WARSHAK V. UNITED STATES: THE *KATZ* FOR ELECTRONIC COMMUNICATION

By Tamar R. Gubins

> *The law, though jealous of individual privacy, has not kept pace with . . . advances in scientific knowledge.*[1]
>
> *"[I]n the application of a constitution, our contemplation cannot be only of what has been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?*[2]

I. INTRODUCTION

Initially, Orin Kerr, a leading scholar in internet surveillance, referred to *Warshak v. United States* as "a rather odd case involving e-mail privacy."[3] When the Sixth Circuit handed down its opinion in June 2007,[4] he boosted his description to "blockbuster." The Sixth Circuit predominantly affirmed a district court preliminary injunction prohibiting the United States from compelling Internet Service Providers (ISPs) to disclose the contents of e-mail communication without providing notice to the account holder unless the government has obtained a warrant supported by prob-

1. Berger v. New York, 388 U.S. 41, 49 (1967).

2. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

3. Posting of Orin Kerr to The Volokh Conspiracy, Warshak v. United States, http://volokh.com/posts/1176832897.shtml (April 17, 2007, 2:53 p.m. EST).

4. Posting of Orin Kerr to The Volokh Conspiracy, Sixth Circuit Blockbuster on E-mail Privacy, http://www.volokh.com/posts/1182181742.shtml (June 18, 2007, 11:49 a.m. EST).

able cause.[5] The affirmation was based on a Fourth Amendment reading finding that an individual has a reasonable expectation of privacy in the contents of such communication, with regard to the commercial ISP that facilitated the transmission.[6] Essentially, the court held that an ISP that stores or sends e-mail is not a third party from whom electronic communication can be compelled without Fourth Amendment limitations. The Sixth Circuit partially modified the district court injunction, allowing warrantless compulsion of communication where an ISP both has a clearly stated policy of monitoring the contents of e-mails and actually does monitor them. The court reasoned that in such instances an informed user would not be able to maintain a reasonable expectation of privacy.[7]

The Sixth Circuit's opinion boldly extended Fourth Amendment protection to e-mail, an extension comparable to the protection of telephonic communication in 1967. At that time, the Supreme Court reversed forty years of precedent to find warrantless wiretapping as an unreasonable Fourth Amendment search.[8] One year later Congress passed the Wiretap Act, providing strong statutory protection for telephone conversations. Since the Wiretap Act, Congress has made a few major revisions and numerous smaller amendments to electronic surveillance laws.[9] The courts, however, have been reluctant to question statutory rules or find Fourth Amendment protection for technologies not covered by congressional acts, resulting in a contraction of such protection.[10] As a result, Americans have effectively lost Fourth Amendment privacy protection with each new development in communication technology. Additionally, Congress has been slow to expand existing statutory protections, and has not instituted meaningful new protection for electronic communications.[11] In today's political climate driven by fears of terrorism, statutory revisions are unlikely to

5. Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *reh'g en banc granted*, Warshak v. United States, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007). Having vacated the original decision in favor of rehearing en banc, the Sixth Circuit heard oral arguments on Dec. 5, 2007.

6. *Id.* at 470.

7. *Id.* at 472-73.

8. *See* Katz v. United States, 389 U.S. 347 (1967).

9. Daniel J. Solove, *The Coexistence of Privacy and Security: Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 769 (2005).

10. *See generally id.*

11. "Loose-and-low" is how one blogger refers to the burdens the Electronic Communications Privacy Act imposes on government officials before they may obtain e-mails. Posting to the Susan Crawford Blog, Boundaries, http://scrawford.net/blog/boundaries/1051/ (Nov. 16, 2007).

provide new protections—protections that judicial reinforcement of Fourth Amendment protection could, and should, provide.

Warshak raises issues of privacy in communication and how electronic communication should be regarded under the law: is it like telephonic and mailed communication, where the Fourth Amendment and statutory protections apply? Or is e-mail like a bank deposit slip, which has statutory protections created by Congress, but not Fourth Amendment protection? *Warshak* also defines who constitutes a third party for the purposes of waiving reasonable expectations of privacy.

In its June 2007 decision, the Sixth Circuit three-judge panel dismissed procedural arguments that would have enabled it to avoid the larger constitutional issues, and announced that electronic communication deserved more protection than Congress's Electronic Communications Privacy Act (ECPA) provides. The Sixth Circuit, however, vacated the opinion and reheard the case en banc in December 2007. Whether the court will repeat this important pronouncement, repudiate it, or use procedural grounds to avoid it, remains to be seen.

Part II of this Note describes the reasoning of the vacated Sixth Circuit decision in *Warshak*. Part III reviews both privacy jurisprudence and the statutory systems protecting individual privacy in communications, and surveys the varying degrees of protection for different types of communication offered by both. Part IV looks at technological changes in communication and shows how a growing share of communications is inadequately protected, reflecting the current state of statutory and jurisprudential interpretation. Part V compares the costs and benefits of protecting privacy by statute versus by case law, and argues that the courts should not always defer to Congress. This Note concludes that the Sixth Circuit and future courts should affirm the principle that the Fourth Amendment provides protection for electronic communication. Congress could then revise and pass surveillance legislation that reflects this important principle.

II. *WARSHAK*: FACTS AND PROCEDURAL HISTORY

A. Factual History and District Court Decision

In March 2005, the Department of Justice opened a fraud investigation into Steven Warshak, the owner of Berkeley Premium Nutraceuticals, Inc., a Cincinnati company that sells natural supplements purported to improve everything from energy levels to sexual performance.[12] In the course of

12. Warshak v. United States, 490 F.3d 455, 460 (6th Cir. 2007), *vacated* Warshak v. United States, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007)

that investigation, the United States obtained a sealed order from a Magistrate Judge in Ohio that required ISP NuVox Communications to provide, among other things, "'[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or entered in directories or files owned or controlled by [Warshak's accounts].'"[13] The order defined "communications not in electronic storage" to be "any e-mail communications received by the specified accounts that the owner or user of the accounts has already accessed, viewed, or downloaded."[14] In September 2005, the government was granted a second, similar order, to receive communications from Yahoo! accounts also in Warshak's name.[15] Both orders prohibited the ISP from divulging the existence or contents of the order to anyone, including Warshak.[16]

For more than a year the government monitored Warshak's communications without his knowledge; he learned of it only after a Magistrate Judge unsealed the orders.[17] Within two weeks of notification Warshak

---

(granting rehearing en banc and staying mandate); Berkeley Brands Enzyte, http://www.bpn.com/enzyte.html (last visited Apr. 6, 2008). In 2006 Warshak was indicted on 107 counts of crimes from wire fraud to money laundering. Posting of Orin Kerr to The Volokh Conspiracy, The Facts and Injunction in Warshak v. United States, http://volokh.com/archives/archive_2007_06_17-2007_06_23.shtml#1182231378 (June 19, 2007, 1:36 AM EST).

13. Warshak v. United States, No. 1:06-cv-357 2006 U.S. Dist. LEXIS 50076 at *3-4 (S.D. Ohio 2007).

14. *Id.* The government thus sought two categories of communication: (1) any opened, downloaded, or viewed communication, no matter how old, and (2) any unopened communication more than 180 days old. *Id*; The Stored Communications Act provides:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant . . . . A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) . . . .

18 U.S.C. § 2703(a) (2000 & Supp. V 2005).

15. *Warshak*, 490 F.3d at 460.

16. *Id.* The notice requirement for a § 2703(d) order can be waived by the court for up to ninety days at a time if "there is reason to believe that notification of the existence of the court order may have an adverse result . . . ." § 2705(a)(1)(A). Section 2705(a)(2) states that an "adverse result" includes "(B) flight from prosecution; (C) destruction of or tampering with evidence;" or the catch-all "(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(a)(2).

17. *Warshak*, 490 F.3d at 460-61.

filed suit against the United States, alleging that the orders and resulting seizures violated the Fourth Amendment and the Stored Communications Act (SCA), and seeking injunctive relief.[18]

The District Court granted a preliminary injunction, persuaded by Warshak's argument that an e-mail is similar to a letter or package, and thus not searchable without a warrant under the Fourth Amendment. It rejected the government's counterargument that an e-mail is more like a postcard, with no "envelope" to block prying eyes.[19] The court stated that an individual has a "reasonable expectation of privacy in his personal emails" which he does not surrender just because the communication is stored on the server of a commercial ISP.[20] The District Court issued a preliminary injunction barring the United States from seizing "the contents of any personal email account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio . . . without providing the relevant account holder or subscriber prior notice . . . ."[21]

B. Vacated Decision by Sixth Circuit Three-Judge Panel

The Sixth Circuit substantially affirmed the injunction granted by the District Court; this Section summarizes that opinion.[22] The United States

---

18. *Id.* at 461.

19. Warshak v. United States, No. 1:06-cv-357, 2006 U.S. Dist. LEXIS 50076, *13-17 (S.D. Ohio 2007).

20. *Id.* at *19.

21. *Id.* at *32. The court found that the reasonable expectation of privacy gave Warshak a likelihood of success on the merits, one of the four equitable factors used to analyze a preliminary injunction. *Id.* at 19. The other three factors, whether Warshak has shown that irreparable harm results absent an injunction, whether such an injunction would substantially harm the United States, and whether an injunction is in the public interest, were also all found to favor a preliminary injunction. *Id.* The court stressed that it is in the public's interest "to be free of unlawful government searches and seizures [because that] is a core concern of the Fourth Amendment." *Id.* at *26, *28. The District Court declined to evaluate Warshak's second assertion, the claim that the Section 2703(d) orders obtained by the United States violated the SCA. *Id.* at *20.

22. The United States made three additional claims, all of which were dismissed by the Sixth Circuit. First, that Warshak's claims lacked standing and were not ripe for adjudication because there was no specific order to get additional communication or account information. As the government had sought such orders in the past and refused to agree not to seek future orders, Warshak's concern was not entirely hypothetical and the court dismissed this argument. *Warshak*, 490 F.3d at 465-68. The government also contended that Warshak's claim could not be upheld because, in mounting a facial challenge, he would need to prove that there is no instance where the Act would be valid. The court listed examples where the rule was not as strict as the government contended, and particularly pointed to an early wiretap case where a facial challenge was upheld. *Id.* at 476-80. Lastly, the government averred that the District Court was mistaken in finding the four factors of preliminary injunction in Warshak's favor, specifically arguing that War-

argued that compelling disclosure from a third party is subject only to a general reasonableness standard, not the stricter probable cause required for a warrant, because an individual loses his expectation of privacy to information that he has voluntarily disclosed.[23] The Sixth Circuit, however, agreed with the District Court regarding reasonable expectation of privacy in the contents of electronic communication. It reasoned that although sharing information with a third party can repudiate the expectation of privacy, a commercial ISP is more like an intermediary—like a postal carrier—than a third party for purposes of Fourth Amendment seizures. If the ISP just stores or sends communication and does not routinely access or monitor it, an account holder maintains a reasonable expectation of privacy to the contents of the communication.[24]

Drawing on telephone eavesdropping cases, the court held that whether an individual maintains a reasonable expectation of privacy in e-mail stored on the server of an ISP depends on (1) with whom the communication is shared, and (2) what information is divulged.[25]

Even though a conversation is transmitted through a telephone company, an individual maintains an expectation of privacy to the content of the conversation with regard to the phone company, since the phone company is not the recipient.[26] The Sixth Circuit distinguished between information shared with a third party and information that an "intermediary . . . merely has the ability to access,"[27] concluding that the latter must have some protection. Otherwise phone conversations, packages or storage containers would have no protection simply because they were stored or sent through an intermediary.[28] Although packages or containers leave the pos-

---

shak would not suffer irreparable harm absent an injunction. The Sixth Circuit agreed with the District Court that Warshak had shown a threat of harm, and at the very least the District Court could not be said to have abused its discretion. *Id.* at 480-81.

23. Brief of Defendant-Appellant at 16-17, Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated* Warshak v. United States, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *available at* http://www.eff.org/legal/cases/warshak_v_usa/warshak_proof_reply_brief.pdf.

24. *See Warshak*, 490 F.3d 455. While the Sixth Circuit agreed that certain third parties can be subpoenaed without a search warrant, they distinguished recipients of communication from the carrier of that communication, warning that the investigated party may still have a "legitimate expectation of privacy attaching to the records obtained." *Id.* at 469 (quoting United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993)).

25. *Id.* at 470.

26. "The mere fact that a communication is shared with another person does not entirely erode all expectations of privacy." *Warshak*, 490 F.3d at 470.

27. *Id.*

28. *Id.*

session of the sender, there are societal expectations that the contents will not be inspected by the intermediary.

The kind of information transmitted is also significant: only content information is entitled to Fourth Amendment protection. In *Smith v. Maryland*, the recording of telephone numbers dialed by a user was not found to be a search, as the numbers were considered unrelated to the contents of the conversations.[29] A reasonable person would assume that phone records regularly seen by telephone company employees, and used by the company to route calls, would not be private. This is not the kind of information to which a person could have a reasonable expectation of privacy, and could be compelled by the government without probable cause. However, the scope of what can be compelled is limited to this kind of information.[30]

By analogy, there are privacy expectations to the contents of e-mails. Although an ISP has access to the communication, it is a carrier—like the post office or phone company—rather than a bona fide third party for the purposes of the third party rule as applied to the contents.[31] The determination that the ISP is not a third party with respect to e-mail contents is crucial. The government could have obtained the contents of the communication without showing probable cause or violating the Fourth Amendment had it subpoenaed a true third party, such as the recipient of the communication. But "this rationale is inapplicable where the party subpoenaed is not expected to access the content of the documents."[32] By analogy to *Smith*, the ISP was a third party with respect to the address on the e-mail, but not its contents. Absent a waiver, the government has two options to compel an ISP to disclose content: obtain a search warrant based on probable cause, or provide notice to the user.

The government argued that Warshak contracted away any expectation of privacy through user agreements and policies allowing the ISP to access e-mails. The court held that while it is possible to waive a privacy expectation, the policy must clearly state that contents will be monitored (such as the right to "audit, inspect, and monitor"), rather than provide a weak caveat that some contents might be accessed on a limited basis.[33] Warshak's user agreement was not a waiver because it merely allowed limited ac-

29. Smith v. Maryland, 442 U.S. 735 (1979).

30. *See Warshak*, 490 F.3d at 471.

31. See *infra* Section III.A.2, for a detailed explanation of the third party rule.

32. *Warshak*, 490 F.3d at 471.

33. *Id.* at 472-73 ("[M]ere accessibility is not enough to waive an expectation of privacy.").

cess.[34] But the Sixth Circuit modified the injunction to allow an ISP to be compelled to disclose e-mails without notice if its user agreement specifically called for monitoring of communication contents.[35]

On October 9, 2007, the Sixth Circuit vacated the panel decision and granted the government's petition for rehearing en banc.[36] The government's brief argued on procedural grounds that the injunction was improperly granted by the Sixth Circuit.[37] *Warshak* was reheard on December 5, 2007. On review the Sixth Circuit could avoid the Fourth Amendment constitutional issue by finding for the government on procedural grounds.

III. JUDICIAL AND STATUTORY PRIVACY PROTECTIONS

A. Fourth Amendment Jurisprudence: Reasonable Expectation of Privacy

The Fourth Amendment of the United States Constitution confers "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," unless a warrant is issued based on probable cause.[38] To determine whether or not a defendant's Fourth Amendment rights are violated, generally courts ask whether a "search" or "seizure" has occurred, and if so, if it was "reasonable."[39] Historically, "trespass or interference with property" has been deemed a search or seizure, and reasonableness has been determined on a case-by-case basis.[40] Subject to many exceptions, the general rule is that a warrantless search or seizure is invalid and the evidence recovered is inadmissible in court.[41]

---

34. *Id.* at 474; The Sixth Circuit was not persuaded that, because all ISPs monitor content for spam and viruses, users have waived their expectation to privacy. The monitoring is mechanized and content is not transmitted to employees. The court analogized that such filters were similar to screening post for explosives.

35. *Id.* at 475.

36. Warshak v. United States, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007).

37. Petition of the United States for Rehearing En Banc, Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated* Warshak v. United States, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *available at* http://volokh.com/files/Warshak_en_banc_petition.pdf.

38. U.S. CONST. amend. IV.

39. Orin S. Kerr, *Search and Seizure: Past, Present, and Future*, *in* OXFORD ENCYCLOPEDIA OF LEGAL HISTORY (forthcoming), *available at* http://ssrn/abstract=757846; *see* DANIEL J. SOLOVE, THE DIGITAL PERSON 188-89 (2004).

40. Kerr, *supra* note 39, at 6; SOLOVE, *supra* note 39, at 189.

41. SOLOVE, *supra* note 39, at 189, 192-93. A common criticism of the 1986 Electronic Communications Privacy Act is that it does not contain this suppression remedy.

The courts have given ample consideration to what constitutes an unreasonable search or seizure in the physical context of the home.[42] It is undisputed that Fourth Amendment protection from unreasonable search and seizures applies to tangible articles on private property when a law enforcement official wishes to enter the property or take items from it.[43] Less clear is what protections apply to articles outside the home, items in public view, or intangibles, like conversation. As technology changes and advances, the courts must constantly re-evaluate the boundaries of protection that the Fourth Amendment provides.[44]

While early Fourth Amendment jurisprudence focused on property rights, the fulcrum of analysis shifted to privacy in the 1960s.[45] The modern test that determines whether Fourth Amendment rights have been violated is a "reasonable expectation of privacy" test.[46] The two prongs of the test ask (1) whether one actually expected privacy, and (2) whether that expectation was reasonable.[47] As the first prong is necessarily subjective, courts usually focus on this second prong.[48]

Therefore, under the ECPA, any electronic communications that are intercepted in violation of the Act are still admissible in court. *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, 1241 (2004).

42. *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001).

43. Kerr, *supra* note 39, at 7-8.

44. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967); *Kyllo*, 533 U.S. 27 (evaluating sensory enhancement technology in light of the Fourth Amendment and holding that use of a thermal-imaging device to detect heat inside a private home, without a warrant, was an unreasonable search).

45. In the 1960s, judicial understanding of the underlying foundation of Fourth Amendment protection moved from property interests to protection of privacy. *See* Wong Sun v. United States, 371 U.S. 471, 485 (1963) ("[T]he Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.'"). *See also* Warden v. Hayden, 387 U.S. 294, 304 (1967) ("The premise that property interests control the right of the Government to search and seize has been discredited. . . . We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts."). *See generally* Kerr, *supra* note 39. However, the Supreme Court at this time cautioned that the Fourth Amendment was more than just a general right to privacy. *Katz*, 389 U.S. at 350 ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.").

46. *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring); *see* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808 (2004).

47. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[T]he rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhib-

Section III.A.1 reviews the historic shift from the property and trespass underpinnings of Fourth Amendment protection to a privacy-based understanding. Section III.A.2 sets forth the connection between privacy rights and disclosure to third parties under the modern framework.

1. Fourth Amendment Protection for Communication: From Physical Trespass to Privacy Protection.

Fourth Amendment protection for communications began with postal mail. In 1878, the Supreme Court held that letters were protected from unreasonable search and seizure, even if in the physical possession of the postal service rather than the sender or recipient.[49] In holding that sealed letters and packages were protected, the court distinguished them from unsealed mail (e.g., postcards) "purposely left in a condition to be examined" and thus not subject to protection.[50]

In the middle of the nineteenth century, the telegraph and the telephone raised new questions about the limits of warrantless surveillance. Taking up this question in the early twentieth century, the Supreme Court initially provided scant protection.

In 1928, in *Olmstead v. United States*, the Court took a narrow, property-centric view of the Fourth Amendment, finding no violation in warrantless phone tapping because it was accomplished without any physical trespass on the defendant's property.[51] While reaffirming that a government agent may not search a sealed letter traveling through the postal service as it was a physical "paper" covered by the Fourth Amendment, it held that applying the same principle to telephone conversations would "attribut[e] an enlarged and unusual meaning to the Fourth Amendment."[52]

---

ited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"); *see generally* Kerr, *supra* note 39, at 8.

48. *See generally* Dorothy K. Kagehiro et al., *Reasonable Expectation of Privacy and Third-Party Consent Searches*, 15 LAW AND HUMAN BEHAVIOR 121, 122 (1991). Not all scholars and commentators agree the Fourth Amendment should be seen in terms of privacy. *See, e.g.*, Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?* 94 COLUM. L. REV. 1751 (1994).

49. *See Ex parte* Jackson, 96 U.S. 727, 733 (1878).

50. *Id.*

51. *See* Olmstead v. United States, 277 U.S. 438, 457 (1928).

52. *Id.* at 464, 466.

Olmstead was later overturned[53] and is now most famous for Justice Brandeis' minority opinion, which is credited with establishing a constitutional right to privacy.[54] Brandeis claimed that the founders' goal for the Constitution was to impart a right to the citizenry "to be let alone" by the government, and that any "unjustifiable intrusion by the Government upon the privacy of the individual . . . must be deemed a violation of the Fourth Amendment."[55] Prophetically, Brandeis speculated that technology might someday allow the government access to private documents without having to enter a house to get them.[56] He went on to ask rhetorically, "Can it be that the Constitution affords no protection against such invasions of individual security?"[57]

After *Olmstead*, the Court shifted to a view of the Fourth Amendment right to privacy that was not based on the physical confines of the home or tangible papers.[58] The apex of this shift[59] came in *Katz v. United States*, a seminal case regarding Fourth Amendment protection in telephone conversations.[60] Katz was convicted of illegal gambling, largely based on telephone conversations he made from a public, but enclosed, telephone booth.[61] Unbeknownst to Katz, and without obtaining a warrant based on probable cause, these conversations were recorded by FBI agents by

---

53. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353 (1967), Berger v. New York, 388 U.S. 41, 51 (1967).

54. *See Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting) (claiming that the founders "conferred, as against the Government, the *right to be let alone*—the most comprehensive of rights and the right most valued by civilized men.") (emphasis added). Thirty-eight years earlier, in 1890, Brandeis and his law partner Samuel Warren had published "The Right to Privacy." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). One possible impetus for the article may have been Warren's frustration that the details of his life were often published on gossip pages. *See* DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 11 (2d ed. 2006).

55. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

56. *Id.* at 474.

57. *Id.*

58. *Compare* Goldman v. United States, 316 U.S. 129 (1942) (finding no Fourth Amendment violation in using a sound magnification device on an adjoining wall to overhear a conversation because there was no trespass) *and* Silverman v. United States, 365 U.S. 505 (1961) (finding a Fourth Amendment violation stemming from a microphone that passed through a heating duct because the microphone constituted a physical intrusion) *with* Wong Sun v. United States, 371 U.S. 471, 485 (1963) ("[T]he Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.'") *and Katz*, 389 U.S. 347.

59. Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV. 904 (2004) ("[*Katz*] is the king of Supreme Court surveillance cases.").

60. *Katz*, 389 U.S. 347.

61. *See id.* at 348.

means of a recording device placed on the outside of the telephone booth, referred to as a wiretap by the court.[62] The Supreme Court held that recording the conversations without first obtaining a warrant limiting the scope of the search was an unconstitutional search and seizure under Fourth Amendment constraints.[63]

The Supreme Court disregarded the government's claim that the phone booth was a public area not entitled to protection. Rather, the Court focused on what a person might want to keep private, regardless of the person's physical surroundings.[64] In doing so the Supreme Court took pains to define the boundaries of the Fourth Amendment broadly, stating that "the *Fourth Amendment* protects people—and not simply 'areas'—against unreasonable searches and seizures."[65]

The four decades since *Katz* have been marked by judicial limiting of the broad Fourth Amendment protections offered by that opinion.[66] The third party doctrine discussed in the next section, in particular, severely limited privacy rights by holding that information shared with another party may be compelled from that party. One commentator went so far as

---

62. *Id.* at 348.

63. *Id.* at 348, 363-64.

64. *Id.* at 351.

65. *Id.* at 353 (emphasis in original). *Katz* also sets up the reasonable expectation of privacy framework for determining if a search or seizure violates the Fourth Amendment. The two-part objective/subjective framework asks first whether an individual relied on a right to privacy, and second if such reliance was reasonable. *Id.* In his dissent Justice Black cautioned that the Court should not "rewrite the Amendment in order 'to bring it into harmony with the times' and thus reach a result that many people believe to be desirable." This is the minimalist approach taken by the majority in *Olmstead*, and exactly what Justice Brandeis cautioned against when he suggested that the Fourth Amendment should be broadened to protect rights that the founders would have wanted the Constitution to protect, even if they could not have foreseen the technological changes that threatened those rights. *Id.* at 364 (Black, J., dissenting).

66. *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976) (finding no expectation of privacy to certain banking records); Smith v. Maryland, 442 U.S. 735 (1979) (holding that no warrant was needed to collect information about dialed numbers through use of a pen register, because there is no reasonable expectation of privacy in phone numbers dialed); Fisher v. United States, 425 U.S. 391 (1976) (holding that the government may compel documents held by an attorney); United States v. Smith, 978 F.2d 171 (5th Cir. 1992) (finding that a telephone conversation held using a cordless phone, and thus involving radio waves traveling from the handset to the base, is obtainable without a search warrant). *But see* Kyllo v. United States, 533 U.S. 27 (2001) (holding that a thermal imaging device, used without a warrant on a public street to measure ambient heat in a suspected marijuana growers home, was an unconstitutional search under the Fourth Amendment). One interpretation of *Kyllo* is that Fourth Amendment protection was upheld not to protect privacy, but because the device was aimed at a home, the "quintessential property interest." *See* Swire, *supra* note 59, at 906 n.9.

to claim that "there has been no case beyond wiretapping where application of the test has led to protection of privacy."[67] Although *Katz* and the *Olmstead* dissent are often referenced as bulwarks of the important principle that the government should not trespass into "the privacies of life," their influence have eroded.[68]

2. Third Parties and Privacy Protection

Although the mail and wiretap cases require a governmental agent to obtain a warrant in order to access a sealed letter or a telephone conversation, the same is not true for obtaining that information from a third party. Despite the protection it provides, *Katz* cautions that information "knowingly expose[d] to the public" is not entitled to Fourth Amendment protection,[69] establishing what Daniel Solove refers to as the "secrecy paradigm": Where information is voluntarily shared with another party, it may be legally obtained without a warrant.[70] This standard applies to information truly open to the public[71] or simply information voluntarily shared with a third party, such as a business, from whom it can be compelled.[72]

The seemingly simple third party rule is complicated by the difficulty in determining what information has been shared in such a way that the individual has waived her right to privacy under federal constitutional norms.[73] There is no reasonable expectation of privacy in bank records, deposit slips or checks, for example, because that information is considered to be "shared" with the bank and visible to its employees.[74] The Court

---

67. Swire, *supra* note 59, at 906.

68. Boyd v. United States, 116 U.S. 616, 630 (1886).

69. *Katz*, 389 U.S. at 351. *See also Ex parte* Jackson, 96 U.S. 727, 735 (1878) (cautioning that the contents of a letter or package may be obtained from the recipient without a warrant, even if they cannot be taken from the sender or intercepted in transit without a warrant); Swire, *supra* note 59, at 906.

70. SOLOVE, *supra* note 39, at 198-99.

71. *See e.g.*, Guest v. Leis, 255 F.3d 325 (6th Cir. 2001) (finding no expectation of privacy in material posted to a public internet billboard).

72. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (finding no legitimate expectation of privacy in bank statements held by a third party bank). *See also* Lopez v. United States, 373 U.S. 427, 438 (1963) (finding no expectation of privacy in a conversation when the third party discloses the content of the conversation).

73. *Miller*, 425 U.S. 435.

74. *Id.* at 442. Patricia Bellia believes that the *Miller* court, in so finding, misread an earlier Supreme Court decision which found that the government could compel papers in the possession of the object's account without a warrant. Patricia Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1401 (2004) (discussing Couch v. United States, 409 U.S. 322 (1973)). Bellia argues that the documents in *Couch* were compellable only because the accountant was given the papers with the expectation that the information would be shared during the preparation of tax material. *Id. Miller*, by

has applied this rule to matters as varied as postcards, because the information therein is freely readable by anyone who handles it;[75] telephone records, because they are viewed by phone company employees in the course of business;[76] and the contents of a garbage bag placed in the street, which are considered available to the public and conveyed to the garbage collector.[77]

On the other hand, information or property that has been placed in the hands of a third party but that is deliberately kept secret is still protected from searches.[78] The contents of a sealed letter, for example, are still protected by the Fourth Amendment even if the letter is in the physical possession of the postal service. The average postal service customer cannot assume that her mail carrier will not read the postcards she mails, but she does have a valid expectation that the carrier will not open a sealed letter and read its contents. Therefore a warrant is required for officials to obtain the contents of a sealed letter. By the same token, even though a phone company has the technical ability to eavesdrop on a phone conversation, *Katz* holds that the parties to the call still maintain a reasonable expectation of privacy in the contents of their telephone conversations.

Within the third party rule there is an important distinction as to what kind of third party can be compelled to disclose information. In the letter example, the rule indicates that a recipient can be required to disclose the contents of the letter to government officials because the information was shared with the recipient by the sender. But the mailman may not be so compelled, because the information was not shared with him. This holds true for the telephone as well. *Katz* instructs that the phone company is not a third party from whom the content of the communication can be compelled, but, of course, the other participant in the conversation is such a

---

contrast, more broadly states any document given to a third party may be compelled. *Id.* (discussing *Miller*, 425 U.S. 435).

75. *Ex parte* Jackson, 96 U.S. 727, 733 (1878).

76. *See* Smith v. Maryland, 442 U.S. 735, 744-46 (1979).

77. California v. Greenwood, 486 U.S. 35, 41-42 (1988). The various states have developed their own, varying jurisprudence with regard to what search and seizure protection one has from local law enforcement. In California, for example, there *is* a reasonable expectation of privacy in dialed telephone numbers and in the contents of sealed garbage bags awaiting pick up. Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 396 n.118 (2006) (cataloguing how each state's jurisprudence addresses the third party doctrine).

78. *See, e.g.*, United States v. Thomas, No. 88-6341, 1989 U.S. App. LEXIS 9628, at *6 (6th Cir. July 5, 1989) (holding that there is a reasonable expectation of privacy in the contents of a safety deposit box, based on the holding in *Katz*).

third party, and the same information could be compelled from that person.[79]

The Sixth Circuit's vacated panel decision applied this proposition to the e-mail context by holding that while the contents of an electronic communication can be compelled from the recipient, the underlying ISP is not a third party from whom the same information could be compelled, because the contents of the communication were not shared with them by either the sender or the recipient. As with phone conversations, a third party's technical ability to gain access to the contents of the communication is not enough to diminish the primary party's expectation of privacy.

B. Statutory Attempts to Protect Privacy

The term "eavesdrop" originated from the act of standing "within the 'eavesdrop' of a house in order to listen to secrets."[80] Changes in communication and technology mean that one does not have to lurk outside a door or window in the hopes of overhearing secrets. In addition to the jurisprudence defining the contours of the Fourth Amendment, state and federal statutes further restrict information gathering by government agents or entities. Many of these statutory provisions were legislative responses to Supreme Court decisions defining Fourth Amendment rights.[81]

Intrusion into private life has always been an issue of public import. In the absence of federal rules, concern over government wiretapping during prohibition triggered several state statutes.[82] Twenty-five states had passed such statutes[83] by the time Justice Brandeis wrote his forceful plea for Fourth Amendment protection against future technological threats to "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[84] The state limitations did not, however, apply to federal officials.

In 1934 Congress passed the Federal Communications Act. Section 605 provided that no one, without permission, should "intercept any . . . communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication. . . ."[85] This early fortification proved inadequate, containing no enforcement provision

79. *See* Bellia, *supra* note 74, at 1405.

80. V THE OXFORD ENGLISH DICTIONARY 45 (2d ed. 1989).

81. Swire, *supra* note 59, at 916.

82. Berger v. New York, 388 U.S. 41, 46 (1967).

83. DANIEL J. SOLOVE ET AL., PRIVACY, INFORMATION, AND TECHNOLOGY 83 (2006).

84. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

85. 47 U.S.C. § 605 (1934).

and allowing illegally-obtained evidence to be used in state courts; many intrusive non-wiretapping activities remained free from restraint.[86]

In 1968 Congress passed the Wiretap Act,[87] codifying *Katz* by requiring government agents to obtain a warrant from a federal judge, based on probable cause, before wiretapping.[88] The Act's purpose was "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized."[89] The Act covered wire and aural communications only, leaving out other kinds of communication.[90]

Almost twenty years later, in 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to update the Wiretap Act and extend coverage to electronic communication and data transmissions.[91] It was passed in part because the Justice Department had decided that the Wiretap Act did not cover e-mail communication and Congress, in response, felt the need to extend some protection to it.[92] The ECPA also encompasses the Stored Communications Act (SCA) and the Pen Register Act.

The SCA applies to electronic communication stored by third parties.[93] On a crude level, the SCA allows the government to compel disclosure of stored communications from a third party by means of a court order under certain circumstances.[94] In fact, the SCA is much more intricate, complicating matters with two distinctions. First, the SCA designates two types

---

86. *See* SOLOVE ET AL., *supra* note 83, at 83. *See, e.g.*, Goldman v. United States, 316 U.S. 129 (1942) (finding no Federal Communications Act § 605 violation where eavesdropping is effected by placing a sound magnification device against a wall to listen to conversations in a neighboring office).

87. The so-called Wiretap Act was formally Title III of the Omnibus Crime Control Act of 1968. Pub. L. No. 90-351, (codified as amended at 18 U.S.C. §§ 2510-22 (2000 & Supp. V 2005)).

88. It is widely understood that the Supreme Court's decisions in *Katz* and *Berger* largely informed the legislative drafting of the Wiretap Act. *See, e.g.*, Solove, *supra* note 9, at 754.

89. S. REP. No. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153.

90. Pub. L. No. 90-351, (codified as amended at 18 U.S.C. §§ 2510-22 (2000 & Supp. V 2005)). It was later amended in 1986 to include electronic communication as well. U.S. DOJ: Prosecuting Computer Crimes Manual at 55 (2007), *available at* http://www.cybercrime.gov/ccmanual/02ccma.pdf.

91. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C §§ 2510-2711 (2000).

92. HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 67 (1999).

93. *See* 18 U.S.C. §§ 2701-2711 (2000).

94. 18 U.S.C. § 2703 (2000).

of providers—electronic communication service providers (ECS) and remote computing service providers (RCS). Secondly, it distinguishes between types of communications—communications opened or stored for more than 180 days versus unopened communication stored for less than 180 days.[95] These distinctions "fr[oze] into the law the understandings of computer network use as of 1986" when the statute was written,[96] conceptions rendered obsolete by later technological development.[97]

Under section 2703(d) of the SCA, the government may obtain electronic information by court order only upon a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation,"[98] a lower threshold than the requirement for obtaining a warrant. Where there is reason to believe that notifying the subject might have an "adverse result," the SCA also allows the government to delay normal requirements of notification to the account holder by ninety days and prevent the compelled party from informing the account holder.[99] The SCA provides four specific examples of "adverse result" in its definition and then further states that an adverse result is anything that "seriously jeop-

95. The crux of the 180 day distinction is that only unopened e-mails less than 180 days old are entitled to very much protection. *See id.* For a detailed explanation of both of these distinctions see Kerr, *supra* note 41. For an in-depth description of the parts of the statute and different interpretations of their application see Bellia, *supra* note 74, at 1413-26.

96. Kerr, *supra* note 41, at 1214.

97. *See, e.g., id.*; Bellia, *supra* note 74, at 1397 ("[The provisions of the SCA] are becoming increasingly outdated and difficult to apply . . . . [R]evision of the statutory framework is urgently needed."); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1559 (2004) ("Many who support the [ECPA] would agree that it has failed to keep pace with changes in and on the Internet . . ."). *See also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("ECPA was written prior to the advent of the Internet. . . . [T]he existing statutory framework is ill-suited to address modern forms of communication. . . .").

98. 18 U.S.C. § 2703(d) (2000).

99. 18 U.S.C. § 2705(a)(1)(A) (2000).

ardiz[es] an investigation."[100] The government used the SCA to obtain Warshak's e-mail and delay notification to Warshak for over 180 days.[101]

The Pen Register Act covers "trap and trace device[s]" used to capture transmitted information.[102] Originally the Pen Register Act allowed the government access only to numbers dialed on a telephone line, but the USA-PATRIOT Act expanded the definition in 2001.[103] Today, upon obtaining a court order, the Act allows the government to "install and use a pen register or trap and trace device" that records "electronic or other impulses," limited to "the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications."[104] This change allows the government to use a trap and trace device to acquire *non-content* information of e-mails—header information.[105] However, it may not be used to acquire *content* information, like the telephone conversation or the body of an e-mail.[106]

Even this simple distinction between content and non-content for pen registers raises questions as technology changes. Under settled law, a dialed phone number is non-content information voluntarily shared with the

---

100. "Adverse result" is defined as (A) fear of harm to themselves or others, (B) flight, (C) destruction of evidence or (D) witness intimidation. 18 U.S.C. § 2705(a)(2). An adverse result may also be anything that "otherwise seriously jeopardiz[es] an investigation," which means that the government can easily get an order prohibiting the ISP from informing the account holder of the 2703(d) order and delaying notification for up to 90 days at a time. 18 U.S.C. § 2705(a)(2)(E) (2000).

101. *See* Warshak v. United States, No. 1:06-cv-357 2006 U.S. Dist. LEXIS 50076 at *3-6 (S.D. Ohio 2007). This Note focuses on protection of privacy from government intrusion. For a discussion of limitations of the SCA with regard to protecting privacy from *private* intrusion, see Rachel V. Groom, Note, In re Pharmatrak & Theofel v. Farley-Jones: *Recent Applications of the Electronic Communications Privacy Act*, 19 BERKELEY TECH. L.J. 455, 460 (2004) ("As [*Theofel*] shows, eighteen years of technological advances raise doubts about the ability of the ECPA to address the problem of privacy violations on the Internet.").

102. 18 U.S.C. § 3121 (2000). A pen register is a device that records the digits one dials when using a telephone, but does not record spoken conversation. *In re* United States, 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007).

103. Solove, *supra* note 9, at 757.

104. 18 U.S.C. § 3121(c) (2000 & Supp. V 2005).

105. Solove, *supra* note 9, at 757.

106. The Pen Register Act codifies the 1979 Supreme Court decision in *Smith v. Maryland*, finding no Fourth Amendment protection from use of a pen register because there is no reasonable expectation of privacy in non-content information. In the telephone communication context, the conversation is the content of the phone call, while the steps one takes to initiate that private conversation are considered non-content. The phone number dialed, for example, would be non-content information and could be acquired through a Pen Register.

service provider that may be collected by means of a pen register. But what about post-cut through dialed digits (PCTDD), which are numbers keyed in after the call is connected?[107] Anyone who has called a credit card company or bank has keyed in account numbers, pins and passwords. The government has argued that such information is like the dialed phone number and is not "content," and thus should be collectable without a warrant.[108] The 1986 Pen Register Act, written before these types of automated systems became popular, does not provide an answer on this issue, and amendments to the Pen Register Act in 2001 offer no additional clarification.[109] Recently, a federal district court in New York decided that PCTDD is content information and that individuals do retain a reasonable expectation of privacy in them.[110]

Overall, the ECPA and its subcomponents, the SCA and Pen Register Act, provide quite narrowly defined protections. These limited provisions do not address the broad, ongoing changes in communications technologies. Even Professor Orin Kerr, who generally believes that privacy protections should be defined by statute, argues that the protections provided by the SCA are inadequate.[111]

IV. UNWITTINGLY SURRENDERING REASONABLE EXPECTATIONS OF PRIVACY WITH NEW COMMUNICATIONS TECHNOLOGIES

Katz provided protection for telephone conversations because the Fourth Amendment protects people, "and not simply 'areas.'"[112] New technologies allow us to communicate in ways not previously envisioned

---

107. PCTDD are any "'digits that are dialed . . . after the initial call setup is completed.'" PCTDD can be account or pin numbers, but can also include telephone numbers, such as when the original connected call is to a calling card or a collect call, which then requires a further input of the destination phone number. *In re* United States, No. H-07-613, 2007 U.S. Dist. LEXIS 77635, *2 at n.1 (D. Tex. 2007).

108. *In re* United States, 515 F. Supp. 2d 325 (E.D.N.Y. 2007).

109. The USA-PATRIOT Act of 2001 updated the Pen Register Act to include wireless communication, but only states that a warrant is necessary for content information without further defining "content." 18 U.S.C. § 3127 (2000), *amended by* USA-PATRIOT Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288 (2001).

110. *In re* United States, 515 F. Supp. 2d at 325.

111. Kerr, *supra* note 41, at 1233-34 (suggesting that congress should bolster the "surprisingly low" standard for compelling communication from third parties as this was "precisely the result that the SCA was enacted to avoid."). Kerr also advocates the adoption of a suppression remedy. *Id.* at 1241. Part V compares judicial and statutory privacy protection.

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

by either the Supreme Court or Congress at the time of *Katz*, and certainly not imagined by the drafters of the Fourth Amendment. Four decades of applying the *Katz* framework to new technologies has generally resulted in a limiting of protection for our communication. Voice mail messages, Voice over Internet Protocol (VoIP), e-mail, and other new communication technologies have blunted *Katz*'s impact, making it easier for the government to gain access to the contents of communications.

Voice mail messages were once protected under the same strict standards as any telephone conversations. Changes to the Wiretap Act through the USA-PATRIOT Act of 2001, however, mean that all voice mail is now considered "stored communication" and may be accessed under the looser standards of the SCA.[113]

VoIP is another new voice technology that might allow normally protected phone conversations to be obtainable without a warrant. VoIP takes analog audio signals and turns them into digital data packets that are transmitted over the Internet, a much more efficient means of communication than the circuit switching employed for typical phone calls.[114] Businesses are switching to IP telephony, as are consumers who find it cheaper and more convenient.[115] But the data packets can be more easily recorded and stored by either party to a conversation, turning this into a form of communication that would fall under the SCA rather than the Wiretap Act.[116] This creates a confusing dual system where some phone conversations are entitled to strong protections under the Wiretap Act, while others are subject to the weaker constraints of the SCA.

Technological changes not only affect which statute covers each category of communication, but also change what one can reasonably expect to keep private. VoIP services, for example, are now able to mine the contents of users' conversations. Pudding Media is a new company that offered free VoIP service in exchange for the ability to target advertisements to users based on the content of their conversations.[117] As a user spoke, voice recognition software sent advertisements to the user's computer

113. *See* Swire, *supra* note 59, at 911.

114. How Stuff Works, VoIP: Circuit Switching, http://communication.howstuffworks.com/ip-telephony2.htm (last visited Apr. 6, 2008).

115. Leslie Cauley, *Consumers Finally Get a Grip on VoIP*, USA TODAY, Feb. 13, 2007, at 1B ("In 2002, VoIP claimed about 150,000 U.S. users. . . . By the end of 2006, it was 8.6 million. . . . Lower cost is its chief draw.").

116. *See* Swire, *supra* note 59, at 911.

117. Louise Story, *A Company Will Monitor Phone Calls and Devise Ads to Suit*, N.Y. TIMES., Sept. 24, 2007, at C1.

based on keywords in the conversation.[118] Trying to alleviate privacy concerns raised following significant press exposure, the company website assured customers that Pudding Media would not record conversations, and that the advertising process would be completely automated.[119] Under the vacated opinion in *Warshak*, this kind of communication would likely be protected. It is not being recorded or stored by the company, and while the company is combing the content of the communication, it is only an automated process so the expectation of privacy is not lost. However, the Sixth Circuit made it clear that users could give up their reasonable expectation of privacy based on how a service provider monitors their communications;[120] it is certainly possible that VoIP service offerings will be modified in a way that would change the reasonable expectation of privacy.

The increasing use of e-mail, the form of communication at issue in *Warshak*, means that communication that would previously have taken place over the telephone is now conducted through commercial ISPs. Consequently, communication that once would have been protected under the Wiretap Act now falls under the SCA. The ease of communication is offset by subjecting most communications to lesser protection.

V. JUDICIAL ACKNOWLEDGEMENT THAT ELECTRONIC COMMUNICATIONS ARE SUBJECT TO FOURTH AMENDMENT PROTECTION IS NEEDED

Katz created Fourth Amendment protection for telephone communication, which Congress later codified in the Wiretap Act. Most judicial decisions after *Katz* limited the broad protection that was created in *Katz* and championed by Justice Brandeis in *Olmstead*.[121] But many still agree that the "privacies of life" are worth protecting.

---

118. *Id.*

119. Pudding Media, Consumers, http://puddingmedia.com/consumers.html (last visited Feb. 3, 2008) (on file with author) ("Pudding Media's technology is based on speech recognition, so the process is completely automated, doesn't involve humans and doesn't record calls."). Pudding Media has since discontinued this direct-to-consumer product offering.

120. Warshak v. United States, 490 F.3d 455, 475 (6th Cir. 2007), *vacated* Warshak v. United States, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007).

121. *See e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976); United States v. Forrester, 495 F.3d 1041 (9th Cir. 2007). *But see* United States v. Thomas, No. 88-6341, 1989 U.S. App. LEXIS 9628 (6th Cir. July 5, 1989); Kyllo v. United States, 533 U.S. 27 (2001).

This Part evaluates the costs and benefits of developing communication protections legislatively, considered in Section V.A, or judicially, considered in Section V.B. Section V.C argues that, in light of the tradeoffs, an initial judicial finding of Fourth Amendment protection for electronic communication (similar to the vacated *Warshak* result) is most appropriate. *Warshak* presents an opportunity for the judicial branch to reaffirm, in the context of electronic communication, the liberal Fourth Amendment protection outlined in *Katz*. When case law and statutory systems attempt to detail a broad proposition and apply it to specific facts, such attempts necessarily limit the original intention. A new *Katz*, one that reiterates the privacy protection offered by the Fourth Amendment and applies that protection to electronic communication, is necessary. Such a rule does not preclude further statutory response, and would likely spur legislative action to add detail, much in the way that the 1968 Wiretap Act gave particular meaning to *Katz*.

A. The Legislative Option

Technologies are ever changing. In considering whether judges or legislatures should take charge of privacy protections, the fast pace of technological development might appear to favor legislative leadership. In theory, legislatures are able to respond quickly to changes in technology by updating legislation regularly.[122] With the Electronic Communication Protection Act, for example, Congress acted quickly to provide a set of rules to govern a new communication medium.

Despite this potential, Congress does not always amend the statutory framework to keep up with changes in technology, which can lead to outdated laws and insufficient protection.[123] Even as the passing of the ECPA exemplifies that Congress is able to react quickly to new technology, the twenty-two year subsequent treatment of the Act demonstrates that Congress does not always revisit and update legislation adequately.[124] The SCA is riddled with outdated elements that Congress has not amended even as electronic communication technologies have been modified and improved.[125] When the ECPA was enacted it would have been impossible to imagine how pervasive e-mail usage would become. No commercial ISP existed until 1990 and the World Wide Web did not become practical

122. Kerr, *supra* note 46, at 807.

123. Solove, *supra* note 9, at 769. Congress has made only five major revisions to electronic surveillance laws in the last seventy years. *Id.*

124. *See* notes 93-97 and accompanying text (SCA description).

125. *See* note 95 and accompanying text (RCS/ECS).

until 1991.[126] The number of Americans using the Internet continues to grow dramatically—from sixty percent in 2004 to seventy-three percent in 2006.[127] The ECS/RCS provider distinction within the SCA, for example, may have been a useful differentiation in 1986, but is mystifying today.[128] Websites now can be ECS providers, RCS providers, both, or neither, creating confusion as to which rules should apply in any given context.[129] Congress has not eliminated or reformed this distinction, despite much public and scholarly criticism.[130]

Congress also has access to expert input, can request committee reviews, and can commission detailed reports on new technologies to better inform statutory changes.[131] This arguably allows a legislature to create well-informed and detailed statutory systems that address privacy concerns arising from new technologies. Opposing this view, Professor Daniel Solove rhetorically asks whether "we really need two years and thousands of pages of detailed information to understand how e-mail works," and contends that expert testimony and amicus briefs can be just as effective in educating judges on the technological issues.[132]

Congress may also be best positioned to take into account the needs of law enforcement. In his concurrence in *Katz*, Justice White highlighted that there might be instances where a warrant would not be required, such as where national security was at issue.[133] Today national security is of paramount concern, and Congress, with its hearings, reports and studies, may best be able to balance the public's privacy rights with the need to provide law enforcement with effective tools to fight crime and terrorism. Certainly Congress has, at times, attempted to reach this balance, such as with the 1978 Foreign Intelligence Surveillance Act and the USA-PATRIOT Act of 2001.

Congress, however, is subject to political realities that do not always make it the best arbiter of constitutional provisions; it may not be able to give equal weight and consideration to all interests. Law enforcement is highly organized and politically savvy, much more so than a diffuse public

126. Mulligan, *supra* note 97, at 1572.

127. JOHN B. HORRIGAN, PEW INTERNET & AM. LIFE PROJECT, HOME BROADBAND ADOPTION 2006 (2006), *available at* http://www.pewinternet.org/pdfs/PIP_Broadband_trends2006.pdf.

128. *See* note 95 and accompanying text (RCS/ECS).

129. Kerr, *supra* note 41, at 1215-18.

130. *See, e.g., id.*

131. Kerr, *supra* note 46, at 807.

132. Solove, *supra* note 9, at 771-72.

133. *See* Katz v. United States, 389 U.S. 347, 363 (1967) (White, J., concurring).

with privacy concerns but little in the way of organized political clout.[134] After the USA-PATRIOT Act was passed, for example, the DOJ created a website to increase public support for the Act, and then-Attorney General John Ashcroft went on a speaking tour of eighteen cities to garner additional backing, all at public expense.[135]

An elected Congress is also easily swayed by public opinion. Such a system responds well to the wishes of the majority, but public fear or outcry can lead to laws that do not give sufficient weight to constitutional concerns or protect all interests.[136] The USA-PATRIOT Act, for example, was passed just forty-five days after 9/11 by wide margins in both the House and Senate.[137] The national atmosphere following such an affecting terrorist action made careful consideration and opposition to the Act difficult, but the growing concern about the Act shows that significant opposition exists.[138] By 2003, many communities and three states had "passed resolutions denouncing the USA-PATRIOT Act as an assault on civil liberties,"[139] and six years after 9/11 the debate is vigorous and all viewpoints are now better represented. This example shows how Congress can quickly react to public fear in ways that do not give sufficient consideration to privacy concerns.

B. Judicial Option

An argument supporting a strong judicial role in defining privacy protections, raised regularly since *Olmstead*, is that the Constitution should be a living document that always has meaning—even after 200 years of tech-

---

134. Swire, *supra* note 59, at 914-15.

135. Dahlia Lithwick & Julia Turner, *A Guide to the Patriot Act, Part I*, SLATE, Sept. 8, 2003, http://www.slate.com/id/2087984. Lithwick & Turner refer to Ashcroft's speaking tour as the "'Patriot Rocks' concert tour." *Id.*

136. *See, e.g.*, Swire, *supra* note 59, at 915 (discussion of the passage of the USA-PATRIOT Act in the wake of the September 11 attack).

137. Office of the Clerk of the U.S. House of Representatives, Final Results for Roll Call 398, http://clerk.house.gov/evs/2001/roll398.xml; United States Senate, U.S. Senate Roll Call Votes 107th Congress—1st Session, http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=107&session=1&vote=00313. The House passed the PATRIOT Act by more than a five to one margin, while in the Senate, one lone senator voted against the Act.

138. *See* Lithwick & Turner, *supra* note 135; *see also* Beryl A. Howell, *Seven Weeks: The Making of the USA-PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1161 (2004) ("The administration was not interested in congressional deliberation, compromise . . . [i]nstead, it wanted its legislation passed immediately" and it pressured "Congress with the uncertain threats of future terrorist attacks and telling the public that congressional delay was handing terrorists an 'advantage.'").

139. Lithwick & Turner, *supra* note 135.

nological changes. Justice Brandeis clearly articulated this argument in his *Olmstead* dissent:

> "Time works changes, brings into existence new conditions and purposes. Therefore a principle to be vital must be capable of wider application than the mischief which gave it birth. This is peculiarly true of constitutions. They are not ephemeral enactments, designed to meet passing occasions. . . . In the application of a constitution, therefore, our contemplation cannot be only of what has been but of what may be. Under any other rule . . . [r]ights declared in words might be lost in reality."[140]

Brandeis then applied this proposition to the Fourth Amendment by arguing that the founding fathers intended it to grant citizens a "right to be let alone" by the government, which should be upheld regardless of the means of intrusion utilized.[141] The concept reiterates an 1886 decision where the Court stated that the Fourth and Fifth Amendments protect more than "rummaging [through] drawers," because "the struggles [of the nations founders] against arbitrary power in which they had been engaged for more than twenty years, would have been too deeply engraved in their memories to have allowed them to approve of such insidious disguises of the old grievance which they had so deeply abhorred."[142]

The majority in *Olmstead* considered whether Brandeis' interpretation of Fourth Amendment protection did more than just apply the Fourth Amendment to new technology and actually read more into the Amendment than was originally intended. At the time, the Fourth Amendment was still interpreted as protecting the physical confines of a person's house or tangible effects.[143] It is now settled law that the Fourth Amendment applies to a sphere of privacy rather than just to physical property.[144] However, the concern raised in *Olmstead*, that the Court should refrain from reading unintended meaning into the Constitution because of technological or societal changes, is an ongoing one. It was echoed by Justice Black's dissent in *Katz* when he stated that "it is [not] the proper role of this Court to rewrite the Amendment in order 'to bring into harmony with the times'

140. Olmstead v. United States, 277 U.S. 438, 472-73 (1928) (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

141. *Id.* at 478.

142. Boyd v. United States, 116 U.S. 616, 630 (1886).

143. *Olmstead*, 277 U.S. at 464-66 ("[T]he courts may not adopt such a policy [protecting the contents of telephone conversations] by attributing an enlarged and unusual meaning to the Fourth Amendment.").

144. *See supra* Section III.A.1.

and thus reach a result that many people believe to be desirable,"[145] and it is still raised today.

Praising Justice Brandeis' dissent in *Olmstead*, Professor Lawrence Lessig goes further, calling not just for judicial interpretation of the Fourth Amendment that applies the words of the Fourth Amendment to today's realities, but inviting judicial activism. Lessig finds it better to "err on the side of harmless activism than on the side of debilitating passivity."[146] Otherwise, Lessig argues, legislatures act without regard to constitutional requirements and the freedom from government intrusion, so highly valued by the Constitution's framers, can be easily eroded.[147]

This viewpoint is criticized by some scholars,[148] but Fourth Amendment jurisprudence, *Katz* in particular, supports a judicial system that actively reinterprets and applies Fourth Amendment privacy protection as new technologies develop.[149] With *Katz* and its companion case, *Berger v. New York*, the Supreme Court reversed decades of leaving privacy protection to state and federal legislatures, and found a Fourth Amendment privacy right to telephone communications.[150] Even more recently, in *Kyllo v. United States*, the Supreme Court reaffirmed that the Fourth Amendment offers protection to new technologies. There, the Court found that using a thermal imaging device without a warrant to measure the ambient heat of a private dwelling in order to determine if drugs were being grown, was an unreasonable search.[151]

Because of the post-1968 reluctance of the courts to broaden Fourth Amendment privacy protection, Orin Kerr claims that this concept of an active court is "romantic but somewhat inaccurate."[152] He admits that *Berger* and *Katz* influenced the subsequent statutory structure but argues that this function of the Court is now defunct, highlighting later judicial deference to the statutory scheme as proof.[153]

---

145. Katz v. United States, 389 U.S. 347, 364 (1967) (Black, J., dissenting).

146. LAWRENCE LESSIG, CODE VERSION 2.0 327 (2006).

147. *See id.* at 325-26.

148. *See, e.g.*, Kerr, *supra* note 46, at 858.

149. *See, e.g.*, *Ex parte* Jackson, 96 U.S. 727 (1878) (applying Fourth Amendment search and seizure rules to documents sent through postal mail); *Katz*, 389 U.S. 347 (giving Fourth Amendment protection to the contents of wire communication).

150. *See supra* Section III.A.1. *See also* Berger v. New York, 388 U.S. 41, 59-60 (1967) (striking down portions of a New York State eavesdropping statute allowing wiretapping without a warrant or judicial review).

151. Kyllo v. United States, 533 U.S. 27 (2001).

152. Kerr, *supra* note 46, at 805.

153. *Id.* at 855.

Kerr argues that making a broad, general ruling claiming Fourth Amendment protection for e-mail, or the "'all at once' approach," leads to overbroad conclusions and mistakes.[154] He believes that a fact-specific, case-by-case review is the appropriate judicial evaluation of electronic communication cases. To bolster his point, Kerr points to mistakes that he claims are found in the *Warshak* analysis.[155]

C. The Middle Ground: Court Involvement, Followed by Additional Congressional Rule-Making

One extreme position would have judges actively define privacy protection. The other would have the legislatures take a central role in demarcating privacy protections, with minimal intrusion from and review by the judicial branch. As the previous Sections show, both approaches have costs and benefits. In reconsidering *Warshak*, the full Sixth Circuit should develop a middle ground, reminding Congress of the intent of the Fourth Amendment by finding a broad privacy right in e-mail communication, but leaving to Congress the detailed rule-making necessary to apply the Fourth Amendment to modern communication.

Warshak comes after more than twenty years of public debate and congressional investigation focused on stored and electronic communication. The technologies may be constantly changing, but the concept of electronic communication is not new. Kerr states that his "argument applies only when technologies are in flux."[156] While electronic communication is constantly evolving, it is no longer a new concept. If the courts wait until technology ceases to advance, they will always defer to Congress. The decades of public debate and congressional action can now inform judicial responses, including that of the Sixth Circuit, to address Fourth Amendment protection for a technological movement that has drastically changed the way Americans communicate, on a scale similar to the invention of the telephone.

In *Warshak*, the government argues that there is no reasonable expectation of privacy in electronic communication because the nature of e-mail means that the ISP has access to the contents of e-mail communication. The provider's employees have access to the e-mail and regularly filter it

---

154. Brief of Amicus Curiae Orin S. Kerr in Favor of the Petition of the United States for Rehearing En Banc at 9-11, Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated* Warshak v. United States, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007), *available at* http://volokh.com/files/warshakamicus.pdf ("[T]he panel opinion includes several conclusions that are highly questionable or simply wrong.").

155. *Id.*

156. Kerr, *supra* note 46, at 859.

for material objectionable to the user, like spam. Under third party doctrine, therefore, there should be no Fourth Amendment protection for this type of material because one cannot reasonably expect it to be private.

Katz, however, stands not just for what one actually expects to be private, but also what society *wants* to be kept private.[157] Given the state of telephony technologies when *Katz* was decided, the Court may have shaped an expectation of privacy in telephone conversations based on what it believed *should* be private, rather than what one could reasonably expect would actually be private.

Prior to *Katz*, for example, the police routinely used wiretapping techniques during prohibition to further their law enforcement objectives.[158] Common practical and social telephone use, too, dictated that telephone users should have known that a third party would easily be able to overhear their conversations. Through the 1960s most phone calls were manually connected by switchboard operators who had the ability to participate in or listen to conversations.[159] Party lines—lines shared between multiple users—were also in widespread use before *Katz*, and eavesdropping on party lines was common.[160] Reminiscing about her childhood party line and the prevalence of eavesdropping, one woman recently said, "I still, to this day, have the feeling that if it's private, you don't talk about it on the phone."[161]

---

157. *In re* United States, 515 F. Supp. 2d 325, 336 (E.D.N.Y. 2007).

158. SOLOVE ET AL., *supra* note 83, at 73 ("Before *Katz*, police frequently tapped phones. A person might expect that wiretapping would be likely.").

159. Wikipedia, Switchboard Operator, http://en.wikipedia.org/wiki/Switchboard_operator (last modified Jan. 29, 2008). Copious references to switchboard operators in old movies and mysteries illustrate that most telephone users at the time of *Katz* might expect an operator to eavesdrop on a call and repeat the fruits of her activities to others.

160. Wikipedia, Telephony, http://en.wikipedia.org/wiki/Party_line_(telephony) (last modified Mar. 19, 2008). *See also* Privateline.com, Telephone History Party Lines, http://www.privateline.com/TelephoneHistory5/partyline.htm (last visited Apr. 6, 2008) ("Party lines for non-business subscribers were the rule before World War II, not the exception. In cities and country, most people shared a line with two to ten to twenty people. You could talk only five minutes or so before someone else wanted to make a call. And anyone on the party line could pick up their receiver and listen in to your conversation."). The 1959 movie "Pillow Talk," where Rock Hudson and Doris Day's characters have their first encounter because she overhears his conversations on their shared party line, is a popular culture example showing the prevalence of shared party lines. This particular example was likely exaggerated because party lines were not common in metropolises like New York City after the 1930s, but they remained in wide use in other parts of the country until much later. Rick Hampson, *Digital Times, Private Lives are Breaking Up Party Lines*, USA TODAY, Oct. 23, 2000, 19A ("In the Midwest . . . half the residential lines were party lines.").

161. Hampson, *supra* note 160.

In later describing the *Katz* test, Justice Blackmun wrote that:

> Situations can be imagined, of course, in which *Katz*' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. . . . [W]here an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment was. In determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper.[162]

Despite awareness that an ISP has the ability to look at e-mails, filter them for spam, or even target advertisements based on the contents of such communications, many think that there *should* be Fourth Amendment protection for e-mail, and *Warshak* is a good opportunity for the courts to find such protection.[163] Like *Katz* did for telephone communication, *Warshak* can find a reasonable expectation of privacy in electronic communication.

The courts need not go farther than the *Katz* holding. It would be sufficient to simply reiterate the Fourth Amendment justification for communication protection and make it clear to congressional rule-makers that privacy protection extends to electronic communication. In 1878, the Supreme Court gave Fourth Amendment protection to mailed correspondence[164] and, in 1967, affirmed that such protection applied to more modern modes of communication.[165] Technology has again revolutionized communication and information storage, and the Court should reaffirm that Fourth Amendment protection applies to communication regardless of the technology used.

Such a decision in *Warshak* would still allow Congress to amend existing statutes or establish new ones. No court decision would be able to address all factual scenarios, so congressional refinements would be neces-

---

162. Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979).

163. *See* Brief of Amici Curiae Electronic Frontier Foundation, ACLU of Ohio Foundation, Inc., ACLU, & Center for Democracy & Technology Supporting the Appellee and Urging Affirmance at 6, Warshak v. United States, 490 F.3d 455 (6th Cir. 2007) (No. 06-4092), *available at* http://w2.eff.org/legal/cases/warshak_v_usa/warshak_amicus.pdf ("It is equally plain that society expects and relies on the privacy of messages that are sent or received using email providers just as it relies on the privacy of the telephone system."). *See also* Reynolds Holding, *E-mail Privacy Gets a Win in Court*, TIME, Jun. 21, 2007, http://www.time.com/time/nation/article/0,8599,1636024,00.html.

164. *Ex parte* Jackson, 96 U.S. 727 (1878).

165. Katz v. United States, 389 U.S. 347 (1967).

sary. In making these rules Congress would draw on resources such as expert opinions and committee reports and would be able to weigh law enforcement needs and national security concerns, but would act with the knowledge that electronic communication was constitutionally entitled to strong privacy protection.

Most importantly, in *Warshak* the Sixth Circuit should not avoid the constitutional issues by denying the injunction on procedural grounds and ignoring the substantive concerns.[166] Even if the Sixth Circuit finds no reasonable expectation of privacy in the contents of e-mail communication, such a finding could galvanize congressional action.[167] The judicial history shows that such court decisions can be effective in spurring a congressional response: a refusal to find Fourth Amendment protection in bank records[168] prompted Congress to pass the Right to Financial Privacy Act, and finding that no right to privacy exists in pen-register data[169] prompted passage of the Pen Register Act.[170] Although the congressional response did not require that law enforcement officials obtain a "super-warrant" to collect information, it did add a layer of privacy protection.[171] In both cases Congress became interested in passing new legislation precisely because of Court decisions that highlighted the issue. While a clear finding of Fourth Amendment protection would provide the most privacy protection for e-mail communication, a substantive finding of no Fourth Amendment protection could still lead to some additional privacy protection by way of congressional action.[172]

VI. CONCLUSION

The Supreme Court used the opportunity presented in the 1960s wiretapping cases *Berger* and *Katz* to remind the country and Congress that the

166. See *supra* note 22 for a summary of the procedural arguments proffered by the United States. *But see* Posting of Orin Kerr to The Volokh Conspiracy, Warshak v. United States, http://volokh.com/posts/1176832897.shtml (April 17, 2007, 2:53 PM EST).

167. *See* Swire, *supra* note 59, at 916-17.

168. United States v. Miller, 425 U.S. 435 (1976).

169. Smith v. Maryland, 442 U.S. 735 (1979).

170. Swire, *supra* note 59, at 916-17.

171. "Super-warrant" refers to a warrant issued under the Wiretap Act, for which the requirements are more strict than a standard Fourth Amendment search warrant. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1282 (2004).

172. *But see id.* at 918 (suggesting that the factors influencing the passage of privacy-protecting statutes after *Miller* and *Smith v. Maryland* no longer exist, and future court decisions may not lead to congressionally sponsored privacy protection).

Fourth Amendment had specific meaning and conferred a particular right against government intrusion, even as new technologies exponentially increased the ability of the government to intrude in the lives of citizens. Far from inhibiting statutory regulation, these cases are part of a history that includes detailed statutory protections regulating government behavior. Soon after these cases were decided Congress passed the Wiretap Act, which was informed by these decisions. Later court decisions that limited Fourth Amendment protection also galvanized Congressional action in this field.

Sometimes in response to court decisions, and sometimes proactively, Congress has admirably enacted or amended laws to govern new technologies and limit the government's ability to use technological advancement as an excuse to intrude on the lives of citizens. Congress can effectively weigh various interests and create the appropriate level of protection. However, due to institutional limitations, the judicial branch must occasionally remind Congress of the essential protection conferred by the Fourth Amendment.

In *Warshak* the Sixth Circuit was presented with an opportunity to again remind Congress that the Fourth Amendment limits government intrusions. The district court and the three-judge Sixth Circuit panel that originally decided the case rose to the occasion. Now the Sixth Circuit, en banc, has the opportunity to affirm that choice.