesses and three sports competitions."[13]

The search calls into question "how much freedom the government has to pursue crimes discovered in electronic files while searching for evidence against other people."[14] In December 2006, the United States Court of Appeals for the Ninth Circuit ("Ninth Circuit") held that the government's search and seizure of the computer files did not violate the unnamed MLB players' constitutional rights. The Court found that the government respected the players' privacy when it acted pursuant to a warrant to investigate the ten named players' illegal steroid use while simultaneously seizing paper and electronic data of those players not listed in the warrant.[15]

As these controversies demonstrate, the right to privacy in electronic communications and files is of widespread interest and of profound importance. Part II of this note considers the Fourth Amendment's protection regarding the search and seizure of physical and virtual personal effects. By examining current constitutional jurisprudence, this note seeks to extrapolate the limits of Fourth Amendment protection with respect to electronic communications. Part III discusses the statutory protection of electronic communications, which was intended to compensate for the narrow interpretation accorded to the Fourth Amendment in circumstances where the communication is revealed to a third party. Part IV of this note provides in-depth analysis of the seminal 2007 United States Court of Appeals for the Sixth Circuit ("Sixth Circuit") decision regarding electronic privacy, *Warshak v. United States*,[16] which squarely confronted unaddressed Fourth Amendment and Electronic Communications Privacy Act ("ECPA") issues.

---

[12] *Id.*; *see also* Bob Egelko, *100 Big-Leaguers Steroid-Positive in 2003 Season; Court Rules Federal Prosecutors Can Use Tests for Investigation,* S.F. CHRON., Dec. 28, 2006, at B1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/12/28/BAGL8N95J51.DTL.

[13] Egelko, *supra* note 12; United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 932 (9th Cir. 2006); *see also* Thompson, *supra* note 11.

[14] Thompson, *supra* note 11.

[15] *Comprehensive Drug Testing, Inc.*, 473 F.3d at 938.

[16] Warshak v. United States, 490 F.3d 455 (6th Cir. 2007).

II. FOURTH AMENDMENT PROTECTION OF ELECTRONIC COMMUNICATIONS

A. FOURTH AMENDMENT LEGAL DOCTRINE

The United States Supreme Court has yet to determine whether, and to what extent, the Fourth Amendment protects electronic communications. As a result, lower courts and scholars alike continue to rely on a series of Supreme Court decisions from the 1960s in an attempt to extrapolate the modern scope of the Fourth Amendment's protection. In *Katz v. United States*, the most notable of the 1960s surveillance cases, the Supreme Court abandoned the traditional Fourth Amendment property-based analysis, which guarded against physical intrusion into a protected area, and held that the Fourth Amendment may be invoked when a person has a "reasonable expectation of privacy."[17] To determine whether a "reasonable expectation" exists, a court must answer two seemingly basic questions: first, does the individual exhibit a subjective expectation of privacy; and second, is society prepared to recognize that person's subjective expectation as reasonable?[18] Together, the two prongs of the "reasonable expectation of privacy" ("REP") test[19] seek to determine whether the government's intrusion violates personal and societal values.[20]

To determine whether an intrusion is constitutional, analysis centers on the reasonableness of the individual's expectation of privacy. A person may invoke the Fourth Amendment's protection when she claims a "'justifiable,' a 'reasonable' or a 'legitimate

---

[17] *Katz*, 389 U.S. at 360 (Harlan, J., concurring); *compare* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (explaining that property-based analysis has endured when it has aided government surveillance) *with* Peter P. Swire, *Correspondence: Katz is Dead. Long Live Katz.*, 102 MICH. L. REV. 904 (2004) (demonstrating that the abandonment of property-based analysis has aided government surveillance).

[18] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[19] Patricia L. Bellia, *The Fourth Amendment and Emerging Communications Technologies*, IEEE SEC. & PRIVACY, May/June 2006, at 20–28, *available at* http://www.computer.org/portal/site/security/menuitem.6f7b2414551cb84651286b108bcd45f3/index.jsp?&pName=security_level1_article&TheCat=1015&path=security/2006/v4n3&file=bellia.xml&;jsessionid=F37dpqwQSpyG2mPRhqLZVZm4yYnTDs1vhhhT9zkdPY69c9RVMByv!-1146783785.

[20] *Oliver*, 466 U.S. at 182–83.

expectation of privacy'"[21] and her assertion is validated when it is in accord with society's expectation.[22] When making this constitutional determination, no single factor controls,[23] but the Supreme Court has considered such factors as the Framers' intent,[24] the ground upon which the search was conducted,[25] societal understandings[26] and the individual's use of the thing seized.[27] Under this framework, "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interest in that property."[28]

With respect to electronic communications, the reasonableness of one's privacy expectation also turns on whether the item seized or intercepted is properly considered identification information or content information. Known also as "envelope information," identification information is normally found on the outside of a letter and no privacy expectation attaches because the postal service must view it in the course of delivery.[29] Similarly, envelope information regarding

---

[21] Smith v. Maryland, 442 U.S. 735, 740 (1979).

[22] Carroll v. United States, 267 U.S. 132, 149 (1925); *but cf.* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007) (arguing that the reasonable expectation of privacy test is "unwieldy and misguided" when applied to modern electronic communications) *and* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007) (arguing that the reasonable expectation of privacy test is "wrongheaded" when applied to third parties).

[23] *Oliver*, 466 U.S. at 177.

[24] *Id.* at 178 (citing United States v. Chadwick, 433 U.S. 1, 7–8 (1977)) (recognizing that the Framers' primary intention was to protect against home intrusion while acknowledging that the Fourth Amendment provides more expansive protections).

[25] *Id.* (citing Jones v. United States, 362 U.S. 257, 267 (1960)) (considering whether an affidavit based on information from an informant was sufficient to establish probable cause for a search warrant but ultimately holding it was not because the affiant did not set forth any personal observations but rather rested wholly on hearsay).

[26] *Id.* (citing Payton v. New York, 445 U.S. 573, 591 (1980)) (societal understanding is examined in order to consider what the Framers might have thought was reasonable).

[27] Mulligan, *supra* note 5, at 1585.

[28] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[29] Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 628 (2003).

electronic communications entails an e-mail's "to" and "from" fields, for which no expectation of privacy exists.[30] But unlike the content of a sealed letter, which is protected by the Fourth Amendment, "courts have struggled to apply the Fourth Amendment to content sent over communications networks . . . because the content of Internet communications is mixed together with envelope information and disclosed to the ISP."[31] Therefore, while it seems as though one's privacy expectation in the content of an e-mail is reasonable, society may not be prepared to recognize this expectation due to the manner in which e-mail is currently transmitted.

B. THE NARROWING OF FOURTH AMENDMENT DOCTRINE SINCE *KATZ*

The REP test enhances an individual's Fourth Amendment protection by expanding the scope of judicial analysis beyond a strictly property-based search and seizure; however, subsequent Supreme Court decisions have narrowed its breadth. Specifically, the "business records cases"[32] curtailed the reach of the REP test by collectively establishing the third party doctrine; that is, these cases held that some types of information failed to satisfy the subjective portion of the test because the individual voluntarily revealed the information to a third party.[33]

Each individual in the business records cases disclosed his personal information to a common private entity including a bank,[34] an accountant[35] and a telephone company,[36] and each maintained a subjective expectation that his information would not be shared. However, the courts determined that, in light of the surrounding circumstances, such expectations were unreasonable. Today, the third party doctrine significantly narrows courts' interpretation of the REP

---

[30] *Id.*

[31] *Id.* at 628–29.

[32] *See* Couch v. United States, 409 U.S. 322 (1973); Cal. Bankers Assn. v. Shultz, 416 U.S. 21 (1974); United States v. Miller, 425 U.S. 435 (1976); *Smith*, 442 U.S. at 735 [hereinafter *Business Records Cases*].

[33] Mulligan, *supra* note 5, at 1578.

[34] *Cal. Bankers Assn.*, 416 U.S. at 21; *Miller*, 425 U.S. at 435.

[35] *Couch*, 409 U.S. at 322.

[36] *Smith*, 442 U.S. at 735.

test, which results in significantly more document searches than would otherwise occur under a moderate or expansive interpretation.[37] Recognizing this, Professor Peter Swire has commented that the REP test "has become a sword for the government, not a shield of personal privacy."[38]

Although the REP test may limit Fourth Amendment protection in some instances, this test serves as a secondary limitation to the initial hurdle of characterizing the intruding actor. The constitutional boundaries of Internet privacy only limit government intrusion and do not restrict private individuals or entities. Therefore, a private entity's search and seizure of a user's personal e-mail is wholly outside the scope of the Fourth Amendment. Distinguishing between public and private actors, therefore, serves as an even greater limitation than the REP test.[39]

Despite the dearth of Supreme Court guidance, lower court authority is emerging regarding the scope of Fourth Amendment protection accorded to electronic communications. When making this determination, courts examine the reasonableness of the government intrusion in light of the particular facts and circumstances as they exist at that time.[40] Distinct from penetrating the home or seizing physical documents, government intrusion into technology-based effects may occur in one of three ways: the government may acquire electronic communications (1) in transmission; (2) in storage held by an Internet Service Provider ("ISP"); or (3) the government may acquire the transactional data linked with transmission or storage of the electronic communication, such as "source or destination information associated with a particular communication" like one's telephone number, e-mail message or IP address.[41]

Electronic communications in transmission may be entitled to the same Fourth Amendment protection as voice communications. The United States Court of Appeals for the Armed Forces has acknowledged, "the transmitter of an e-mail message enjoys a

---

[37] Swire, *supra* note 17, at 907.

[38] *Id.* at 910.

[39] *Jacobsen*, 466 U.S. at 133 (White, J., concurring); *see also* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 306 (2001) (acknowledging that "constitutional arguments effectively address only half the problem").

[40] *Jacobsen*, 466 U.S. at 115.

[41] Bellia, *supra* note 19.

reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."[42]

As to whether an individual has a reasonable expectation of privacy in one's stored electronic communication, *United States v. Miller* suggests that no reasonable expectation of privacy exists because the subscriber has surrendered any Fourth Amendment protection by voluntarily conveying her communications to a third party, namely her ISP.[43] However, a three-judge panel for the Sixth Circuit held otherwise in *Warshak v. United States*.[44] There, the Court held that the plaintiff maintained a reasonable expectation of privacy in his stored e-mails because the ISP did not access this information in the ordinary course of its business.[45]

Finally, regarding transactional data, Supreme Court decisions indirectly suggest that an individual is least likely to have a reasonable expectation of privacy in her envelope information because intermediaries along the way view it in order to transmit the communication to its intended destination.[46]

Today, many ISP subscribers are likely to subjectively expect that their electronic communications will remain private. Despite the likelihood of satisfying the first, subjective prong of the REP test, there are three main arguments against society's recognition of electronic communication privacy. If persuasive, any one of these arguments would cause the REP test's second prong to fail.

First, once the sender transmits a message, arguably, the user relinquishes control over the recipient's handling of it.[47] The sender's

---

[42] United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996).

[43] Patricia L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1402 (2004); *Miller*, 425 U.S. at 442; *see* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); United States v. Hambrick, No. 99-4793, 2000 WL 1062039 (4th Cir. 2000); United States v. Cox, 190 F. Supp. 2d 330 (N.D.N.Y. 2002).

[44] *Warshak*, 490 F.3d 455.

[45] *Id.* at 473–74.

[46] *See Miller*, 425 U.S. at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."); *Smith*, 442 U.S. at 743–44; *Couch*, 409 U.S. at 335; Hoffa v. United States, 385 U.S. 293, 302 (1966); *but cf.* Bellia, *supra* note 19 (arguing that Web communications reveal not only locations but also "give significant clues about th[e] file," including content that is protected under the Fourth Amendment).

[47] *See Business Records Cases*; *see also* Bellia, *supra* note 43, at 1386.

reasonable expectation of privacy is lost at the moment the recipient opens the electronic communication.[48] While the sender who forwards an e-mail to others may have a reasonable expectation of privacy upon transmission, this expectation vanishes upon receipt because the sender cannot control what the recipient chooses to do with it. The message may be forwarded on the recipient's whim without regard for the sender's privacy expectations. Likewise, communications made in chat rooms to the public-at-large "lose any semblance of privacy"[49] as do messages posted on electronic bulletin boards[50] for the same reason. Additionally, a person who voluntarily provides information to a third party via peer-to-peer networking[51] lacks any reasonable expectation of privacy because she has "essentially open[ed] the computer to the world."[52]

Second, society cannot recognize an individual sender's right to privacy because the sender relies on several third parties to transmit the message to the recipient.[53] By transmitting the electronic communication through intermediaries, the sender's original expectation of privacy is frustrated.[54] The Fourth Amendment's protection can only be invoked for an undisturbed expectation of privacy; once frustration occurs via voluntary disclosure to a third party, the Fourth Amendment does not prohibit governmental seizure of the non-private information.[55]

---

[48] Mulligan, *supra* note 5, at 1590.

[49] *See Maxwell*, 45 M.J. at 419; United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997); State v. Evers, 815 A.2d 432 (N.J. 2003).

[50] Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2007).

[51] DENNIS NICEWANDER, 17TH CIR., FLA., FOURTH AMENDMENT ASPECTS OF INTERNET COMMUNICATIONS AND TECHNOLOGY, http://www.locatethelaw.org/Searches/PDF/Expectations.pdf ("Peer-to-peer typically refers to file sharing programs . . . and once you find a desired file on the network, a direct connection is established between you and the possessor of the file and the file is transferred directly to your computer.").

[52] Recording Indus. Assn. of Am. v. Verizon Internet Serv., 257 F. Supp. 2d 244, 267 (D.C. 2003).

[53] Bellia, *supra* note 43, at 1385–86.

[54] *See Miller*, 425 U.S. at 443; *see*, *e.g., Jacobsen*, 466 U.S. at 114–19.

[55] *Jacobsen*, 466 U.S. at 117. (A package containing cocaine was shipped to the defendants by a private carrier and was damaged in transit. The carrier opened it and called federal agents who took a small sample, without a warrant, for testing. The Supreme Court held that the

Third, society may be uncomfortable recognizing an individual's right to privacy because it is warned of the omnipresent threat of the Internet's vulnerability to attack.[56] Or, society may be uncomfortable because the general public regularly uses devices that diminish one's privacy. For example, helicopters and airplanes permit overhead surveillance of one's private property but the general public flies regularly despite this blatant invasion of privacy.[57]

III. STATUTORY GAP-FILLING: THE STORED COMMUNICATIONS ACT OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

Based on the Supreme Court's precedent in the business records cases, Congress enacted legislation piecemeal to prohibit private individuals from infringing upon others' privacy rights.[58] The need for this legislation arose from two primary forces. First, law enforcement needed clearly defined standards regarding whether, and to what extent, electronic communications were protected against intrusion.[59] Second, technology had progressed to the point where "the contents of a communication could be accessed at multiple points in time, from multiple parties, and at multiple locations."[60] Congress finally

---

sealed package was an effect to which a person has a legitimate expectation of privacy; however, when an agent of a private freight carrier frustrated the individual's privacy expectation by opening the package himself and turning it over to government officials, a warrant was not required.).

[56] Bellia, *supra* note 43, at 1386.

[57] *Compare* Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that a thermal-imaging device used by a police detective to investigate whether the petitioner was growing marijuana inside his house violated the petitioner's Fourth Amendment right because the sense-enhancing technology was not "in general public use") *with* California v. Ciraolo, 476 U.S. 207, 214–15 (1986) (holding an aerial inspection by police via airplane did not violate the defendant's Fourth Amendment right because the defendant had overtly cultivated marijuana in his backyard) *and* Florida v. Riley, 488 U.S. 445, 448–50 (1989) (holding that an aerial inspection by police via helicopter did not violate the defendant's Fourth Amendment right because the defendant's marijuana cultivation was plainly visible through missing roof panels on his greenhouse).

[58] Paige Norian, Comment, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U. L. REV. 803, 811 (2003).

[59] Mulligan, *supra* note 5, at 1563.

[60] *Id.* at 1558.

delineated the scope of electronic privacy rights when it adopted the Electronic Communications Privacy Act ("ECPA") of 1986.[61]

The ECPA is arguably expansive in two respects. First, the ECPA protects an individual's privacy interest in electronic communications, storage and transactions.[62] Second, the ECPA protects individuals from government, individual and third-party intrusion.[63] As one component of the ECPA, Congress statutorily defined the scope of one's reasonable expectation of privacy in stored electronic communications when it passed the Stored Communications Act of 1986 ("SCA").[64]

Congress enacted the SCA for three main reasons: (1) it was uncertain whether an individual could retain a reasonable expectation of privacy with regard to information sent to ISPs; (2) a subpoena compelling an ISP to disclose certain sought-after information did not require probable cause; and (3) most ISPs are private entities and are able to search through stored files, that is, the Fourth Amendment prohibits neither the search nor subsequent disclosure.[65]

Although the ECPA and the SCA filled in some Fourth Amendment gaps, the SCA also permitted varying degrees of departure from the procedural stringency imposed by the Fourth Amendment. Whereas the Fourth Amendment prohibits government intrusion unless there is probable cause, the SCA identifies a range of circumstances in which law enforcement officials are authorized to access electronic communications by satisfying a lower standard.[66] Specifically, the SCA distinguishes between three types of communications that affected the government's ability to compel disclosure.[67] First, § 2703 of the SCA mandates that the government entity obtain a search warrant before obtaining communications held "in electronic storage" with an electronic communication service

---

[61] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amendment in scattered sections of 18 U.S.C.).

[62] Mulligan, *supra* note 5, at 1564.

[63] Elbert Lin, Note, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1113 (2002).

[64] Stored Communications Act of 1986, 18 U.S.C. §§ 2701–2711(2000).

[65] Mulligan, *supra* note 5, 1569–70.

[66] §§ 2701–09, 2711–12 (2000); Bellia, *supra* note 43, at 1413.

[67] *See* § 2703.

("ECS") provider for 180 days or less.[68] This section is the most stringent because government officials must demonstrate probable cause before a judge can issue a warrant.[69] When the government obtains a warrant, notice need not be given to the individual whose electronic communications are being searched.[70]

Second, § 2703 of the SCA enables the government to require a remote computing service ("RCS") provider to provide electronic storage content existing for longer than 180 days in one of three ways[71]: (1) law enforcement may obtain a search warrant compelling the RCS to disclose the information without notifying the subscriber[72]; (2) investigators may compel a third-party ISP to produce the communications via subpoena, although the government must notify the subscriber that her ISP has been subpoenaed[73]; and (3) if the government is able to evince "specific and articulable facts showing that there are reasonable grounds to believe" that the information sought to be compelled is "relevant and material to an ongoing criminal investigation," then a § 2703 court order may be issued, but like the process attached to the subpoena, the subscriber must be notified of such disclosure.[74] As a basic rule of thumb, the longer the electronic communication is in existence, the more the substantive legal protection against government access relaxes.[75]

IV. *WARSHAK V. UNITED STATES*: USHERING IN A NEW ERA OF ELECTRONIC PRIVACY PROTECTION?

The SCA is complicated and often interpreted in contradictory ways. For instance, the United States Court of Appeals for the Third

---

[68] § 2703(a).

[69] Bellia, *supra* note 19.

[70] Mulligan, *supra* note 5, at 1570.

[71] 18 U.S.C. § 2703(a)–(b) (2000); *see* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1218–19 (2004).

[72] § 2703(b)(1)(A).

[73] § 2703(b)(1)(B).

[74] § 2703(b)(1)(B)(ii) (citing §2703(d)).

[75] Mulligan, *supra* note 5, at 1570.

Circuit held that an e-mail message that had been received was in electronic storage with an RCS; thus post-transmission retrieval did not violate the SCA.[76] However, the United States Court of Appeals for the Ninth Circuit reached the opposite result.[77] Similarly, the retrieval of text messages stored for back-up protection purposes was not found to violate the SCA.[78] As these examples demonstrate, the interpretation of the SCA is much like that of the Fourth Amendment– the spectrum of judicial interpretation with regard to changing technologies varies dramatically.

Both the Fourth Amendment and the SCA were scrutinized in 2007 and a groundbreaking result was reached when one Circuit defied widespread understanding. In June 2007, the United States Court of Appeals for the Sixth Circuit single-handedly rewrote the law of Internet privacy[79] by relaxing the third party doctrine when it handed down *Warshak v. United States*.[80] The opinion largely rests on the notion that e-mail is an "ever-increasing mode of private communication, and protecting shared communications through this medium is as important to the Fourth Amendment principles today as protecting telephone conversations has been in the past."[81] Privacy advocates viewed this decision as a major victory, because it became the controlling law in the Court's jurisdiction for a period of time and because other federal jurisdictions would likely look to it for guidance.[82]

In *Warshak*, the United States was engaged in a criminal investigation of the plaintiff, Steve Warshak, for mail and wire fraud, money laundering and other related offenses in connection with his small business.[83] In 2005, a United States Magistrate Judge issued an

---

[76] Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635 (E.D. Pa. 2001), *aff'd,* 352 F.3d 107, 113–14 (3d Cir. 2003).

[77] Theofel v. Farey-Jones, 341 F.3d 978, 985 (9th Cir. 2003).

[78] *Quon*, 309 F. Supp. 2d at 1209.

[79] Posting by Orin Kerr to Volokh Conspiracy blog, http://volokh.com/posts/1182271994.shtml (June 21, 2007, 03:36 EST).

[80] *Warshak*, 490 F.3d 455.

[81] *Id.* at 473.

[82] The Sixth Circuit's jurisdiction includes Ohio, Michigan, Tennessee and Kentucky.

[83] *Warshak*, 490 F.3d at 460.

order under SCA § 2703 that required Warshak's ISPs, NuVox Communications, and Yahoo! to turn over information pertaining to his e-mail accounts, including his subscriber information, the contents of communications older than 180 days, and log files and backup tapes.[84] The order was issued under seal and disclosure to Warshak was delayed until ninety days after it occurred.[85] One year later, the government notified Warshak of both orders.

Warshak filed suit seeking declaratory and injunctive relief. He alleged that "the compelled disclosure of his e-mails without a warrant violated the Fourth Amendment."[86] When the government refused to assure Warshak that it would not seek additional SCA orders, Warshak moved for a temporary restraining order and a preliminary injunction.[87]

The United States District Court for the Southern District of Ohio found that the government violated Warshak's Fourth Amendment rights when it failed to obtain a search warrant based on a showing of probable cause.[88] It reasoned that e-mails held by an ISP were analogous to sealed letters held by the post-office and in both instances, the sender maintained an expectation of privacy.[89] Based on the merits of Warshak's constitutional claim, the district court deemed it unnecessary to reach his SCA claim.[90] The district court found that Warshak did not meet the facial challenge burden by demonstrating that the government seized his e-mails on a showing of less than probable cause.[91] Rather, the court was troubled by the government's *ex parte* authorization. Under these circumstances, the court was only willing to say that the constitutional flaws of the SCA were "facial in nature" and granted an order preliminarily enjoining all seizures of e-

---

[84] *Id.*

[85] *Id.*

[86] *Id.* at 462.

[87] *Id.* at 461.

[88] *Warshak v. United States*, 2006 U.S. Dist. LEXIS 50076, *20 (S.D. Ohio 2006).

[89] *Warshak*, 490 F.3d at 461.

[90] *Id.*

[91] *Id.*

mail in the court's jurisdiction unless notice and a hearing were administered.[92]

The United States appealed and made four substantive arguments. First, the United States argued that Warshak lacked standing to challenge future searches under the SCA because his claims were hypothetical and failed to show imminent harm.[93] Second, it argued that Warshak's claims were not ripe because he challenged future government seizures of his e-mails that were uncertain to occur.[94] Third, the United States argued that the Fourth Amendment's probable cause standard was inapplicable in the context of SCA seizures.[95] The government contended that a § 2703 court order was not a "search" within the meaning of the Fourth Amendment, but rather, was a compelled disclosure, akin to a subpoena.[96] Fourth, it argued that Warshak's claim was not the proper subject of a facial challenge to § 2703 of the SCA. As a result, the Sixth Circuit was faced directly with the question of "whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-à-vis the party who is subject to compelled disclosure–in this instance, the ISPs."[97]

The Sixth Circuit first concluded that Warshak had standing to challenge future searches pursuant to the SCA because the government had seized his e-mails in the past and he was still under investigation. Warshak's claim was not hypothetical because the government had a policy of seizing e-mails without a warrant or notice to the account holder, and, in Warshak's case, it refused to guarantee that it would abstain from future seizures.[98] Thus, Warshak was subject to imminent constitutional harm.

Warshak's claim was also ripe for adjudication, the Sixth Circuit found, because there was a substantial likelihood that the unconstitutional conduct he sought to enjoin would occur again in the future. Simply put, the government's *ex parte* approach eliminated a

---

[92] *Id.* at 462.

[93] *Id.* at 465.

[94] *Id.* at 467.

[95] *Id.* at 464.

[96] *Id.* at 468.

[97] *Id.* at 469.

[98] *Id.* at 467.

more appropriate time for judicial review. If the Court deemed his claim unripe then Warshak would have suffered continuing Fourth Amendment violations.[99]

After disposing of the government's procedural arguments, the Sixth Circuit responded to the substantive challenges. The Court held that a person maintains a reasonable expectation of privacy in one's e-mails and, as a result, the government was required to meet the Fourth Amendment's probable cause standard before it could require ISP disclosure.[100] In reaching this conclusion, the Sixth Circuit focused on two narrow questions to distinguish situations where information is shared with third parties and the person maintains a reasonable expectation of privacy from those situations where the third party doctrine applies and the individual's expectation is unreasonable. The Court first assessed with whom the information was shared compared to who was excluded, and second, whether the information shared was identification information or content information.[101]

When examining with whom Warshak's e-mails were shared, the Sixth Circuit analogized an individual's privacy interest in the content of an e-mail to one's privacy interest in the content of a telephone call, as recognized in *Katz* and *Berger*.[102] The Court refrained from making a broad assertion with regard to the third party doctrine in the context of e-mails and instead stated that the sharing of information does not "entirely erode" all reasonable expectations of privacy.[103] First, the Sixth Circuit reasoned that although a third party intermediary, such as an ISP, has *access* to the information sought by the government, mere access does not diminish one's reasonable expectation of privacy because "there is a societal expectation that the ISP or phone company will not do so as a matter of course."[104] The Court would not permit the government to "bootstrap" the intermediary's limited access to the subscriber information (in this case the IP address or, in *Katz,* the phone number) to allow it to access the content of the communication

---

[99] *Id.* at 467–68.

[100] *Id.* at 475.

[101] *Id.* at 470–71.

[102] *Id.*

[103] *Id.* at 470.

[104] *Id.* at 471.

(the content of an e-mail or the substance of a telephone conversation).[105]

Second, the Sixth Circuit reasoned that the ISP's ability to scan for child pornography and viruses was insufficient to waive the expectation of privacy in the e-mail's content.[106] The Court reasoned that scanning an e-mail for particular terms, images or similar indicia of wrongdoing would not disclose the substance of the e-mail because, like the post office, which screens packages for drugs and explosives, neither the content of the package nor the content of the e-mail is revealed.[107]

Third, the Sixth Circuit examined Warshak's facial challenge to the applicable portion of the SCA.[108] Although a facial challenge to a legislative act is "the most difficult challenge to mount" because "the challenger must establish that no set of circumstances exist under which the Act would be valid," the Sixth Circuit held that Warshak satisfied this burden.[109] The Court reasoned that when the government seizes an e-mail from an ISP without a warrant supported by probable cause, without "notice to the account holder to render the intrusion the functional equivalent of a subpoena," or without even a showing that the user waived the expectation of privacy or did not maintain one, then no set of circumstances exists for which § 2703 of the SCA would be valid.[110] The Court held the narrow, facial invalidation of the SCA was justified.[111]

The United States Court of Appeals for the Sixth Circuit ultimately held that when a user does not expect a third party to access one's e-mail in the normal course of business, "the party maintains a reasonable expectation of privacy, and subpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement."[112] On remand, the Court permitted

---

[105] *Id.*

[106] *Id.* at 474.

[107] *Id.*

[108] *Id.* at 476.

[109] *Id.* at 477.

[110] *Id.*

[111] *Id.* at 479.

[112] *Id.* at 475.

the government to seize private e-mails in electronic storage under the following circumstances: (1) by obtaining a search warrant under the Fourth Amendment; (2) by providing notice to the account holder when seeking a court order; or (3) by showing specific, articulable facts, demonstrating that the ISP or other entity has complete access to the e-mails in the normal course of its business, which demonstrates that the user has waived any expectation of privacy.[113]

In July 2007, the United States petitioned for rehearing en banc.[114] Three nonprofit organizations and three law professors filed amicus curiae briefs, but the Sixth Circuit refused to consider any amicus briefs.[115] These briefs evince the current debate surrounding this issue and the main arguments can be organized into two main camps.

On one hand, proponents such as Professor Peter Swire argue that the courts should determine the outer limits of government surveillance. Professor Swire argues that courts should define how the Fourth Amendment applies to new technologies, because not only is this the courts' proper role in government, but also judicial determinations have influenced subsequent legislation in many positive ways.[116] Professor Swire advocates for a "searching, substantive inquiry into whether a search violates a person's 'reasonable expectation of privacy.'"[117]

Should courts undertake this searching inquiry, proponents like Professors Susan Freiwald, Patricia Bellia and Deirdre Mulligan argue that courts would extend the Fourth Amendment's protection to one's personal e-mail, because users maintain a reasonable expectation of privacy in their personal e-mails, regardless of whether they are in

---

[113] *Id.* at 475–76.

[114] Brief of Respondent-Appellant, *Warshak*, 490 F.3d 455; *see also* Brief of Plaintiff-Appellee, *Warshak*, 490 F.3d 455.

[115] Posting by Orin Kerr to Volokh Conspiracy blog, http://www.volokh.com/posts.html (September 7, 2007, 14:44 EST); *see* Brief for Steven Warshak-Patricia L. Bellia & Susan Freiwald as Amici Curiae Supporting Petioner-Appellee, Warshak v. United States, 490 F.3d 455, No. 06-4092 (6th Cir. 2007); Brief for Steven Warshak-Kevin S. Bankston et. al. as Amici Curiae Supporting Petitioner-Appellee, Warshak v. United States, 490 F.3d 455, No. 06-4092 (6th Cir. 2007); Brief for the United States-Orin S. Kerr as Amici Curiae Supporting Respondent-Appellant, Warshak v. United States, 490 F.3d 455, No. 06-4092 (6th Cir. 2007).

[116] Swire, *supra* note 17, at 922.

[117] *Id.* at 931.

transmission, have already been accessed, or are in storage.[118] These advocates argue that an e-mail user maintains a subjective expectation of privacy in an e-mail so long as the user does not expose it to the public.[119] In addition, society objectively recognizes that e-mails are private because of their widespread use. Individuals use e-mail for a host of reasons, and in some instances, e-mail may be more revealing than a telephone call because the historical exchange of e-mail can reveal multiple exchanges over time whereas a phone conversation only reveals information discrete to that exchange.[120] There is no doubt that

> [o]ne who looks at our e-mails obtains a detailed view into our innermost thoughts; no previous mode of surveillance exposes more. When we compose private and professional e-mails, embed links to Internet sites in some, and attach documents, pictures, sound files and videos to others, we rely on the privacy of the medium.[121]

Proponents object to applying the third party doctrine in this instance because the user is not the one revealing its personal information to the world; rather, by the very nature of the service, the third party ISP has access to the e-mails which does not in any way eliminate one's expectation of privacy. In this instance, the ISP is a holding container that merely has access to the e-mails by transmitting them and later holding them in storage. But, proponents argue, the relationship between the user and the ISP in no way enables the government to step in and access the user's personal e-mail.[122]

Proponents argue that personal e-mails are entitled to the Fourth Amendment's protection and that the government is therefore bound by the warrant requirement. The Professors point out that "any other result would be destructive of society's ability to communicate."[123]

---

[118] Brief for Steven Warshak-Patricia L. Bellia & Susan Freiwald, *supra* note 115, at 3; *see* Mulligan, *supra* note 5, at 1592.

[119] Brief for Steven Warshak-Patricia L. Bellia & Susan Freiwald, *supra* note 115, at 4.

[120] *Id.* at 5–6.

[121] *Id.* at 10–15; *see* Mulligan, *supra* note 5, at 1594–96.

[122] Brief for Steven Warshak-Patricia L. Bellia & Susan Freiwald, *supra* note 115, at 10–15; *see* Mulligan, *supra* note 5, at 1594–96.

[123] Brief for Steven Warshak-Patricia L. Bellia & Susan Freiwald, *supra* note 115, at 6.

Opponents like Professor Orin Kerr argue that the legislature, not the courts, should determine privacy rights in the face of rapidly changing technology.[124] Professor Kerr suggests that technology continues to change, and quickly; Kerr argues that "[w]hat counts as a 'reasonable expectation of privacy' is very much up for grabs" because "no one knows whether an expectation of privacy in a new technology is 'reasonable.'"[125] The argument then goes that instead of relying on a dynamic interpretation of the Fourth Amendment, the right to privacy should be defined by Congress via statute.[126]

Professor Kerr makes three arguments regarding why Congress, rather than the courts, should determine the scope of the right to privacy in electronic communications. First, Kerr points to the fact that courts only settle matters regarding disputes that have occurred in the past; this backward looking inquiry only enables courts to decide matters regarding technologies that have long been introduced.[127]

Second, Kerr points out that courts are bound by stare decisis, which limits the judiciary's ability to change legal principles quickly in response to societal changes.[128] In contrast, the legislature enjoys broad discretion to enact new statutes or update legislation by amendment.[129] Third, Professor Kerr argues that courts have limited information before them when deciding a case, and based on this limited information, judges lack the expertise or precision to respond to novel and complicated issues surrounding modern technology.[130] In contrast, Congress has access to a wide range of inputs, which enables it to gain a comprehensive understanding of the technological facts.[131]

Professor Kerr acknowledges that he is primarily concerned with institutional incompetence when it comes to quickly changing technology, and Kerr advocates for judicial caution in the face of a rapidly changing environment.

---

[124] *See generally* Kerr, *supra* note 17.

[125] Kerr, *supra* note 17, at 808.

[126] *Id.* at 853.

[127] *Id.* at 868.

[128] *Id.* at 871.

[129] *Id.*

[130] *Id.* at 875.

[131] *Id.*

In his Brief of Amicus Curiae favoring the United States' petition for rehearing en banc, Professor Kerr operationalizes his academic arguments. He argued that the Sixth Circuit three-judge panel decided *Warshak* "with essentially no facts before" it and did so "counter to well-established limits on the judicial power."[132] Kerr expressly argued that the three-judge panel acted improperly; he implicitly stated that it did so based on limited knowledge; "[i]t reconfigured the field of e-mail privacy without even a factual hearing."[133] Instead of taking a "cautious and careful manner[ed approach] fully informed by the facts" the three-judge panel took an "all-at-once" approach, which is contrary to the proper role of the judiciary.[134]

Warshak is at the forefront of the privacy debate, and arguments supporting or criticizing the decision can be divided into two main perspectives. At the time of this writing, this matter has not yet been settled because the United States' petition for rehearing will likely be decided in the near future, at which time we may obtain a further grasp on *Warshak*'s impact on this area of law.

V. CONCLUSION

The notion of Internet privacy is still widely debated and by no means certain. Currently, an Internet user can be monitored by both "Big Brother" and "Little Brother," that is, subject to both government and private entity surveillance.[135] While the Fourth Amendment provides a general restraint on surveillance, it does not provide blanket protection regarding Internet privacy. Government actors are limited by the Fourth Amendment despite the Supreme Court's interpretation of the third party doctrine.

Congress attempted to expand this narrow coverage when it passed the ECPA, thereby protecting electronic communications from certain types of surveillance. However, as Professor Freiwald points out, the ECPA "fails to mention the World Wide Web or the Internet,"[136]

---

[132] Brief for the United States-Orin S. Kerr, *supra* note 115, at 1.

[133] *Id.* at 4.

[134] *Id.* at 9.

[135] *See* Helms, *supra* note 39, at 293; Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1395 (2001); Lin, *supra* note 63, at 1086.

[136] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 45 (2004).

which exemplifies the datedness of the Act. Although the ECPA sought to fill the "gaps" in Fourth Amendment jurisprudence relating to electronic privacy, technology has progressed to the point where the ECPA suffers from significant "gaps" of its own that were not at issue at the time of its passage.

Whether or not Internet protection expands or contracts is likely to be determined by Congress because the courts have been hesitant to squarely address these issues. Because the Judicial and Legislative branches balked at the opportunity to restrain the Executive branch and the private sector, the Executive branch has taken significant actions that call into question the adequacy of Fourth Amendment and ECPA protection. Accordingly, although the Fourth Amendment and the ECPA were intended to protect individuals from intrusions into their privacy, the need for more precise and clearly defined protection is apparent.