Fordham Law Review

Volume 78 | Issue 1 Article 9

2009

Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment

Alexander Scolnik

Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment

Cover Page Footnote

J.D. Candidate, 2010, Fordham University School of Law; B.E., 2006, Cooper Union. I would like to thank my advisor, Professor Katherine Strandburg, for her insightful comments and feedback and my family and friends for their support and encouragement.

PROTECTIONS FOR ELECTRONIC COMMUNICATIONS: THE STORED COMMUNICATIONS ACT AND THE FOURTH AMENDMENT

*Alexander Scolnik**

As e-mail and other forms of electronic communications began becoming widely used, Congress recognized the need to protect these new forms of communication from impermissible intrusion. Unsure whether the flexible approach to determining the extent of Fourth Amendment protections as announced in Katz v. United States *would extend to electronic communications, Congress enacted the Electronic Communications Privacy Act (ECPA) to ensure a baseline level of protection. This Note argues that the Fourth Amendment does extend to electronic communications and, therefore, the provisions of the ECPA that allow the government to access certain electronic communications without a search warrant are unconstitutional.*

TABLE OF CONTENTS

INTRODUCTION 350
I. COMMUNICATIONS AND THE FOURTH AMENDMENT 351
A. *The Third-Party Doctrine* 355
1. Delivery and Routing Information Directly Conveyed to Third Parties 356
2. Records and Information Stored in Databases Managed by Third Parties 357
B. *Fourth Amendment Standards Evolve with Technology* 361
1. Telephone Conversations 362
a. Olmstead v. United States 362
b. Katz v. United States 363
2. Postal Mail 365
3. Telegraph Messages 368
C. *Legislative Actions To Protect Electronic Communications* 372
1. Motivation for the Electronic Communications Privacy Act 372

* J.D. Candidate, 2010, Fordham University School of Law; B.E., 2006, Cooper Union. I would like to thank my advisor, Professor Katherine Strandburg, for her insightful comments and feedback and my family and friends for their support and encouragement.

2. The Electronic Communications Privacy Act Framework 375
3. Internet Use After the Electronic Communications Privacy Act 378
4. Protections Under State Law 380
II. DIFFERENT LEVELS OF PROTECTION AFFORDED BY THE STORED COMMUNICATIONS ACT AND THE FOURTH AMENDMENT 382
A. *The Stored Communications Act in Action* 382
B. *Applying the Fourth Amendment to Electronic Communications* 383
1. E-mail: *Warshak v. United States* 384
2. Text Messages: *Quon v. Arch Wireless Operating Co.* 386
3. Protection for Other Electronic Information 389
a. *Information Held by, but Not Directed to, Third Parties* 389
b. *Information Reviewed by Third Parties* 392
III. SECTION 2703 OF THE STORED COMMUNICATIONS ACT IS UNCONSTITUTIONAL AS APPLIED 393
CONCLUSION 397

INTRODUCTION

Imagine that local law enforcement officers suspect one of the town's residents is trafficking drugs. The officers have a hunch that this person may be involved but have never observed anything that would give them probable cause to obtain a warrant to search him or any of his property. But, with some legwork, the officers discover that the suspect uses a free, public e-mail service. They then serve a subpoena on that service directing the provider to turn over all of the suspect's messages that are over 180 days old and prohibiting the provider from notifying the suspect. In response to this request, the officers receive thousands of old messages spanning everything from legitimate business correspondence to personal messages, online shopping receipts, and beyond. Still armed with nothing more than a hunch, the officers begin to comb through this individual's voluminous e-mail records describing all manner of personal information on a quest for probative evidence.

Congress recognized the potential problems that could flow from unlimited review of e-mails and other electronic communications in this and similar situations and grew concerned that existing Fourth Amendment jurisprudence might not encompass these new forms of communication. This is partly because electronic communications frequently pass through third-party intermediaries during transmission, and even though the messages are not directed to the providers, these third parties often store copies of the communications on their servers. In response to these concerns, Congress enacted the Electronic Communications Privacy Act

(ECPA)[1] to guarantee a baseline level of protection for electronic communications including e-mail.[2]

Despite the ECPA's goal of broadly protecting electronic communications, the Act is premised on computer technology from the 1980s, and the developments over the past twenty years render some provisions of the ECPA inconsistent with the requirements of the Fourth Amendment.[3]

Part I of this Note describes the current Fourth Amendment framework and how it has been applied to other forms of communication as well as to information that passes through third-party intermediaries. Part I also discusses the history behind the ECPA. Part II examines the conflict between two recent cases, which hold that electronic communications are protected by the Fourth Amendment, and the provisions of the ECPA, which allow access to these communications on a lesser showing than is required under the Constitution. Finally, Part III concludes that § 2703(b) of the Stored Communication Act (SCA), which allows law enforcement access to electronic messages greater than 180 days old without a warrant, is unconstitutional as applied.

I. COMMUNICATIONS AND THE FOURTH AMENDMENT

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[4] The U.S. Supreme Court has consistently stressed that the Fourth Amendment right to be free from unreasonable search and seizure is an individual right that "protects people, not places."[5] When drafting the Fourth Amendment, the framers could not have anticipated technological advances such as e-mail and other forms of electronic communications that would later arise and be used by the public.[6] Similarly, they could not have envisioned the new modes of surveillance that would become available for government use in investigating crime.[7] However, the framers did intend to protect individuals from unreasonable government interference,[8] and, consequently, courts continually have had to interpret the broad language of

1. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C §§ 2510–22, 2701–12, 3121–27 (2006)); *see also infra* Part I.C.

2. *See infra* Part I.C.

3. *See infra* Part II.B.

4. U.S. CONST. amend. IV.

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

6. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 115, 118–19 (1999).

7. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450–52 (1989) (holding that aerial surveillance of an individual's home from a helicopter does not violate the Fourth Amendment).

8. *See* LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 150 (1999).

this amendment in light of new technological and social developments in order to define the scope of the protections it offers.[9]

The Supreme Court has recognized that, apart from the specific items enumerated, "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[10] "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property."[11]

Government agents typically must obtain a warrant specifying the area to be searched and the items to be seized before they may conduct a search to comply with the requirements of the Fourth Amendment.[12] The Framers abhorred general warrants and writs of assistance,[13] and, to ameliorate these concerns, required that government agents obtain warrants supported by probable cause before conducting searches.[14] The Constitution incorporates this concern by requiring that "no Warrants shall issue" unless they "particularly describ[e] the place to be searched, and the persons or things to be seized."[15] The specificity requirement prevents agents from engaging in "fishing expeditions" that were possible under general warrants.[16]

---

9. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (concluding that the use of a thermal imager to detect heat radiating from a home is a search within the meaning of the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that aerial surveillance of a home is not a search in an age "where private and commercial flight in the public airways is routine"); *Katz*, 389 U.S. at 352–53 (recognizing that telephone conversations are protected under the Fourth Amendment); *see also infra* Part I.B.

10. Schmerber v. California, 384 U.S. 757, 767 (1966) (finding no Fourth Amendment violation where a police officer directed a physician to draw a blood sample from a person suspected of drunk driving).

11. Boyd v. United States, 116 U.S. 616, 630 (1886) (holding that forcing a criminal defendant to produce incriminating documents is a search within the meaning of the Fourth Amendment).

12. U.S. CONST. amend. IV; *see, e.g.*, Maryland v. Dyson, 527 U.S. 465, 466 (1999) (noting that "[t]he Fourth Amendment generally requires police to secure a warrant before conducting a search"). The primary exception to the warrant requirement is for situations involving exigent circumstances where the law enforcement officer does not have time to procure a warrant because of dangerous conditions, possible disappearance of evidence, or other similar concerns. *See, e.g.*, *Schmerber*, 384 U.S. at 770. For a discussion of practical examples stemming from this exception, see Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473–74 (1985).

13. Writs of assistance were generally used in support of customs and excise investigations and enabled the bearer to search any and all houses he or she suspected might contain probative evidence. *See generally* William J. Cuddihy, *"A Man's House Is His Castle": New Light on an Old Case*, REVS. IN AM. HIST., Mar. 1979, at 64, 64–69.

14. *See* LEVY, *supra* note 8, at 158; Cuddihy, *supra* note 13, at 64–69.

15. U.S. CONST. amend. IV.

16. *See* Louis Fisher, *Congress and the Fourth Amendment*, 21 GA. L. REV. 107, 115 (1986) ("The spirit and letter of the fourth amendment counselled against the belief that Congress intended to authorize a 'fishing expedition' into private papers on the possibility that they might disclose a crime."). The warrant requirement is not a mere technicality, but strikes the appropriate balance between the rights of individuals to be free from unreasonable searches and the government's need to uncover probative evidence. *See, e.g.*, Brinegar v.

In spite of the broad protection the Fourth Amendment offers from warrantless searches, not all government actions that uncover probative evidence are "searches" within the meaning of the Fourth Amendment,[17] and the Fourth Amendment does not protect individuals from searches in all areas.[18] Justice John Marshall Harlan II, concurring in the judgment in *Katz v. United States*,[19] suggested that individuals are protected by the Fourth Amendment in only those areas where they have both a subjective expectation of privacy and that expectation is objectively reasonable.[20] *Katz* arose when government agents used an electronic surveillance device attached to the exterior of a phone booth to eavesdrop on the caller's conversation.[21] Although not explicitly enumerated in the text of the Fourth Amendment, the majority concluded that an individual using a public phone booth is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," and found that the contents of phone conversations are protected under the Fourth Amendment.[22]

The Supreme Court has since embraced Justice Harlan's two-prong approach for determining the scope of Fourth Amendment protections.[23] A subjective expectation of privacy alone is insufficient to create a privacy right, because, as the Court noted, regardless of how private he believes his actions are, a burglar in an abandoned summer cabin should not be protected by the Fourth Amendment.[24] In that situation, any subjective expectation of privacy the burglar might have is not one society recognizes as reasonable.[25] Although the Court stressed that when considering whether an expectation of privacy is reasonable, "arcane distinctions developed in property and tort law . . . ought not to control," the expectation must be one that has a source outside the Fourth Amendment.[26] This is a flexible test designed to account for the many varied situations under which Fourth Amendment searches may take place.[27] However, inherent in the flexibility is a level of uncertainty as to the extent of protection in areas the

---

United States, 338 U.S. 160, 176 (1949). Additionally, the Fourth Amendment's exclusionary rule offers strong protections to those whose rights have been violated by barring the government from using any illegally obtained evidence. Mapp v. Ohio, 367 U.S. 643, 657–58 (1961).

17. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 408–09 (2005) (holding that a drug-detecting dog's sniff is not a search).

18. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 148 (1978) (holding that passengers in a car are not entitled to Fourth Amendment protection for search of the car).

19. 389 U.S. 347 (1967).

20. *See id.* at 361 (Harlan, J., concurring).

21. *Id.* at 348 (majority opinion).

22. *Id.* at 352.

23. *See, e.g.*, *Rakas*, 439 U.S. at 151 (Powell, J., concurring).

24. *Id.* at 143 & n.12 (majority opinion).

25. *Id.*

26. *Id.* at 143.

27. *See, e.g.*, Cecil J. Hunt II, *Calling in the Dogs: Suspicionless Sniff Searches and Reasonable Expectations of Privacy*, 56 CASE W. RES. L. REV. 285, 313–14 (2005).

Supreme Court has not previously considered, particularly in new media such as electronic communications.[28]

Katz did, however, affirm that individuals do not have reasonable expectations of privacy and, therefore, are not protected by the Fourth Amendment, where they voluntarily expose items to public view.[29] From this premise, the Court has developed a third-party exception that finds that individuals do not have reasonable expectations of privacy in items turned over to third parties, and that the Fourth Amendment therefore does not govern search and seizure of items in a third party's possession.[30]

E-mail and other forms of electronic communications are transmitted over servers which are frequently run by third parties. For example, if we were to imagine that Jeremy used the free e-mail account provided by his Internet service provider (ISP) to compose an e-mail to his friend Richard at Richard's work e-mail account, the message would go from Jeremy's computer, through his ISP's servers and over the Internet, to the mail server run either by Richard's company or another third-party ISP. The message will then be directed to Richard's mailbox, where it will sit until he attempts to retrieve it. When Richard downloads the message, if he wants to forward it to his coworker James, the message will go up from Richard's computer to the server run by his firm, and into James's mailbox.[31] Although Richard is the only intended initial recipient of Jeremy's e-mail message, the message passes through Jeremy's ISP's server, where administrators have the technical capability to inspect the contents of the message. However, when Richard forwards that same message to James at an address inside his firm, the message stays on the firm's e-mail server and does not pass through the hands of any third parties.[32]

Many e-mail messages, such as the hypothetical one discussed above from Jeremy to Richard, are sent through free, public services or pass through servers run by third-party ISPs at many points during transmission. This third-party interaction with the communication complicates Fourth Amendment analysis.[33]

---

28. *See* Kyllo v. United States, 533 U.S. 27, 43 (2001) (Stevens, J., dissenting); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188.

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

30. *See infra* Part I.A.

31. For a more detailed description of how e-mail works, see Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1562–63 (2004); Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1050–51 (2008); *see also* Wikipedia, E-Mail, http://en.wikipedia.org/wiki/Email (last visited Aug. 20, 2009).

32. There is, of course, the possibility that Richard and James's office will not run its own mail server, but will rely on the services provided by a third party ISP.

33. *See infra* Part I.A–B.

A. *The Third-Party Doctrine*

The Fourth Amendment may protect an individual from unreasonable searches of items she seeks to maintain as private, but the Supreme Court has in several cases adopted a "Third-Party Doctrine," which finds that an individual no longer has such an expectation of privacy where the items in question are voluntarily turned over to third parties.[34] For example, the Court found that the infamous president of the Teamster's Union, James "Jimmy" Hoffa, could not assert a Fourth Amendment challenge to suppress statements he voluntarily made to a third party who later turned and communicated the substance of those conversations to government agents.[35] Hoffa made the incriminating statements in his hotel room to an associate Edward Partin, who Hoffa expected would keep the information private.[36] However, in doing so the Court noted that Hoffa was "not relying on the security of the hotel room; he was relying upon his misplaced confidence that Partin would not reveal his wrongdoing."[37] In this situation, Hoffa voluntarily turned the information over to the third party and, therefore, could not control that individual's use of the information or later complain if he chose to inform others, notably the government, about it.[38]

Based on decisions like *United States v. Hoffa*,[39] the government is free to subpoena messages from their intended recipients without implicating the Fourth Amendment. However, individuals do not forfeit all Fourth Amendment protections merely by conveying some information to third parties.[40] Particularly in light of new technology and new forms of communication and surveillance, as present in *Katz*, the Supreme Court has had to balance these competing interests to determine the extent of an individual's protections.

Applying the principles of *Hoffa*, and focusing on information directed to third parties, the Court carved out an exception to the otherwise strong protections afforded to telephone conversations[41] and postal mail[42] for delivery and routing information that is directly conveyed to third parties for their use in connecting and delivering the communications.[43] The Court

34. For a defense of this doctrine, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

35. United States v. Hoffa, 385 U.S. 293, 302–03 (1966).

36. *Id.* at 302.

37. *Id.*

38. *Id.* at 302–03. The Court also relied on its earlier decision in *Lopez v. United States*, 373 U.S. 427 (1963), which noted that the risk of being "betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak." *Id.* at 465 (Brennan, J., dissenting).

39. 385 U.S. 293.

40. *See infra* notes 136–37 and accompanying text.

41. *See infra* Part I.B.1.b.

42. *See infra* Part I.B.2.

43. *See infra* Part I.A.1.

similarly held that other information voluntarily conveyed to third parties and stored in their databases is not protected by the Fourth Amendment.[44]

1. Delivery and Routing Information Directly Conveyed to Third Parties

After *Katz*, although phone companies have the technical sophistication to easily listen to or record phone conversations,[45] the content of these conversations is protected under the Fourth Amendment.[46] However, in *Smith v. Maryland*,[47] the Supreme Court approved the government's use of pen registers[48] to track the telephone numbers individuals dialed.[49] In contrast to the strong protections for the substance of phone conversations, the Court concluded that individuals do not have reasonable expectations of privacy in the numbers dialed since they voluntarily convey this information to the phone company.[50] The Court inferred from the fact that customers received itemized bills listing the long-distance calls they made, "[t]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[51] With this awareness, the Court held that, in general, individuals do not have even a subjective expectation of privacy in the phone numbers they dial.[52]

However, the Court went on to apply the second prong of the *Katz* test, and held that, even if the particular defendant in *Smith* did have a subjective expectation of privacy in the telephone numbers he dialed, it was not an expectation society recognized as reasonable in light of the telephone companies' regular practice of recording this information.[53] Therefore, the government's use of this information still would not violate the Fourth Amendment.[54]

Similarly, although postal workers could easily open and inspect the contents of the letters and packages they are delivering, these communications are strongly protected by the Fourth Amendment.[55] At the same time, the U.S. Postal Service is expected to deliver the items deposited

44. *See infra* Part I.A.2.

45. *See* HAROLD F. TIPTON & MICKI KRAUSE, INFORMATION SECURITY MANAGEMENT HANDBOOK 178 (4th ed. 2002); Wikipedia, Telephone Tapping, http://en.wikipedia.org/wiki/Telephone_tapping (last visited Aug. 20, 2009).

46. *See* Katz v. United States, 389 U.S. 347, 353 (1967); *infra* Part I.B.1.b.

47. 442 U.S. 735 (1979).

48. "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977).

49. *Smith*, 442 U.S. at 741–42.

50. *Id.* at 742.

51. *Id.* at 743.

52. *Id.* at 742.

53. *Id.* at 744–45.

54. *Id.*

55. *See infra* Part I.B.2.

with it to their intended recipients. In doing so the Postal Service is expected to, and indeed must, read the address and other information displayed on the exterior of the package.[56] Because this information is not only voluntarily turned over, but also directed to the third-party Postal Service, it is not protected by the Fourth Amendment.[57]

These decisions recognize that the mere fact that some part of a communication, such as the telephone number or delivery address, is directed to a third party, does not give that third party access to the entire communication. Additionally, although the third party may have the potential to access information in its possession, this does not suffice to bring the information within the purview of the third-party doctrine or limit Fourth Amendment protections.[58]

A limited application of the third-party doctrine to information actually conveyed to the third party is also applicable to electronic messages.[59] Electronic communications will also generally pass through servers controlled by third parties before ultimately arriving in the intended recipient's mailbox.[60] Like the Postal Service, e-mail providers' computer systems are expected to "read" some of the address information so that they may properly route and deliver the messages.[61] However, e-mail providers are not expected to review the content of the messages, and Part III of this Note concludes that, because they are only expected to read the noncontent, address information, the sender does not forfeit her Fourth Amendment rights in the content of the message.[62]

2. Records and Information Stored in Databases Managed by Third Parties

In addition to information directly conveyed to third parties for their use, many entities also maintain databases that contain information gathered from their users and customers.[63] Consistent with its decisions regarding information turned over to third parties, the Supreme Court has held that where records are entrusted to third parties, the third party's concurrent access may eliminate an individual's privacy interest and, consequently, the protections she is afforded under the Fourth Amendment. For example, in

---

56. For a description of the United States Postal Service's mail sorting system, see Wikipedia, United States Postal Service, http://en.wikipedia.org/wiki/United_States_Postal_Service (last visited Aug. 20, 2009).

57. *See Ex parte* Jackson, 96 U.S. 727, 733 (1877); *see also* United States v. Huie, 593 F.2d 14, 14–15 (5th Cir. 1979) (finding no Fourth Amendment violation in performing a "mail cover" by recording all information on exterior of mail before delivering).

58. *Cf. infra* Part I.A.2.

59. *See infra* Part II.A–B.

60. *See supra* notes 31–33 and accompanying text.

61. *See supra* notes 31–33 and accompanying text.

62. *See infra* Part III.

63. For a discussion of the vast array of information compiled in both private and public databases, see Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002).

United States v. Miller,[64] the Court concluded that individuals do not have reasonable expectations of privacy in financial records held by third parties.[65]

In *Miller*, Mitchell Miller was convicted of carrying on the business of a distiller without giving bond in an attempt to avoid the whiskey tax.[66] The government subpoenaed checks and financial records from the two banks used by Miller and relied on those documents as evidence at trial.[67] The Court held that, like Jimmy Hoffa speaking to his associate, Miller had "assumed the risk" that any documents he turned over to the bank could later find their way into the hands of the government.[68] Therefore, Miller had no reasonable expectation of privacy in their contents and could not claim the protections of the Fourth Amendment.[69]

Much like in *Smith*, where the Court held that there was no reasonable expectation of privacy in the numbers dialed because they had been "turned over" to the phone company,[70] here too, by turning his checks over to the bank, the Court concluded that Miller lost any expectation of privacy he might otherwise have had by maintaining the checks in his private possession.[71]

The agents in *Miller* actually reviewed microfilm copies of Miller's records, which further supported the Court's conclusion that the Fourth Amendment did not protect Miller in this situation because the items searched were not Miller's "private papers," but the bank's business records.[72] However, the Court then went on to note that even if the agents had viewed the originals created by Miller and held by the bank, Miller still would not have a reasonable expectation of privacy in them.[73] This is because "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions."[74] Even the deposit slips and monthly accountings were not protected because they only contained information that, according to the Court, had been "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[75]

Similarly, three years earlier, in *Couch v. United States*,[76] the Court held that an individual could not assert either Fourth or Fifth Amendment

64. 425 U.S. 435 (1976).
65. *Id.* at 442.
66. *Id.* at 436.
67. *Id.* at 437–38.
68. *Id.* at 443.
69. *Id.* ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").
70. Smith v. Maryland, 442 U.S. 735, 744 (1979); *supra* notes 47–54 and accompanying text.
71. *Miller*, 425 U.S. at 442–43.
72. *Id.* at 440.
73. *Id.* at 442.
74. *Id.*
75. *Id.*
76. 409 U.S. 322 (1973).

challenges to prevent the government from subpoenaing tax records in the possession of the individual's accountant.[77] Writing for the majority, Justice Lewis Powell found that the defendant could not have a reasonable expectation of privacy in the records she handed over to her accountant because they were in the possession of a third party, and she knew that much of the information would have to be turned over to the government while preparing her taxes.[78] However, in dissent, Justice William Douglas noticed that "[u]nder these circumstances, it hardly can be said that by giving the records to the accountant, the petitioner committed them to the public domain."[79] Unlike Justice Douglas's dissent, Justice Powell's opinion conceives of privacy under the Fourth Amendment as binary—as soon as a third party is given access to information the individual's privacy interest vanishes.[80] However, Justice Douglas recognized the societal understanding that, although a third party had access to the information, the third party was expected to keep it private and not to disseminate it freely.[81]

Like the financial institutions in *Smith* and the accountants in *Couch*, ISPs frequently maintain databases containing personal and transactional information about their users, and often store and archive copies of the electronic communications they process.[82] Many individuals also use Internet-based e-mail (Webmail) systems where all of their messages are stored in electronic mailboxes on their e-mail providers' remote servers.[83] Some lower courts have taken an expansive view of the third-party exception, and have found that individuals do not have reasonable expectations of privacy in credit card statements,[84] utility records,[85] motel registration records,[86] or employment records.[87] Some information in these databases, such as subscriber information, is directly conveyed to the ISP for its use, and is not protected by the Fourth Amendment after *Miller*.[88] However, even though other information, such as archival or backup copies of messages, are not stored by the ISP for its use, an expansive interpretation of the third-party doctrine could potentially eliminate a user's Fourth Amendment protections for this information.[89]

---

77. *Id.* at 335–36.
78. *Id.* at 335.
79. *See id.* at 340 (Douglas, J., dissenting).
80. *See id.* at 329 (majority opinion).
81. *Id.*
82. *See infra* notes 257–59 and accompanying text.
83. *See infra* notes 251–59 and accompanying text.
84. United States v. Phibbs, 999 F.2d 1053, 1077–78 (6th Cir. 1993).
85. United States v. Starkweather, No. 91-30354, 1992 WL 204005, at *1–2 (9th Cir. Aug. 24, 1992); United States v. Porco, 842 F. Supp. 1393, 1398 (D. Wyo. 1994).
86. United States v. Willis, 759 F.2d 1486, 1498 (11th Cir. 1985).
87. United States v. Hamilton, 434 F. Supp. 2d 974, 979–80 (D. Or. 2006).
88. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (acknowledging that "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation").
89. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 153 (2007). In the context of electronic communications, although third-party intermediaries will sometimes have access

Smith and *Miller* have been criticized over time, particularly as more personal information is incorporated into privately managed databases.[90] Private entities had already accumulated large amounts of information before *Smith* and *Miller* were decided.[91] However, with a greater number of transactions being completed electronically, far more records are being created and stored, and the universe of information contained in databases controlled by third parties is greatly expanding.[92] Since this information is currently accorded no Fourth Amendment protection, and may be accessed with a subpoena, the government frequently relies on it during criminal investigations and prosecutions.[93] Even when information culled from databases is used to combat serious threats such as terrorism, the public has not always been in favor of extensive government use of this data.[94]

---

to the information, they are generally expected not to freely divulge it. For example, GMail, a popular free e-mail provider, specifically states on their website that they do not read users' e-mail. *See* Does Google Read My Mail?, http://mail.google.com/support/bin/answer.py?answer=6599&topic=12787 (last visited Aug. 20, 2009).

90. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1137 (2002) ("*Smith* and *Miller* have been extensively criticized throughout the past several decades. . . . [They] are the new *Olmstead* and *Goldman*."); *see also* Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 85 (1974) (Douglas, J., dissenting) ("In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum."). *But see generally* Kerr, *supra* note 34 (defending the third-party doctrine).

91. *See* Kenneth L. Karst, *"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 342–43 (1966). For example, in 1960, First National Bank of Boston began using an underground bunker made of steel-reinforced concrete strong enough to survive a three megaton blast to maintain records. John H. Fenton, *Bank Constructs a Bomb Shelter*, N.Y. TIMES, Dec. 2, 1960, at 41. The facility was not designed to store money or valuables—only microfilm and duplicates of original transactions. *Id.*

92. *See, e.g.*, SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 15–16 (2000); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (1998) (comparing the different amount of information recorded when an individual visits a brick-and-mortar shopping mall and when the individual shops for the same merchandise online); *Know-alls: Datamining*, THE ECONOMIST, Sept. 27, 2008, at 73. Additionally, DNA information is increasingly being stored in government maintained databases. For a discussion of the constitutionality of DNA extraction statutes, see Charles J. Nerko, Note, *Assessing Fourth Amendment Challenges to DNA Extraction Statutes after* Samson v. California, 77 FORDHAM L. REV. 917 (2008).

93. *See, e.g.*, United States v. Miller, 425 U.S. 435, 444 (1976); Walker v. S.W.I.F.T. SCRL, 491 F. Supp. 2d 781, 785–86 (N.D. Ill. 2007) (subpoenaing financial information for terrorist tracking); United States v. Lazar, No. 04-20017, 2006 WL 3761803, at *1 (W.D. Tenn. Dec. 20, 2006) (denying motion to suppress illegally subpoenaed healthcare records). For a detailed discussion of the evolution of the third-party doctrine and Justice John Paul Stevens's views on the subject, see Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731 (2006).

94. For example, in the wake of the September 11 terrorist attacks, the Department of Defense began the Total Information Awareness Project (T.I.A.) to help anticipate and stop terrorist attacks based on information culled from databases. *See* Jeffrey Rosen, *The Year in Ideas: Total Information Awareness*, N.Y. TIMES, Dec. 15, 2002, at E65; American Civil Liberties Union, Q&A on the Pentagon's "Total Information Awareness" Program (Apr. 20, 2003), http://www.aclu.org/privacy/spying/15578res20030420.html. However, just a few years later, in response to concerns that aggregating all this information posed a threat to

In light of the rapidly expanding universe of information turned over to third parties, an expansive interpretation of *Miller* permits easy access to a tremendous amount of information. In its later decisions involving these issues, the Supreme Court began to recognize some of the potential problems stemming from the increased pooling of information in databases. For example, in *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[95] a CBS news correspondent made a request under the Freedom of Information Act to obtain information about the members of the Medico family contained in their "rap sheets."[96] The Court noted that, in spite of the fact that much of the information summarized in the rap sheets may have been public at one time, there was still a privacy interest in preventing disclosure of the compilation.[97] More relevant to the Fourth Amendment inquiry, the majority also recognized that "[i]n an organized society, there are few facts that are not at one time or another divulged to another."[98] The Court also concluded that privacy and the "Third Party Doctrine" are, for Fourth Amendment purposes, not binary, and "'the fact that an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information.'"[99] This approach is more analogous to the theory proposed several years earlier by Justice Douglas in *Couch*.[100] In the arena of electronic communications, because ISPs are generally expected to keep communications private, it limits arguments that electronic communications are not protected under the Fourth Amendment merely because a third party retains backup or archival copies on its server. This analysis also comports with the distinction drawn in *Smith* and *Katz* between information actually turned over to the phone company for its use, and information merely in its possession.[101]

B. *Fourth Amendment Standards Evolve with Technology*

As technology evolves, giving individuals new forms of communicating and government agents increasingly sophisticated tools for surveillance, courts have had to continually interpret the Fourth Amendment and define the extent of its reach in light of these new advances. When writing for the majority in *Kyllo v. United States*,[102] even Justice Antonin Scalia, a staunch

---

personal privacy, Congress halted the project. Adam Clymer, *Congress Agrees To Bar Pentagon from Terror Watch of Americans*, N.Y. TIMES, Feb. 12, 2003, at A1.

95. 489 U.S. 749 (1989).

96. *Id.* at 757.

97. *Id.* at 762–63, 767 (noting there is a "privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public").

98. *Id.* at 763.

99. *Id.* at 770 (quoting William H. Rehnquist, Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?, Nelson Timothy Stephens Lecture at the University of Kansas Law School, (Sept. 26–27, 1974).

100. *Cf.* Couch v. United States, 409 U.S. 322, 335–36 (1973).

101. *See supra* notes 49–58 and accompanying text.

102. 533 U.S. 27 (2001).

believer in originalism,[103] remarked on the dangers that would flow if the Fourth Amendment was not construed in a flexible manner.[104] In particular, the Supreme Court considered the applicability of the Fourth Amendment to telephone conversations and postal mail, and in both cases concluded that the contents of the communication were protected by the Fourth Amendment.[105] Additionally, although never decided in a reported judicial decision, commentators at the time argued that telegraph messages should also be protected under the Fourth Amendment.[106]

1. Telephone Conversations

The Supreme Court has not always been as responsive to evolving technology as it was in *Kyllo*.[107] In 1928, the Court first considered whether telephone conversations were protected by the Fourth Amendment, and concluded they were not.[108] It was not until almost forty years later when the Supreme Court reconsidered this important question and, in light of the growing importance of the telephone, concluded the Fourth Amendment did extend to these communications.[109]

a. *Olmstead v. United States*

In *Olmstead v. United States*,[110] federal agents discovered Roy Olmstead was involved in an illegal conspiracy to distribute intoxicating liquors after listening in to conversations between Olmstead and his coconspirators.[111] The agents had tapped Olmstead and his coconspirators' telephones without entering onto private property.[112] Focusing on the elements of trespass, the Court concluded that "the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched."[113]

However, in dissent, Justice Louis Brandeis expressed his belief that in expounding the Constitution, the Court should not be so constrained by the

---

103. For example, *see* Scott Turow, *Scalia the Civil Libertarian?*, N.Y. TIMES MAG., Nov. 26, 2006, at 22. Turow notes that "[t]o Scalia, the Bill of Rights means exactly what it did in 1791, no more, no less. The needs of an evolving society, he says, should be addressed by legislation rather than the courts." *Id.*

104. *Kyllo*, 533 U.S. at 35–36 (rejecting a mechanical interpretation of the Fourth Amendment).

105. *See infra* Part I.B.1–2.

106. *See infra* Part I.B.3.

107. *See supra* note 104 and accompanying text.

108. *See infra* Part I.B.1.a.

109. *See infra* Part I.B.1.b.

110. 277 U.S. 438 (1928).

111. *Id.* at 456; *see also* Mabel Walker Willebrandt, *The Inside of Prohibition*, N.Y. TIMES, Aug. 19, 1929, at 14.

112. *Olmstead*, 277 U.S. at 464.

113. *Id.* at 465.

limited scope of what the forefathers anticipated.[114] Even in 1928, Justice Brandeis recognized that

> [t]he 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.[115]

Justice Brandeis's premonition did not then carry the day, and the Court's five-to-four decision in *Olmstead* left law enforcement free to eavesdrop on telephone conversations.[116] However, as the government increasingly relied on information gleaned from wiretaps, the public began to question the majority's wisdom in condoning this activity.[117]

b. *Katz v. United States*

Although telephones were widely used when *Olmstead* was decided,[118] the telephone became increasingly important to daily life over time, and, almost forty years later, a situation similar to that in *Olmstead* arose in *Katz v. United States*.[119] This time, however, the Court came to a different conclusion. In *Katz*, government agents attached an electronic surveillance device to the exterior of a public phone booth and used it to eavesdrop on Charles Katz's conversation.[120] Agents overheard Katz placing bets and obtaining gambling information, and used the information garnered from these conversations against him at trial.[121] In contrast to *Olmstead*, the *Katz* Court rejected the government's argument that because there was no physical entry into the phone booth, and therefore no trespass, the

---

114. *Id.* at 472 (Brandeis, J., dissenting).

115. *Id.* at 474.

116. *See, e.g.*, United States v. Nardone, 106 F.2d 41, 43–44 (2d Cir. 1939) (relying on *Olmstead* and approving law enforcement use of wiretaps); Valli v. United States, 94 F.2d 687, 691 (1st Cir. 1938) (same).

117. *See, e.g.*, Anthony Lewis, *Tangled Issue of Wiretapping*, N.Y. TIMES, Aug. 21, 1960, at SM18. *But see Dewey Approves Wiretapping Curb*, N.Y. TIMES, June 17, 1938, at 7 (arguing that stronger laws regulating wiretapping would only protect "gangsters and criminals"). Just six years after *Olmstead*, Congress enacted legislation making wiretapping a federal crime. Federal Communications Act of 1934, Pub. L. No. 90-351, 82 Stat. 223, (repealed 1947). However, § 605 did not apply to wiretapping by state actors and did not cover bugging or other forms of surveillance. *See* Solove, *supra* note 90, at 1138–39. Although recognized as an important step practically, this legislation did little to affect government surveillance, and commentators urged Congress and the courts to enact broader protections. *See* Alan F. Westin, *Science, Privacy and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1205, 1223–32 (1966).

118. *See* RUTH SCHWARTZ COWAN, A SOCIAL HISTORY OF AMERICAN TECHNOLOGY 161–62 (1997).

119. 389 U.S. 347 (1967).

120. *Id.* at 348.

121. *See id.* For a more detailed description of the factual underpinnings, see *Katz v. United States*, 369 F.2d 130, 131–32 (9th Cir. 1966).

surveillance did not implicate the Fourth Amendment.[122] Even though privacy in phone booths was not explicitly enumerated in the text of the Fourth Amendment, the majority concluded that an individual using a public phone booth is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[123] Recognizing the importance of, and widespread reliance on, this new technology, the Court noted that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[124]

By abandoning its previous approach to the Fourth Amendment, which focused on physical trespass, the Court recognized the importance the telephone had come to have in society.[125] In doing so, *Katz* corrected the Court's previous error in *Olmstead*, which placed substantial emphasis on historical usages and failed to consider the practical import of the government's actions.[126] Critics have noted that, in contrast to *Katz*, *Olmstead* "symbolizes the Court's lack of responsiveness to new technology, unwarranted formalism in its constitutional interpretation, and failure to see the larger purposes of the Fourth Amendment."[127] Additionally, *Katz* is notable for Justice Harlan's concurrence suggesting that individuals are protected by the Fourth Amendment in areas where they have a subjective expectation of privacy as long as that expectation of privacy is objectively reasonable.[128]

Although *Katz* was decided three years before *Smith*, the two decisions demonstrate the limits of the third-party doctrine. While an entire phone call—numbers dialed and content of the conversation—is "turned over" to a third-party telephone company, these decisions acknowledge that the third-party exception does not give government agents unbridled access to the entire call.[129] The telephone number dialed is directly conveyed to the phone company so that it may connect (and bill for) the call,[130] but the

122. *Katz*, 389 U.S. at 353. The Court went on to note that "the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." *Id.*

123. *Id.* at 352.

124. *Id.*

125. *Id.*

126. *See* Solove, *supra* note 90, at 1086 (describing *Olmstead* as "a relic of the past, a long discredited decision"); *see also* Fred P. Graham, *High Court Eases Curbs on Bugging; Adds Safeguard*, N.Y. TIMES, Dec. 19, 1967, at 1.

127. Solove, *supra* note 90, at 1086.

128. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also supra* notes 18–20 and accompanying text.

129. *See supra* notes 49–58 and accompanying text. Similarly, even though § 605 of the Wiretap Act was not successful in limiting government eavesdropping, it recognized the importance of restricting private wiretapping. *See supra* note 117.

130. For a discussion of the history of telephone networks from manually connected operator switchboards to present-day digital switching, see Wikipedia, Telephone Exchange, http://en.wikipedia.org/wiki/Telephone_exchange (last visited Aug. 20, 2009). For a detailed technical discussion of how telephone calls are connected and routed, see STEPHEN J. BIGELOW ET AL., UNDERSTANDING TELEPHONE ELECTRONICS (4th ed. 2001).

content of the call is not similarly directed.[131] Even though both the number dialed and content of the phone conversation pass through the third party, the content of the phone call is not "turned over" in the same way that the telephone number dialed is. *Katz* recognizes that Fourth Amendment protections for the content of the conversation are not diminished simply because the content passes through the third-party-intermediary phone company.[132]

E-mail plays a central role in daily life and is used in place of postal mail or the telephone for many communications.[133] Just as the increased use and importance of the telephone played into the Court's constitutional analysis in *Katz*, the importance of modern day electronic communications also should inform the constitutional analysis. Additionally, the distinction between the strong protections offered for the content of phone conversations and the far weaker protections offered for numbers dialed demonstrates the boundaries of the third-party doctrine. This distinction also demonstrates that law enforcement cannot parlay a third party's limited access to one part of an item into access to all of it.[134]

2. Postal Mail

The Supreme Court reached a very similar result to the decision it would later reach in *Katz* when, in *Ex parte Jackson*,[135] it held that the Fourth Amendment protects the contents of letters and packages deposited in the U.S. mail system.[136] The text of the Fourth Amendment specifically includes "papers," and the Court concluded that "[t]he constitutional guaranty of the right of the people to be secure in their papers against

131. *Compare Katz*, 389 U.S. at 352 (holding that the contents of telephone conversations are protected under the Fourth Amendment), *with* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (concluding that the telephone numbers an individual dials are not protected under the Fourth Amendment because they are conveyed to the third-party telephone company).

132. *Cf. supra* notes 49–54 and accompanying text. This result does not change even though the phone company has the technological sophistication to, and could quite easily, eavesdrop on the phone conversation. *See supra* note 45 and accompanying text. In the mid-1990s, however, several circuit courts held that individuals did not have reasonable expectations of privacy in the contents of conversations made using cordless telephones. *See, e.g.*, United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992); Tyler v. Berodt, 877 F.2d 705, 706–07 (8th Cir. 1989). Early cordless telephones used radio frequencies to communicate and conversations could easily be intercepted by third parties within range. *See* BRAD GRAHAM & KATHY MCGOWAN, 101 SPY GADGETS FOR THE EVIL GENIUS 165–66 (2006); *see also Smith*, 978 F.2d at 178. These courts considered the details of how the technology worked and found that, because the cordless telephone systems could be easily intercepted, it was not reasonable for the user to expect privacy. *See Smith*, 978 F.2d at 180. Surprisingly, although the court noted that the materials to tap a regular phone could be readily purchased for under twenty-five dollars, they did not find that this reduced an individual's expectation of privacy in wired communications. *Id.* at 179 n.10.

133. *See infra* notes 251–54 and accompanying text.

134. *See supra* notes 129–32 and accompanying text.

135. 96 U.S. 727 (1877).

136. *Id.* at 733.

unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[137]

Notably, postal mail, like e-mail, is turned over to third parties who are physically capable of opening and inspecting the contents of the letters they have been given to deliver. During the colonial period individuals traditionally used wax to seal their letters, but this wax was ineffective and often failed to keep the letters securely closed.[138] Despite attempts to ensure that the mails would remain private,[139] the public widely believed they were not secure, which prompted a number of prominent individuals to write in code in an attempt to keep their communications private.[140] Thomas Jefferson, for example, remarked in a letter that "the infidelities of the post office and the circumstances of the times are against my writing fully and freely."[141] In response to these concerns, Congress passed several laws prohibiting the improper opening of mail,[142] but, despite the reality that mail was not being kept private, the Supreme Court ultimately held that Fourth Amendment protections extended to include postal mail.[143]

Particularly in light of these factual underpinnings, Professor Daniel J. Solove suggests that the Court's decision was more than just a recognition of an existing privacy interest, but was an example of the Court constructing a privacy interest that was necessary to preserve the integral role the mails had come to play in society.[144] Justice Joseph Story believed, just as Thomas Jefferson had, that individuals would not be completely candid in their correspondence without having an expectation of privacy.[145] In such a situation, Justice Story anticipated that the public would simply stop using the mails "to the detriment of the 'well-being of society,'" resulting in slowed economic growth and unnecessary burdens being placed on commercial transactions forced to use less effective means of communication.[146]

---

137. *Id.*

138. *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 56 (2000); *see also* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1142–43 (2002). A *New York Times* editorial from the period remarked on the lack of security for postal mails, noting "[t]he ordinary letter, sealed with its red wafer, and into which the prying eyes of the village postmistress so often peeped." *Writing—By the Card*, N.Y. TIMES, July 10, 1873, at 4.

139. For example, Benjamin Franklin was in charge of the colonial mails and required all of his employees to swear an oath not to open the mail. SMITH, *supra* note 138, at 49; David J. Seipp, *The Right to Privacy in American History* 13 (Harvard Univ., Working Paper No. W-77-5, 1977).

140. SMITH, *supra* note 138, at 50–51; *see also* Seipp, *supra* note 139, at 12–24.

141. Letter from Thomas Jefferson to John Taylor (Nov. 26, 1978), *in* 7 THE WRITINGS OF THOMAS JEFFERSON, at 309 (Paul Leicester Ford ed., 1905).

142. SMITH, *supra* note 138, at 50–51.

143. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

144. *See* Solove, *supra* note 138, at 1143.

145. SMITH, *supra* note 138, at 51–52 (citing JOSEPH STORY, COMMENTARIES ON EQUITY JURISPRUDENCE 221 (2d ed. 1830)).

146. *Id.* at 51–52.

In *Ex parte Jackson*, although the Court held that the sealed contents of the communications were protected, it concluded that the address and other information on the exterior of the package were not.[147] Similarly, postcards, pamphlets, and other materials "purposely left in a condition to be examined" when deposited with the Postal Service are afforded no Fourth Amendment protections.[148] This reasoning recognizes that although the item is placed in the custody of the Postal Service, the author of a letter still retains an expectation of privacy in the contents because the Postal Service is not expected to read that information. At the same time, the Postal Service is not expected to turn a blind eye to readily visible information. Quite the contrary, it is expected to deliver the letter to its intended recipient, and in doing so must read the address and other information contained on the package.[149] While not the focus of the Court's decision, this distinction serves to protect the "content" information of a communication, and only allows the government warrantless access to the "noncontent" information. It also recognizes that depositing an item with a third party does not necessarily give that individual carte blanche to do what she wishes. In this case, although third parties theoretically could read everything, they are expected to read only the information directed to them—the information on the exterior.[150]

Although the Court in *Smith* did not discuss *Ex parte Jackson*, it reached a similar result, and together, the two cases highlight the limits of the third-party doctrine. In the case of a telephone, the number dialed is necessarily and intentionally conveyed to the phone company so that the company may complete the call.[151] Similarly, individuals expect the Postal Service to read the addresses written on the exteriors of the letters they are sending so that the letters will be delivered properly.[152] However, as the Court recognized in *Ex parte Jackson*, individuals do not expect the third-party carrier—or any other party—to read the contents of the items they are mailing.[153] These decisions highlight that a third party merely having access to an item does not suffice to bring the information within the purview of the third-party doctrine, and also recognize the importance of extending Fourth Amendment protections to dominant forms of communication.

147. *Ex parte* Jackson, 96 U.S. at 732–33; *see also* United States v. Huie, 593 F.2d 14, 14–15 (5th Cir. 1979) (holding that performing a "mail cover" and recording all information on exterior of mail before delivering does not violate the Fourth Amendment).

148. *Ex parte* Jackson, 96 U.S. at 733.

149. *Cf. supra* note 29 and accompanying text (describing *Katz's* holding that what a person voluntarily exposes to the public view is not protected by the Fourth Amendment).

150. *See Ex parte* Jackson, 96 U.S. at 733.

151. *See supra* notes 50–54 and accompanying text.

152. *See supra* note 147 and accompanying text.

153. *See supra* note 137 and accompanying text; *cf. supra* notes 138–46 and accompanying text.

3. Telegraph Messages

Telegraph transmissions share some of the characteristics of present day electronic communications, but the process of sending a telegram is far less automated and requires greater human interaction.[154] Like postal mail and e-mail, most telegrams traveled over networks run by third parties.[155] However, unlike sealed letters, telegraph messages are far more exposed to review by intermediaries while in transit.[156] Notwithstanding this reality, commentators writing while telegraphs were widely used viewed these messages as the then-modern-day equivalent of postal mail and believed that they should be protected to the same extent as the mails.[157]

After Samuel Morse demonstrated his telegraph in 1838, telegraph networks were quickly deployed across the United States and other countries, enabling people to send instantaneous messages.[158] Despite the higher cost of sending messages by telegraph, the telegraph's speed advantage displaced some business from the Post Office.[159] Users would write out their messages and hand them over to telegraph operators to encode and transmit across the telegraph lines.[160] At the other end, another operator would capture, decode, and transcribe the transmission, and then deliver the message to its intended recipient.[161] In addition to the potential for eavesdropping during transmission, telegraphy in this setting requires that the operators on both ends actually read the messages.[162] At the time, telegraph operators sought to maintain an impersonal attitude to the messages they delivered, but, particularly in small towns, they were "privy to most everything that went on in the town."[163]

During the American Civil War, the telegraph was widely used, and government officials grew concerned about security leaks.[164] To uncover treason and guard military secrets, the government seized and reviewed all

154. *See infra* notes 161–63 and accompanying text.

155. *See generally* LEWIS COE, THE TELEGRAPH (1993).

156. *See infra* notes 161–63 and accompanying text.

157. *See infra* notes 167–88 and accompanying text.

158. *See generally* James B. Calvert, The Electromagnetic Telegraph (Dec. 26, 2008), http://mysite.du.edu/~jcalvert/tel/morse/morse.htm.

159. *See id.*; *see also Over Land and Ocean*, N.Y. TIMES, May 17, 1896, at 8 (describing the development of the worldwide telegraph network and the speed at which messages can be transmitted using the telegraph).

160. *See generally* COE, *supra* note 155.

161. *See id.*; *see also, e.g.*, Peterson v. W. Union Tel. Co., 74 N.W. 1022, 1022 (Minn. 1898) (describing the process of sending a telegraph); Pegram v. W. Union Tel. Co., 2 S.E. 256, 257–58 (N.C. 1887).

162. *See* COE, *supra* note 155, at 70–71 (describing a particularly capable operator who was able to remember several minutes of transmitted messages while sharpening a pencil before transcribing); *see also Peterson*, 74 N.W. at 1022. Additionally, telegraphy students would frequently practice by listening to the wires at the local telegraph office. COE, *supra* note 155, at 107.

163. *See* COE, *supra* note 155, at 116.

164. *See* Seipp, *supra* note 139, at 46.

telegrams.[165] After the war, Congress undertook additional investigations and sought to uncover evidence from the files of telegraph operators, particularly Western Union, the primary telegraph operator at the time.[166] Members of the public were outraged when they discovered that Congress was reviewing telegraph messages.[167] Eventually, members of the legislature discovered that even their own messages were being reviewed.[168] Even though Congress promised it would keep the information it learned confidential, these assurances were not enough to appease the public's concerns.[169] In response, Western Union adopted Rule 128, which prohibited the disclosure of messages to anyone other than the intended recipient.[170]

Acting under orders from the company's president, William J. Orton, Western Union managers began to refuse government requests to turn over private telegrams, while Orton and other groups urged Congress to enact legislation to protect these messages.[171] Representative James A. Garfield, who went on to serve as the twentieth President of the United States, noted that the telegraph is, "next to the post office, the custodian of more secrets in relation to public and private affairs than any other institution on earth," and urged Congress not to require Western Union to turn over the requested telegrams.[172] On the other side, Senator Roscoe Conkling noted that the process of sending a telegraph is akin to asking a third party to deliver an oral message, and therefore one cannot expect that the message will be kept private, and cannot complain if the government requires its disclosure.[173] Other members of Congress were similarly concerned that limiting access to this evidence might unnecessarily burden criminal and other investigations.[174] In a controversial action, Congress passed a resolution requiring the telegraph managers to deliver the requested messages.[175]

In response to this action, and to protect against disclosure going forward, Western Union made arrangements to destroy messages after delivery.[176] Although this would serve to protect their communications

---

165. *See id.*

166. *See id.* at 47.

167. *See, e.g.*, *Secrets of the Telegraph*, N.Y. TIMES, June 24, 1876, at 4.

168. *See, e.g.*, *Eavesdropping Extraordinary*, N.Y. TIMES, May 18, 1874, at 4. Congress also reviewed nearly three-quarters of a ton of stored messages to find evidence during its investigation of the prominent financier Jay Cooke. Seipp, *supra* note 139, at 47–48.

169. *See, e.g.*, *Secrets of the Telegraph*, *supra*, note 167.

170. WESTERN UNION TELEGRAPH COMPANY, RULES, REGULATIONS, AND INSTRUCTIONS 55 (Cleveland 1866).

171. *See* Seipp, *supra* note 139, at 48–50.

172. 5 CONG. REC. 328 (1876) (statement of Rep. Garfield).

173. 5 CONG. REC. 445 (1877) (statement of Sen. Conckling).

174. *See* 5 CONG. REC. 477 (1877) (statement of Sen. Edmunds).

175. *Id.*; *The Investigating Committees*, N.Y. TIMES, Dec. 13, 1876, at 4; *see also* Seipp, *supra* note 139, at 51–52.

176. Seipp, *supra* note 139, at 53. Currently, Internet companies are also considering reducing the amount of time they store personally identifiable information. For example, Yahoo! used to keep search logs for thirteen months but now only retains some personally identifiable information for ninety days. *See* Press Release, Yahoo! Inc., Yahoo! Sets New

from government review, businesses were opposed to this measure as it would then be impossible to prove that Western Union had been responsible for mistakes in transmission.[177] With some Western Union managers facing imprisonment for failing to comply with congressional demands, Western Union ultimately did not destroy the messages, and complied with the requests.[178]

Eventually, prominent legal commentators like Judge Thomas M. Cooley, began to suggest that the rationale underlying finding strong Fourth Amendment protections for postal mail was equally applicable to communications by telegraph.[179] Judge Cooley also expressed his view that the law cannot limit the protection afforded to telegraph users on the theory that they could send their messages by other means.[180] Telegraph use, and the need for quick communication, had become so important that Judge Cooley remarked, "Neither is the use of the telegraph a matter of mere choice. Business transactions cannot be successfully carried on without resort to its facilities, and the exigencies of family communication are daily demanding the most speedy transmission of messages that shall be found possible."[181] With these considerations in mind, Judge Cooley concluded that "the right to have telegraphic communication protected, as that by mail is, seems unquestionable."[182] Notably, because of how they are transmitted, telegraph messages were, as Senator Conkling noted, far more akin to asking a third party to deliver a message than depositing a sealed letter with the post office.[183]

Western Union proposed a bill to protect telegraphic messages to the same extent as postal mail, and, although the bill was favorably reported out of committee, it was never passed.[184] Congress kept its authority to demand messages from the telegraph companies but limited its subpoenas to particular and germane messages.[185] Later state and federal cases considering the validity of government subpoenas only considered the statutory protections for telegraph messages and did not consider whether

---

Industry Privacy Standard with Data Retention Policy (Dec. 17, 2008), http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=354703; *see also* Miguel Helft, *Yahoo Puts New Limits on Keeping User Data*, N.Y. TIMES, Dec. 18, 2008, at B3.

177. Seipp, *supra* note 139, at 53.

178. *Id.* at 54.

179. Thomas M. Cooley, *Inviolability of Telegraphic Correspondence*, 27 AM. L. REG. 65, 71 (1879); *see also* Seipp, *supra* note 139, at 55.

180. Cooley, *supra* note 179, at 71.

181. *Id.*

182. *Id.* at 73. Judge Cooley remarked, "[i]f the [telegraph] operator can be compelled to produce them, then on the same reasons a postmaster may be brought into court and compelled to produce the undelivered postal cards for examination." *Id.* at 77.

183. *Cf. supra* notes 161–62 and accompanying text.

184. Woods & Bradley v. Frank Miller & Co., 7 N.W. 484, 484 (Iowa 1880) (noting that "[t]he contents of [telegraph] messages, unlike the contents of letters, are necessarily known to the persons engaged in transmitting them"); H.R. REP. NO. 46-1262, at 1 (2d Sess. 1880); Seipp, *supra* note 139, at 57–58.

185. Seipp, *supra* note 139, at 58.

they were protected under the Fourth Amendment. These decisions concluded that, although telegraph messages were not entitled to the same level of protection as mail, the subpoenas requesting telegraph messages must at least specify the telegram by date and subject.[186]

Several states later adopted laws forbidding the tapping and interception of telegraph messages, and by 1909 thirty states had adopted laws forbidding employees of private telegraph companies from disclosing messages to anyone other than the intended recipient.[187] However, these laws either explicitly exempted judicial subpoenas, or were interpreted to include such exceptions by the courts.[188] With the invention and widespread adoption of the telephone, telegraph use soon dropped. With decreased use, concern over government and third-party seizure of telegrams also diminished, leaving the issue unresolved.[189]

This issue arose before the Supreme Court adopted the two-part *Katz* test,[190] and the Court never decided whether telegraph messages were protected by the Fourth Amendment. But, even where telegraph operators reviewed the entire contents of the telegrams they transmitted, members of the public still expected these messages to be kept private and were outraged at government review of these communications.[191] Commentators at the time, like Judge Cooley, argued that telegraphs were the modern day analogue of postal mail, and as such, should be given the same protections of the Fourth Amendment.[192]

Modern-day electronic communications share some similarities with the way in which telegraph messages were transmitted, though e-mail messages are not nearly as exposed to the carriers as telegraph messages were.[193] The strong opposition to leaving telegraph messages unprotected further supports finding that e-mail and other electronic communications are protected under the Fourth Amendment. Additionally, the experience with telegraph messages also highlights the importance of extending strong constitutional protections to new and important modes of communication.

---

186. *Id.* at 58–59; *see In re* Storror, 63 F. 564, 567–68 (N.D. Cal. 1894); United States v. Hunter, 15 F. 712, 714–15 (N.D. Miss. 1882); W. Union Tel. Co. v. Bierhaus, 36 N.E. 161, 162–63 (Ind. App. 1894); *Ex parte* Jaynes, 12 P. 117, 117 (Cal. 1886); *Ex parte* Brown, 72 Mo. 83, 95 (1880); Nat'l Bank v. Nat'l Bank, 7 W. Va. 544, 546–47 (1874); State v. Litchfield, 58 Me. 267, 269–70 (1870).

187. Seipp, *supra* note 139, at 93–94; *see also* ALAN F. WESTIN, PRIVACY AND FREEDOM 337 (1967).

188. *E.g.*, *Woods & Bradley*, 7 N.W. at 484–85; *Ex parte* Brown, 7 Mo. App. 484, 491–92 (1879); Seipp, *supra* note 139, at 94.

189. Currently, no reported decisions appear to consider the use of telegraph messages in criminal prosecutions. Given the state of the art, it is unlikely this issue will ever be resolved. *Cf.* Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 583–84 (2007).

190. *See supra* notes 20, 23–28 and accompanying text.

191. *See supra* notes 167–70 and accompanying text.

192. *See supra* note 179 and accompanying text.

193. *See supra* note 31.

C. *Legislative Actions To Protect Electronic Communications*

In the 1980s, as electronic communications became increasingly widely used, legislators grew concerned that the existing Fourth Amendment and statutory framework left these new media vulnerable to government and private interception, and sought to enact legislation to protect them.[194] Although the 1968 Wiretap Act was only eighteen years old when the ECPA was enacted, commentators noted that the old Wiretap Act was already obsolete, and this new action was necessary to protect the important, emerging field of electronic communications.[195]

1. Motivation for the Electronic Communications Privacy Act

At the request of the House Committee on the Judiciary, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, and the Senate Committee on Governmental Affairs, the Office of Technology Assessment (OTA)[196] created a report summarizing the current protections available to electronic communications.[197] The OTA Report found that current protections for electronic mail were "weak, ambiguous, or nonexistent,"[198] and concluded that "[t]he existing statutory framework and judicial interpretations thereof do not adequately cover new and emerging electronic surveillance technologies."[199] In part because of the Supreme Court's treatment of information conveyed to third parties, when Congress enacted the ECPA it was unclear whether users maintained reasonable expectations of privacy in remotely stored files such that they would be protected under the Fourth Amendment.[200] Consequently, Congress wanted to ensure that these communications could not be freely seized.[201]

The OTA Report began by noting that "[a]lthough the principle of the fourth amendment is timeless, its application has not kept abreast of current

194. *See Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 11 (1986) (letter from Sen. Patrick Leahy to Honorable William French Smith, Att'y Gen. of the United States (Jan. 26, 1984)); *see also New Law To Protect Consumer Data Sought*, N.Y. TIMES, Sept. 19, 1985, at A18.

195. *See* Linda Greenhouse, *The Wiretapping Law Needs Some Renovation*, N.Y. TIMES, June 1, 1986, at E4.

196. The Office of Technology Assessment was a nonpartisan agency established in 1972 to assist Congress with complex and highly technical issues that affect society. The office closed in September 1995 when Congress withdrew funding. *See* The OTA Legacy, http://www.princeton.edu/~ota/ (last visited Aug. 20, 2009).

197. OFFICE OF TECHNOLOGY ASSESSMENT, OTA-CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985) [hereinafter OTA REPORT].

198. *Id.* at 29.

199. *Id.* at 10.

200. *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, 1208 (2004); *see also supra* notes 20, 23–28 and accompanying text.

201. *See infra* notes 216–19 and accompanying text.

technologies."[202] The report discussed government surveillance of several different methods of electronic communications, and recognizes the increasing importance of e-mail.[203] The report also noted that in attempting to define the level of protection that should be afforded to new technologies, it is helpful to compare to them to their pre-electronic analogues.[204] In the case of e-mail, the report concluded that the analogue is first class mail, which is afforded strong Fourth Amendment protections.[205]

In spite of the inherent unpredictability of the *Katz* test, and the possible applicability of the third-party doctrine, the report concluded that a sender's messages will likely be protected by the Fourth Amendment while stored on her computer or in her remote electronic mailbox.[206] Similarly, the recipient would also enjoy protection under the Fourth Amendment while the message is stored either in an electronic mailbox on his personal computer or in an electronic mailbox on his e-mail provider's server.[207] Although the report concluded that the existing constitutional and statutory framework did not protect messages while in transit,[208] it recognized that the information conveyed in these messages may be personal and that, in general, individuals expect that the contents will remain private among the group with whom they are communicating.[209] The OTA Report also considered that, as a practical matter, e-mail providers have access to the communications and frequently retain copies of messages in their databases for backup protection and billing purposes.[210] After *Miller*, the OTA Report noted that these additional copies may limit an individual's Fourth Amendment protections.[211]

The OTA Report proposed three possible paths for Congress to pursue: (1) legislate to ensure e-mail has the same degree of protection as first class mail; (2) give protection to the message while in the sender's and recipient's electronic mailboxes, but not specifically legislate to define the protection afforded during transmission, and instead rely on the existing aural limitation in Title III; or (3) wait to see how the e-mail market and

202. OTA REPORT, *supra* note 197, at 3. The report noted that, although the *Katz* standard for determining the extent of Fourth Amendment protections is broad and flexible, reasonable expectation of privacy is "nebulous" and predicting its meaning in new contexts is difficult. *Id.* at 17–18.

203. *See id.* at 45–46.

204. *See id.* at 51; *cf.* notes 179–82 and accompanying text.

205. *See* OTA REPORT, *supra* note 197, at 51; *see also supra* notes 136–37, 147–48 and accompanying text.

206. *See* OTA REPORT, *supra* note 197, at 48–49.

207. *See id.* at 48–50. Although the report recognized the limited protection for records stored by third parties after *Miller*, it did not find that it worked to reduce an individual's expectation of privacy in her electronic communications. *See id.* at 50; *cf. supra* notes 65–75.

208. *See* OTA REPORT, *supra* note 197, at 49.

209. *See id.* at 50.

210. *See id.*

211. *See id.*; SLOBOGIN, *supra* note 89, at 153; *see also supra* Part I.A.2.

case law develop to see if any action is necessary.[212] Under any approach, the OTA Report recognized that intercepting a large quantity of e-mail may constitute a fishing expedition[213] and that, regardless of where it is intercepted, because the communications are electronic and there are in effect an infinite number of "copies," it may be difficult or impossible for the user to tell if a message has been seized.[214] The report also concluded that "given the high threat to civil liberties posed by interception of electronic mail . . . the governmental interest in interception would have to be quite compelling" to justify interception.[215]

At a subcommittee hearing, Representative from Wisconsin and Chairman of the House Judiciary Subcommittee Robert Kastenmeier noted that "new modes of communication have outstripped the legal protection provided under statutory definitions bound by old technologies. The unfortunate result is that the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the Government."[216] Representative Kastenmeier went on to say that "Congress needs to act to ensure that the new technological equivalents of telephone calls, telegrams, and mail are afforded the same protection provided to conventional communications."[217] Senator Patrick Leahy also participated in developing the ECPA, and during the hearing recognized that, although we may have shifted to a new form of communication, the public's privacy interest in its communications has not changed.[218] Senator Leahy remarked that the "rules don't change at all. The technology changes. All the legislation does is to make sure that the rules stay consistent with the technology."[219]

Introducing the ECPA to the House of Representatives, Representative Kastenmeier explained that the "Act updates existing Federal wiretapping law to take into account new forms of electronic communications such as electronic mail, cellular telephones, and data transmission by providing such communications with protection against improper interception."[220] The Act was designed to provide broad protection in this quickly evolving and largely unknown field, and Representative Kastenmeier justified the broad scope by explaining that "[a]ny attempt to write a law which tries to

212. *See* OTA REPORT, *supra* note 197, at 51–52.

213. *See id.* at 50; *cf. supra* notes 12–16 and accompanying text.

214. *See* OTA REPORT, *supra* note 197, at 51; *cf.* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (anticipating technology would evolve to permit "the Government, without removing papers from secret drawers, [to] reproduce them in court").

215. *See* OTA REPORT, *supra* note 197, at 51.

216. *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 1 (1986) (statement of Rep. Kastenmeier, Chairman, Subcomm. on Courts, Civil Liberties and the Admin. of Justice of the H. Comm. on the Judiciary).

217. *Id.* at 2.

218. *Id.* at 18 (statement of Sen. Leahy, Vice Chairman S. Select Comm. on Intelligence).

219. *Id.*

220. 132 CONG. REC. 14,885 (1986) (statement of Rep. Kastenmeier).

protect only those technologies which exist in the marketplace today . . . is destined to be outmoded within a few years."[221] Although focused on electronic communications, the act recognized that the goal was to protect the "sanctity and privacy of the communication" itself.[222] Despite its attempt to protect communications broadly, commentators have noted that the ECPA's provisions are narrow, and that it is not a "catch-all" designed to provide general protections to all computers and computer networks.[223]

The ECPA enjoyed strong support from both the House and the Senate, and from industry and the public when it was enacted.[224] The OTA report and statements from the bill's sponsors all suggest that Congress sought to provide broad protection to electronic communications so that they were at least as strongly protected as traditional forms of communication such as first class mail and telephone calls.[225]

2. The Electronic Communications Privacy Act Framework

The ECPA was enacted in 1986, amending Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[226] and has not been significantly modified since.[227] The Act contains three main sections: Title I protects wire, oral, and electronic communications while in transit (Wiretap Act);[228] Title II contains the Stored Communications Act (SCA), which protects communications held in electronic storage;[229] and Title III restricts the use of pen registers (Pen Register Act).[230] The section relevant to the protection of e-mails, text messages, and other forms of electronic communications is Title II—the SCA.[231] Even though the statute would

---

221. *Id.* at 14,886.

222. *Id.* Senator Leahy worked with Representative Kastenmeier to craft the bill and, recognizing the importance of protecting communications, noted that "the law must advance with the technology to ensure the continued vitality of the fourth amendment." S. Rep. No. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

223. *See* Kerr, *supra* note 200, at 1214–15.

224. *See* 132 CONG. REC. 14,886 (statement of Rep. Kastenmeier); *New Law To Protect Computer Data Sought*, *supra* note 194; *Houses Approves Privacy Measure To Help Electronic Communications*, BOSTON GLOBE, Oct. 3, 1986, at 71. However, some commentators writing shortly after the bill was enacted noted that the protection accorded was not as broad as it appeared at first glance. *See, e.g.*, Robert Corn, *New Law Offers Easy Listening*, THE NATION, Dec. 20, 1986, at 696.

225. *See supra* notes 217–19 and accompanying text.

226. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C §§ 2510–22, 2701–12, 3121–27 (2006)).

227. The most significant changes were caused by the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C.), but this did not modify the protections afforded to electronic communications at issue in this Note.

228. 18 U.S.C. §§ 2510–22.

229. *Id.* §§ 2701–12.

230. *Id.* §§ 3121–27.

231. Most circuit courts to address this issue found that in order for the Wiretap Act to apply, the communication must be intercepted contemporaneously with transmission. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878

seem to be quite important and it is frequently used, commentators have noted that the "statute is dense and confusing, and few cases exist explaining how the statute works."[232]

The SCA imposes a fine or imprisonment for any intentional access to a facility where electronic communication service is provided, but does not apply to conduct authorized by the person or entity providing the service.[233] The SCA differentiates between providers of "Electronic Communication Service" (ECS), "which provides to users thereof the ability to send or receive wire or electronic communications,"[234] and "Remote Computing Service" (RCS), which is characterized by "the provision to the public of computer storage or processing services by means of an electronic communications system."[235] When the SCA was passed, computers were far more expensive and far less powerful than they are today. In addition to using third-party service providers to send and receive messages, some also outsourced what may now be considered to be basic computer tasks, including processing and file storage.[236] However, as the services provided continue to expand and evolve, the delineation between ECS and RCS providers has blurred.[237]

The SCA generally prevents both ECS and RCS providers from disclosing data in electronic storage, but has an important exception for electronic messages stored by an RCS. The statute clarifies that the government may only obtain the contents of an electronic communication that has been in storage with an ECS for less than 180 days pursuant to a warrant.[238] However, the government does not need a warrant supported by probable cause to obtain communications maintained in an ECS that are

(9th Cir. 2002). *But see* United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (en banc). In *United States v. Councilman*, the SCA was arguably inapplicable because the e-mail had been intercepted by the user's ISP and fell within the statutory exemption. 418 F.3d at 81. Sitting en banc, the U.S. Court of Appeals for the First Circuit concluded that Congress intended "electronic communication" to be defined broadly to cover transient electronic storage and the interception of e-mail in such storage. *Id.* at 85.

232. Kerr, *supra* note 200, at 1208. Kerr also notes that "[t]he uncertainty has made it difficult for legislators to legislate in the field, reporters to report about it, and scholars to offer scholarly guidance in this very important area of law." *Id.*

233. 18 U.S.C. § 2701.

234. *Id.* § 2510(15). "Existing telephone companies and electronic mail companies are providers of electronic communication services." S. REP. NO. 99-541, at 14 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3568. In the simplest case, a commercial ISP acts as an ECS for unopened e-mail sitting on its server. *See* Kerr, *supra* note 200, at 1216.

235. 18 U.S.C. § 2711(2). For example, a provider that allows users to upload files for remote storage would be an RCS under the statute. *See* Kerr, *supra* note 200, at 1216.

236. *See* S. REP. NO. 99-541, at 3, *as reprinted in* 1986 U.S.C.C.A.N. at 3557. Although increasingly sophisticated computers have decreased the need for consumers to rely on external sites for data processing and storage, many have begun to once again store records on remote servers and are increasingly using "cloud computers" for processing because of their convenience. *See, e.g.*, *Let it Rise*, THE ECONOMIST, Oct. 25, 2008, at 1, 1–2.

237. *See* Kerr, *supra* note 200, 1216–17.

238. 18 U.S.C. § 2703(a). The government must obtain a warrant because the contents are believed to be protected by the Fourth Amendment. H.R. REP. NO. 99-647, at 68 (1986).

more than 180 days old or to obtain communications stored in an RCS.[239] The government may use either an administrative subpoena, if authorized by statute, or a court order to obtain this information.[240] A court order only requires "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation," which is less than is required to establish probable cause and obtain a warrant.[241] There is no requirement that the government specify the type of messages it is seeking or the date of the messages. Although the government is required to give notice to the subscriber,[242] it may delay notice for ninety days where there is reason to believe that notification may have an "adverse result."[243] And, if the government does elect to procure a warrant, then it is not required to give notice to the subscriber at all.[244] Section 2703 of the SCA also requires ECS and RCS providers to disclose the name, address, method of payment, and other information about subscribers when subpoenaed.[245]

When enacting the ECPA, Congress found that "[m]ost—if not all—electronic communications systems . . . only keep copies of messages for a few months."[246] The Committee concluded that beyond this point, the storage is more akin to that of business records maintained by a third party, which are accorded less protection.[247] This is in part because when the Act was drafted, users generally needed to take affirmative steps to move e-mail messages they wanted to preserve into storage in order for e-mail providers to save them beyond 180 days.[248] Professor Deirdre Mulligan of Boalt Hall School of Law suggests that this practical reality of e-mail use at the time is important in reconciling Congress's reference to providing "first-class mail-like protections" to e-mail, and the distinction between e-mail less than 180 days old and greater than 180 days old.[249] This also helps explain why communications greater than 180 days old are only afforded the same protection as records stored in a remote server.[250]

---

239. 18 U.S.C. § 2703(b).

240. *Id.* § 2703(b)(1)(B).

241. *Id.* § 2703(d). The court may quash or modify the order on motion from the provider if the "records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." *Id.*

242. *Id.* § 2703(b)(1)(B).

243. *Id.* § 2705(a); *see also id.* § 2705(a)(2) (defining "adverse result").

244. *Id.* § 2703(b)(1)(A).

245. *Id.* § 2703(c)(2).

246. H.R. REP. NO. 99-647, at 68 (1986). The Committee chose 180 days because it found that electronic communications providers generally retained e-mail for six months. Mulligan, *supra* note 31, at 1584.

247. H.R. REP. NO. 99-647, at 68. This does not appear to account for the fact that the record keeper was not the intended recipient of the message and probably did not look at the records.

248. *See* Mulligan *supra*, note 31, at 1584.

249. *See id.* at 1584–85.

250. *See* 18 U.S.C. § 2703(b); *see also supra* note 239 and accompanying text. While internally consistent, this does not explain why remotely stored records are afforded less

3. Internet Use After the Electronic Communications Privacy Act

Internet and e-mail use have dramatically increased since the SCA came into force.[251] More and more households have broadband Internet access in their homes,[252] and a 2008 report found that nearly 70 percent of Americans used Internet Webmail services, stored data and photos online, or used online software programs.[253] The study found that in the eighteen- to twenty-nine-year-old age group, 77 percent of users surveyed used a Webmail service.[254] 49 percent of users surveyed stated they would be "very concerned" if their providers allowed law enforcement to access their files when requested to do so. 15 percent would be "somewhat" concerned, and 11 percent would be "not too" concerned.[255] However, 22 percent stated they would be "not at all" concerned if the government were allowed access.[256]

In addition to its increased use, e-mail is routinely held on providers' servers for increasing periods of time, and, in some cases, even indefinitely. For example, several companies, including Google, offer free Webmail service. When Google launched its Webmail service, GMail, in 2004, it provided users with one gigabyte of storage for free.[257] Now, just five years later, GMail users have over seven and a half gigabytes of storage available, and that amount is continually increasing.[258] With so much space at their disposal, users are encouraged not to delete their messages, but to archive them so that they are always available and always

protection than electronic records stored on premises. *Cf., e.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding legitimate expectation of privacy in personal computer in dorm room connected to university network); United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) (discussing privacy interest in personal computer).

251. *See generally* PEW INTERNET, INTERNET: THE MAINSTREAMING OF ONLINE LIFE 59 (2005), *available at* http://www.pewinternet.org/~/media//Files/Reports/2005/Internet_Status_2005.pdf.pdf (discussing increase in Internet use between 2000 and 2004 and how the "Web has become the 'new normal' in the American way of life").

252. *See generally* PEW INTERNET, HOME BROADBAND ADOPTION 2008 (2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Broadband_2008.pdf.

253. *See generally* PEW INTERNET, USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES SEPTEMBER 2008 1 (2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf.

254. *See id.* at 5.

255. *See id.* at 7.

256. *See id.* This survey is not immediately applicable to determining whether a search is reasonable under the Fourth Amendment because the respondents would likely factor in whether they had any potentially incriminating information in their accounts when assessing how concerned they, personally, would be if law enforcement were allowed to access their accounts. However, for a more detailed discussion of societal expectations of privacy, see SLOBOGIN, *supra* note 89.

257. This was nearly five hundred times the space provided on comparable free services at the time. *See* David Pogue, *What Big Brother? Gmail from Google Wins a Fan, Despite Its Ads Review*, INT'L HERALD TRIB., May 15, 2004, at 16; Katie Hafner, *In Google We Trust? When the Subject Is E-mail, Maybe Not*, N.Y. TIMES, Apr. 8, 2004, at G1.

258. *See* Posting of Rob Siemborski to Official Gmail Blog, http://gmailblog.blogspot.com/2007/10/more-gmail-storage-coming-for-all.html (Oct. 12, 2007, 1:05 EST).

searchable.[259] Irrespective of the level of protection that should be afforded to these messages, this use does not comport with Congress's general perception of e-mail use when it drafted the SCA, particularly the expectation that mail would rarely be retained for more than 180 days.[260] Although these servers store e-mail, they store it for the user, and there is no indication that the providers read the private correspondence.[261]

In addition to storing e-mail on remote servers, individuals are also increasingly turning to third parties for remote file storage and backup.[262] Users generally expect the information stored remotely to be kept private, and the providers also promise not to view the data stored on their servers.[263]

Despite the changes in e-mail and computer use, the SCA has been largely unmodified. In 2000, Representative Charles Canady introduced a bill amending certain provisions of the 1986 ECPA,[264] and, although the bill was favorably reported out of committee,[265] it was ultimately not enacted. The proposed amendments included a number of changes, and, relevant to electronic communications, would have required the government to demonstrate probable cause before accessing location information for cellular phones and to procure a warrant before accessing e-mail messages greater than one year old—doubling the time required under the 1986 act.[266] The report does not explain the significance of the change to one year,[267] but one year is still a far shorter period of time than the period for which messages are typically retained.[268] More recently, the Constitution Project, a coalition of twenty-five organizations and seventy-five individuals interested in constitutional law, recommended that the President and Congress take action to ensure Fourth Amendment protections for all location information, all e-mail messages (regardless of how old they are), and, additionally, for some user-generated content stored on remote servers.[269]

---

259. Pogue, *supra* note 257 (noting "[o]ne gigabyte changes everything"); Hafner, *supra* note 257.

260. *Cf. supra* notes 246–48.

261. *See, e.g.*, Does Google Read My Mail?, http://mail.google.com/support/bin/answer.py?answer=6599&topic=12787 (last visited Aug. 20, 2009).

262. *See* Peter Wayner, *You Know About Backups. Now, Do It Online.*, N.Y. TIMES, Oct. 23, 2008, at B7; David Pogue, *Fewer Excuses For Not Doing a PC Backup*, N.Y. TIMES, Jan. 4, 2007, at C1.

263. *See, e.g.*, Carbonite Online Backup, Data Security, http://cp-carbonite.kb.net/display/4n/kb/article.aspx?aid=1061&searchstring=&n=&tab=browse&bt=4n&s= (last visited Aug. 20, 2009); Mozy.com, Decho Corporation Privacy Policy, http://mozy.com/privacy (last visited Aug. 20, 2009).

264. H.R. 5018, 106th Cong. (2000).

265. *See* H.R. REP. NO. 106-932, at 23 (2000).

266. H.R. 5018.

267. H.R. REP. NO. 106-932, at 15.

268. *Cf., e.g.*, *supra* notes 259–60 and accompanying text.

269. *See* THE CONSTITUTION PROJECT, LIBERTY AND SECURITY: RECOMMENDATIONS FOR THE NEXT ADMINISTRATION AND CONGRESS 184–85 (2008), *available at*

4. Protections Under State Law

In addition to the protections provided by federal law and under the U.S. Constitution, several state legislatures have taken steps to protect electronic communications. State constitutions also have a role to play. For example, the New Jersey Supreme Court has held that the New Jersey Constitution provides broader protection in some cases than the Fourth Amendment of the U.S. Constitution.

In *State v. Reid*,[270] the New Jersey Supreme Court found that under the state constitution individuals have reasonable expectations of privacy in their Internet Protocol (IP) addresses, and law enforcement may not compel disclosure of the subscriber information linked to an IP address from an ISP without a grand jury subpoena.[271] In *Reid*, Shirley Reid's employer discovered that someone had changed the company's shipping information on a supplier's website in order to create a disruption and suspected Reid might have been responsible.[272] The supplier provided the police with the IP address used to make the modification, which the police used to trace back to the ISP that controlled that IP address.[273] The police subpoenaed all information pertaining to the IP address recorded at the time the modification was made and discovered that Reid had been assigned that IP address at the time the shipping information was changed.[274]

The court noted that the language of the Fourth Amendment is nearly identical to its counterpart language in the New Jersey Constitution.[275] The court also acknowledged that, after the Supreme Court's decisions in *Miller* and *Smith*, an individual cannot challenge the disclosure of this information under the Fourth Amendment.[276] However, the court held that the New Jersey Constitution offers broader protections than the U.S. Constitution. In particular, the court relied on the fact that the state constitution had been interpreted to protect disclosure of telephone numbers dialed or bank records even though such disclosure is permissible under the U.S. Constitution.[277]

---

http://2009transition.org/liberty-security/index.php?option=com_docman&task=doc_download&gid=49&Itemid=.

270. 945 A.2d 26 (N.J. 2008).

271. *Id.* at 28.

272. *Id.* at 29.

273. *Id.*

274. *Id.* at 29–30. IP addresses are unique addresses assigned to each computer connected to the Internet. Most individuals connect to the Internet through an ISP that is assigned a fixed range of IP addresses to distribute to its users. It is possible to look up which ISP a particular IP address belongs to on a public service, but generally impossible to determine the user with which a particular IP address is associated without contacting the ISP. *See, e.g.*, United States v. Carter, 549 F. Supp. 2d 1257, 1262–63 (D. Nev. 2008); *Reid*, 945 A.2d at 29–30.

275. *Reid*, 945 A.2d at 31–32.

276. *Id.* (collecting cases).

277. *Id.* at 32 (citing State v. McAllister, 875 A.2d 866 (N.J. 2005) (bank records); State v. Hunt, 450 A.2d 952 (N.J. 1982) (dialed telephone numbers)); *cf. supra* notes 49, 65 and accompanying text.

The court found that subscriber information is analogous to bank records and phone numbers dialed because, in all of these situations, individuals are forced to turn the information in question over to the providers as part of using the service.[278] The court noted that "when users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential."[279] Even though a decoded IP address does not allow access to the contents of an individual's transactions on the Internet, it still may reveal intimate details about personal affairs, such as where the person shops or in which political organizations he or she is involved.[280] In light of these concerns, the court held that individuals were entitled to the same level of protection for their subscriber information as for phone and banking records.[281]

Several other states also recognize the privacy interest in subscriber information, and Minnesota and Nevada both have enacted statutes prohibiting disclosure of personal subscriber information without consent.[282] No state appears to have legislated to define whether an ISP may monitor an individual's Internet use, but Connecticut and Delaware both prohibit employers from monitoring their employees' Internet and e-mail use without first giving them notice.[283]

While *Reid* did not consider the level of protection afforded to the contents of e-mail communications, subscriber information is generally afforded less protection than information that reveals the content of an individual's correspondence.[284] The flexibility in construing language nearly identical to that contained in the U.S. Constitution, combined with the recognition of the sensitivity of information that can be culled from these databases, suggests that the contents of electronic communications would almost certainly be protected under the New Jersey Constitution. This approach also casts doubt on the wisdom of the Court's earlier decisions in *Smith* and *Miller* and, in particular, raises questions about whether their reach should be extended to cover electronic communications stored in remote databases.[285]

---

278. *Reid*, 945 A.2d at 33.

279. *Id.*

280. *Id.* (citing Daniel J. Solove, *The Future of Internet Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287 (2004)).

281. *Id.* at 33–34.

282. MINN. STAT. ANN. §§ 325M.01–09 (West 2004); NEV. REV. STAT. ANN. § 205.498 (LexisNexis 2006); *see also* National Conference of State Legislatures, State Laws Related to Internet Privacy, http://www.ncsl.org/programs/lis/privacy/eprivacylaws.htm (last visited Aug. 20, 2009).

283. CONN. GEN. STAT. ANN. § 31-48d (West 2003); DEL. CODE ANN. tit. 19, § 705 (2005); *see also* National Conference of State Legislatures, *supra* note 282. For a humorous look at e-mail monitoring in the workplace, see *The Office: E-mail Surveillance* (NBC television broadcast Nov. 22, 2005).

284. *Cf., e.g.*, *supra* notes 129–32, 151–53 and accompanying text.

285. *But see generally* Kerr, *supra* note 34 (advocating for retaining the broad third-party doctrine).

II. DIFFERENT LEVELS OF PROTECTION AFFORDED BY THE STORED COMMUNICATIONS ACT AND THE FOURTH AMENDMENT

Although Congress sought to broadly protect electronic communications with the SCA, it did not give Fourth Amendment-like protections to all electronic communications. Two recent cases that considered the level of constitutional protection afforded to electronic communications have concluded that the messages are protected by the Fourth Amendment irrespective of how long they have been stored. Because § 2703(b) of the SCA permits the government to access electronic communications greater than 180 days old with a showing of less than probable cause, these cases suggest that the statute provides an unconstitutionally low level of protection.

A. *The Stored Communications Act in Action*

Under the SCA, government agents may only obtain electronic communications less than 180 days old pursuant to a warrant issued by a court with jurisdiction over the offense under investigation.[286] However, § 2703(b) permits law enforcement to obtain documents in storage for more than 180 days with just a subpoena or court order.[287] Under this section, the government does not need to establish probable cause, but must only "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[288] Additionally, the government may delay notifying the individual whose communications are being monitored by up to ninety days.[289]

In *Warshak v. United States*,[290] law enforcement used the SCA to obtain court orders directing the defendant's ISPs to turn over all of the defendant's messages greater than 180 days old stored on their servers.[291] The order prohibited the providers from informing Warshak about the search and allowed the government to delay notifying Warshak for ninety days.[292] However, where users have reasonable expectations of privacy in messages stored on their ISP's server, these communications are protected under the Fourth Amendment and law enforcement must generally obtain a warrant before they may review them.[293] If these messages are protected under the Fourth Amendment, the provision in § 2703(b) of the SCA that allows access to communications greater than 180 days old, without first

286. 18 U.S.C. § 2703(a) (2006).
287. *Id.* § 2703(b).
288. *Id.* § 2703(d).
289. *Id.* § 2705.
290. 490 F.3d 455, 460 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008) (finding claim was not ripe for judicial review).
291. *Id.* at 460.
292. *Id.*
293. *See supra* notes 12–20 and accompanying text.

demonstrating probable cause and securing a warrant, conflicts with the Constitution's requirements.[294]

B. *Applying the Fourth Amendment to Electronic Communications*

When applying legal rules to the Internet, Professor Orin Kerr points out that courts and lawyers have two choices: they can either take the perspective of a user and try to draw analogies between "realspace" and cyberspace, or take an external perspective and apply the law to the transactions underlying the network's operation.[295] In the Internet context, the different perspectives may lead to particularly divergent results, because a user may be fully immersed in the network, but have no idea of its inner workings.[296] For example, from a user's perspective, e-mail is the equivalent of postal mail, and should thus be entitled to the same high standard of Fourth Amendment protection.[297] However, from an external perspective, that same message is stored on both the recipient's computer and the sender's computer and may have been transmitted between two different ISPs, either of which may have also retained a copy.[298] From this perspective, Fourth Amendment protections are less clear.[299]

Some early decisions to address the protection afforded to electronic communications placed considerable emphasis on the technical details of how electronic messages are transported and delivered.[300] For example, in *United States v. Councilman*,[301] the U.S. Court of Appeals for the First Circuit engaged in an in-depth review of how e-mail is transmitted between computers.[302] Although such a highly technical analysis is not required under the *Katz* test focusing on reasonableness,[303] even courts considering the technical details of how an electronic message is transmitted have found that a third party's limited interaction with a message during delivery does not limit the Fourth Amendment protections.

In *Warshak v. United States*, a unanimous panel of the U.S. Court of Appeals for the Sixth Circuit held that e-mail messages were protected under the Fourth Amendment in spite of the third-party ISP's limited access.[304] More recently, the U.S. Court of Appeals for the Ninth Circuit

---

294. *Cf.* 18 U.S.C. §§ 2703(a)–(b).

295. Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 359–60 (2003).

296. *Id.* at 362.

297. *Id.* at 365–66; *cf.* Cooley, *supra* note 179, at 73 (drawing an analogy between telegrams and postal mail).

298. Kerr, *supra* note 295, at 366; *cf.* Wikipedia, E-Mail, *supra* note 30.

299. *See* Kerr, *supra* note 295, at 366–67.

300. *See, e.g.*, Saul Hansell, *You've Got Mail (and Court Says Others Can Read It)*, N.Y. TIMES, July 6, 2004, at C1.

301. 418 F.3d 67 (1st Cir. 2005).

302. *See id.* at 69–70.

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

304. 490 F.3d 455, 460 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008) (finding claim was not ripe for judicial determination); *see infra* Part II.B.1.

concluded in *Quon v. Arch Wireless Operating Co.*[305] that individuals have reasonable expectations of privacy in their text messages and that those messages are, therefore, also protected by the Fourth Amendment.[306] Additionally, in other analogous areas, courts have found that a third party's limited access to some part of an electronic communication does not eliminate all Fourth Amendment protections, further supporting the decisions in *Warshak* and *Quon*.[307] However, these decisions conflict with § 2703(b) of the SCA, which is premised on the concept that electronic communications stored by third parties are not protected under the Fourth Amendment.

1. E-mail: *Warshak v. United States*

While investigating Steven Warshak and Berkeley Premium Nutraceuticals, Inc.—the company Warshak controlled—for mail and wire fraud, money laundering, and other federal offenses, the government obtained an order from a magistrate judge under § 2703 of the SCA that required Warshak's ISPs to turn over all "electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled by Warshak."[308] The court issued the orders under seal and prohibited the ISPs from informing Warshak.[309] Over a year after the orders issued, the government finally informed Warshak about the orders.[310]

In addition to challenging the use of the messages as evidence, because the government failed even to comply with the delayed notice provisions contained in the SCA, Warshak also raised a Fourth Amendment challenge to the search of these messages.[311] Writing for a unanimous panel of the Sixth Circuit, Judge Boyce F. Martin, Jr. found that the reasonable expectation of privacy question must "focus on two narrower questions than the general fact that the communication was shared with another."[312] First, courts need to "identify the party with whom the communication is shared."[313] Second, courts must consider the precise information conveyed to the party from whom disclosure is sought.[314]

The court recognized that the depositor in *Miller* and the caller in *Smith* had assumed the risk that the bank and phone company might disclose the

305. 529 F.3d 892 (9th Cir. 2008).
306. *Id.* at 903; *see infra* Part II.B.2.
307. *See infra* Part II.B.3.
308. *Warshak*, 490 F.3d at 460.
309. *Id.* Identical orders were presented to NuVox Communications and Yahoo!, where Warshak held e-mail accounts. *Id.*
310. *Id.* at 460–61.
311. *Id.* at 461.
312. *Id.* at 470.
313. *Id.*
314. *Id.*; *cf.* Couch v. United States, 409 U.S. 322, 340 (1973) (Douglas, J., dissenting) (recognizing the difference between disclosing information to one person and to the general public).

information they had voluntarily conveyed to them.[315] However, the panel concluded that the "assumption of risk" is limited to the information actually conveyed to the provider, which, in the context of a phone conversation, does not include the content of the call.[316] This distinction led the court to hold that the third-party exception only permits the government to compel disclosure of the specific information to which the third party had access.[317] "It cannot, on the other hand, bootstrap an intermediary's limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation)."[318] Even though the "ISP *could* access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course."[319] Consistent with the third-party doctrine, the court noted there would be no Fourth Amendment violation if the government subpoenaed the recipient of the e-mails.[320] However, here, the government subpoenaed the ISP, which was "not expected to access the content of the documents, much like the phone company in *Katz*."[321]

Even though the court found that Warshak did have a reasonable expectation of privacy in his e-mails, it did not declare the statute unconstitutional. The court instead issued an injunction prohibiting the government from compelling disclosure of e-mails unless it first obtained a warrant, provided notice to the account holder, and allowed him the same judicial review he would have if subpoenaed.[322] Alternatively, the order allowed the government to simply subpoena the e-mails if it could show "specific, articulable facts, demonstrating that an ISP or other entity has complete access to the e-mails in question and that it actually relies on and utilizes this access in the normal course of business, sufficient to establish that the user has waived his expectation of privacy with respect to that entity."[323]

On rehearing en banc, a majority of the Sixth Circuit found the issue was not fit for judicial review as it was unclear whether the government intended to perform further ex parte review of Warshak's e-mail.[324] The majority also noted that the lack of Fourth Amendment challenges to the SCA since its inception in 1986 further validated the court's decision not to address the Constitutional issue.[325] Except for this reference, the majority

315. *Warshak*, 490 F.3d at 470.
316. *Id.* at 471; *see also* Katz v. United States, 389 U.S. 347, 353 (1967).
317. *Warshak*, 490 F.3d at 471.
318. *Id.*
319. *Id.*; *see also supra* note 132 and accompanying text.
320. *Warshak*, 490 F.3d at 471.
321. *Id.*; *cf. supra* note 261 and accompanying text.
322. *Warshak*, 490 F.3d at 475–76.
323. *Id.* at 476.
324. Warshak v. United States, 532 F.3d 521, 526 (6th Cir. 2008) (en banc).
325. *Id.* at 531.

did not discuss the panel's earlier conclusions regarding the constitutionality of § 2703 of the SCA.[326] In dissent, Judge Martin remarked that "[i]nstead of reaching the question that is on everyone's mind—whether or not the delayed notification provision of the Stored Communications Act is constitutional—the majority sidesteps the question."[327] Expressing his discontent with the majority's decision, Judge Martin went on to speculate, "[I]f I were to tell James Otis and John Adams that a citizen's private correspondence is now potentially subject to ex parte and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless."[328]

Although the panel's initial decision is no longer in force, its reasoning regarding the underlying constitutional issue is still persuasive. Taking an internal perspective and accepting the validity of the Supreme Court's third-party doctrine, the panel recognized that, although Warshak's messages were stored in a commercial ISP's database, the ISP was not a party to the communications and its limited interaction with the communications did not vitiate Warshak's legitimate expectation of privacy in them.[329] Recognizing that Warshak had a reasonable expectation of privacy in the messages would extend Fourth Amendment protections to them and render § 2703 of the SCA unconstitutional.

2. Text Messages: *Quon v. Arch Wireless Operating Co.*.

More recently, in *Quon v. Arch Wireless Operating Co.*, the Ninth Circuit found that city employees have reasonable expectations of privacy in text messages sent from pagers provided by their employers.[330] The city of Ontario, California contracted with Arch Wireless for wireless text messaging services, and distributed pagers to various city employees, including Ontario Police Department Sergeants Jeff Quon and Steve Trujillo.[331] The city lacked an official policy for the pagers but had a general technology policy limiting the use of computer equipment to city-related business.[332] The policy admonished that users "'should have no expectation of privacy or confidentiality when using these resources.'"[333]

---

326. *See id.* at 533.

327. *Id.* at 535 (Martin, J., dissenting).

328. *Id.* at 538.

329. *See supra* notes 317–22 and accompanying text.

330. 529 F.3d 892, 903 (9th Cir. 2008). A similar issue appeared before the U.S. Court of Appeals for the Ninth Circuit several months before *Quon* in United States v. McCreary, No. 05-10818, 2008 WL 399148, at *1 (9th Cir. Feb. 12, 2008). The defendant in *McCreary* challenged the government's use of § 2703 of the SCA to obtain transcripts of text messages he sent. *Id.* However, the court found there was substantial independent evidence of McCreary's guilt and did not reach the constitutional issue. *Id.*

331. *Quon*, 529 F.3d at 895.

332. *Id.* at 896.

333. *Id.* (quoting the City of Ontario Computer Usage, Internet and E-Mail Policy).

Each pager had a monthly character allotment under the contract, and the city's unofficial policy was to refrain from auditing usage so long as the users paid any overages.[334] However, as part of an internal affairs investigation, city officials obtained transcripts of some officers' usage and discovered personal and sexually explicit messages.[335] The officers and the parties with whom they were communicating brought an action challenging the police department's review of their messages under the Fourth Amendment and the SCA.[336]

The district court concluded that "electronic storage" as defined in the SCA[337] included storage after transmission and that to read it more narrowly and find it only covers pretransmission storage would undermine the purpose of the SCA.[338] The court then denied Arch Wireless's motion to dismiss the claim, rejecting the argument that, because the sergeants were not subscribers, they were not users of the system and not entitled to the protections of the SCA.[339]

The district court later granted the defendants' summary judgment motion, finding that Arch Wireless was an RCS under § 2702(a) of the SCA and committed no harm when it released the text message transcripts to its subscriber, the city.[340] However, the district court found that, in light of the informal policy that the officers' pager use would not be monitored if they paid the overage charges, the officers had reasonable expectations of privacy in the messages they sent.[341]

On appeal, the Ninth Circuit affirmed in part, reversed in part, and remanded for further proceedings.[342] The court disagreed with the district court's conclusion that Arch Wireless was acting as an RCS.[343] Although an RCS may release private information with the consent of a subscriber, addressee, or intended recipient, an ECS may only release the information with the consent of the addressee or intended recipient.[344] The court looked at the plain language of the SCA and its "common-sense definitions" and found that Arch Wireless provided the city with electronic communication services and not just remote storage, even though it retained backup copies

334. *Id.* at 897.
335. *Id.* at 898.
336. *Id.*
337. 18 U.S.C. § 2510(17) (2006).
338. Quon v. Arch Wireless Operating Co., 309 F. Supp. 2d 1204, 1209 (C.D. Cal. 2004).
339. *Id.* at 1209–10.
340. *Quon*, 529 F.3d at 898; Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1133, 1138 (C.D. Cal. 2006).
341. *Quon*, 529 F.3d at 899. The district court then held a jury trial on the officers' intent in reviewing the messages to determine if the review was reasonable, and the jury concluded it was, absolving the police department of liability. *Id.*
342. *Id.* at 911.
343. *Id.* at 902–03.
344. *Id.* at 900.

of the messages city employees transmitted.[345] Concluding that Arch Wireless was acting as an ECS, the court found that it violated the SCA by releasing the messages without consent from either the sender or the intended recipient.[346]

Most relevant for present purposes, the Ninth Circuit affirmed the district court's determination that the users had reasonable expectations of privacy in their text messages and that they were therefore protected by the Fourth Amendment.[347] Even though the official department policy indicated that the officers should not expect any privacy while using the department-supplied technology, the court concluded that because Sergeant Quon had in the past exceeded the character limit and his messages had not been reviewed, the department followed an "informal policy" of not reviewing messages.[348] Because the department did not review the messages, the policy did not foreclose the officer's expectations of privacy.[349]

Similar to the Sixth Circuit's reasoning in the panel decision in *Warshak*, the court also recognized the distinction between *Katz*, which offered strong protection for the content of a phone conversation, and *Miller*, which found there was no protection for telephone numbers dialed, and held that the content of the text messages was protected.[350] The court opined that the fact "[t]hat Arch Wireless may have been able to access the contents of the messages for its own purposes is irrelevant" when determining the scope of the user's privacy.[351] Because the parties "did not expect that Arch Wireless would monitor their text messages, much less turn over the messages to third parties without . . . consent," Arch Wireless's limited access did not diminish the user's reasonable expectations of privacy.[352] The Court did, however, note that whether an expectation of privacy is reasonable was a "context-sensitive" inquiry and, had Sergeant Quon permitted the department to review his messages, none of the parties to the conversations would have had a reasonable expectation of privacy.[353] In

345. *Id.* at 900–01. The Ninth Circuit also reached a similar result when it found that a provider of e-mail services was an ECS even though it retained e-mails for backup protection. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1070 (9th Cir. 2004).

346. *Quon*, 529 F.3d at 903.

347. *Id.* at 904.

348. *Id.* at 907; *see also, e.g.*, Haynes v. Attorney Gen., No. 03-4209, 2005 WL 2704956, at *4 (D. Kan. Aug. 26, 2005) (discussing fact-specific inquiry to determine whether employee had legitimate expectation of privacy and collecting cases).

349. *Cf., e.g.*, United States v. Mosby, No. 08-CR-127, 2008 WL 2961316, at *5 (E.D. Va. July 25, 2008).

350. *Quon*, 529 F.3d at 904–05. The Court also noted that there was no meaningful difference between the text messages at issue and the e-mail messages at issue in *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), where the Ninth Circuit concluded that there was no privacy in the to/from address of e-mail messages because users should be aware that information is available to ISPs for routing. *Quon*, 529 F.3d at 904–05.

351. *Id.* at 905.

352. *Id.* at 906.

353. *Id.* This is similar to the panel's decision in *Warshak*, which found that the government may be able to access the messages from the ISP with just a court order or

this case, in spite of the warnings not to expect privacy while using department-supplied technology, because the police department followed a policy of not auditing his messages as long as he paid the overage, the Ninth Circuit agreed that Sergeant Quon had a reasonable expectation of privacy in the text messages.[354]

Quon, like *Warshak*, recognized the limits of the third-party doctrine and that a user's expectation of privacy was not eliminated merely because a communication was stored on a third party's server.[355] Arch Wireless was expected to provide text messaging services, including storing and transmitting messages, but the parties did not expect that Arch Wireless would review or disclose their private messages.[356] Unlike Hoffa speaking to his associate, Arch Wireless was not a party to the conversations, but merely a storage facility, and the users did not assume the risk that they would disclose their messages.[357]

3. Protection for Other Electronic Information

a. *Information Held by, but Not Directed to, Third Parties*

As the Supreme Court recognized in *Katz*, the mere fact that a conversation is shared with another does not eliminate all Fourth Amendment protections.[358] In the electronic communications context, both *Quon* and the panel opinion in *Warshak* recognized that individuals have reasonable expectations of privacy in electronic communications, even where the communications pass through third-party intermediaries who could theoretically review the contents of the communications.[359] In this situation, practice and societal expectations indicate that the service providers, like the phone company in *Katz*, will not review the communications.[360]

However, consistent with *Katz*'s mandate that information voluntarily exposed to the public is not subject to Fourth Amendment protection,[361] several courts have found that an individual does not have a reasonable expectation of privacy in her personal, subscriber information conveyed to

---

subpoena if the ISP had a practice of reviewing the messages. *See* Warshak v. United States, 490 F.3d 455, 475–76 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

354. *Quon*, 529 F.3d at 906. The court also rejected the police department's argument that Sergeant Quon lacked a reasonable expectation of privacy because the California Public Records Act, CAL. GOV'T CODE § 6253 (West 2008), makes public records open to inspection by the public. *Quon*, 529 F.3d. at 907.

355. *See supra* Part II.B.1–2.

356. *See Quon*, 529 F.3d at 905–06.

357. *Cf.* United States v. Hoffa, 385 U.S. 293, 302 (1966).

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

359. *See supra* Part II.A–B.

360. *See supra* Part II.A–B.

361. *Katz*, 389 U.S. at 351.

an ISP.[362] Law enforcement officers are often aware of the IP address[363] associated with a user engaging in illegal activity online, but must obtain that user's subscriber information from the ISP in order to ascertain the identity of the actual person linked to that IP address.[364] Several courts have held that users do not have legitimate expectations of privacy in this information because they voluntarily conveyed it to their third-party ISP, and it is therefore not protected by the Fourth Amendment.[365] These courts find that this information is akin to the bank records in *Miller*, which were voluntarily turned over to the third party for its use and hence were not protected by the Fourth Amendment.[366]

Highlighting the difference between information simply made available to a third party and information directed to a third party, some courts have found that pen registers cannot be used to capture post-cut-through dialed digits (PCTDD).[367] Frequently, individuals enter credit card, social security, personal identification, or other numbers into a phone system in response to prompts from an automated system at the other end of the line after a call is connected. These PCTDDs can, in principle, be recorded by pen registers.[368] In considering a request from law enforcement for approval to use such a device, a court noted that although the phone company certainly could view this information if it chose, unlike dialed telephone numbers, which are used to connect a call and may show up on an invoice, this information is not regularly recorded or processed by the phone company.[369] Relying on the Sixth Circuit's panel decision in *Warshak*, the court also noted that finding no expectation of privacy wherever an intermediary merely has the potential to access information would eviscerate important Fourth Amendment protections recognized previously by the Supreme Court.[370]

---

362. *E.g.*, United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

363. *See supra* note 274 and accompanying text.

364. For example, in *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008), the government was able to locate an individual distributing pornography in an Internet chat room by tracing the user's IP address back to his ISP and requiring the ISP to disclose the user's true identity and address. *Id.* at 1199–200.

365. *See, e.g.*, *id.* at 1204–05 (collecting cases). *But cf. supra* notes 270–81 and accompanying text.

366. *See supra* Part I.A.2; *cf.* 18 U.S.C. § 2703(c)(2) (2006) (permitting law enforcement to request subscriber information from ISPs).

367. *E.g.*, *In re* U.S. for an Order Authorizing the Use of a Pen Register & a Trap & Trace Device on Wireless Tel., No. 08 MC 0595, 2008 WL 5255815, at *3 (E.D.N.Y. Dec. 16, 2008); *In re* U.S., Misc. Case No. H-07-613, 2007 WL 3036849, at *6–9 (S.D. Tex. Oct. 17, 2007); *In re* U.S. for Orders (1) Authorizing the Use of Pen Registers & Trap & Trace Devices, 515 F. Supp. 2d 325, 339 (E.D.N.Y. 2007).

368. 515 F. Supp. 2d at 336.

369. *Id.* at 337.

370. *Id.* at 337–38. The court noted that even though it is not their usual practice, because the telephone company has the ability to listen in to phone conversations, only considering this factor would eliminate the Fourth Amendment protections for telephone calls that the U.S. Supreme Court expressly noted existed in *Katz*. *Id.*; *see* Katz v. United States, 389 U.S. 347, 353 (1967).

In addition to finding protection for information held by third parties but not directed to them, some courts have held that individuals maintain reasonable expectations of privacy in historical cell site information recorded by their wireless providers.[371] Wireless providers record their users' locations when their phones are active, and, by obtaining an individual's historical cell site information, law enforcement officials can track where an individual has been.[372] Some courts have concluded that, even though cellular providers regularly store this information, users still have reasonable expectations of privacy in it.[373] Even though this information is stored in the provider's database where the provider could access it, one court has recognized that because the provider would not regularly as a matter of course review this information, let alone identify a customer's location to a third party, users still have reasonable expectations of privacy in this information.[374] These holdings go beyond the decisions in *Warshak* and *Quon* because the cellular provider is not an intermediary with respect to the historical cell site information, but actually the intended recipient of it. These decisions suggest that information in the possession of others is still private if it is not generally disclosed and appear to conflict with the Supreme Court's earlier decision in *Miller*.[375] However, both the proposed 2000 amendments to the ECPA and the Constitution Project's proposals advocate adopting Fourth Amendment-like protections for historical location information—just as the courts in these cases have found.[376]

Although it was never the subject of a reported decision, even in the case of telegraph communications—where an operator read and transmitted a message to another operator who received and transcribed it—the public still expected those communications to remain private.[377] Because of the way the system worked, unlike telephone companies or ISPs, who merely have the capability to review communications, here the operators were actually privy to the content of the transmissions.[378] In spite of these technical realities, many individuals still viewed these communications as

371. *See, e.g.*, *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 612 (W.D. Pa. 2008); *In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Info. and Historical Cell Site Info. for Mobile Identification Nos.: (XXX) XXX-AAAA, (XXX) XXX-BBBB, (XXX) XXX-CCCC, 509 F. Supp. 2d 64, 74 (D. Mass. 2007).

372. *See* Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 310–11 (2004); *see also* Amy Harmon, *Lost? Hiding? Your Cellphone Is Keeping Tabs*, N.Y. TIMES, Dec. 21, 2003, at N1.

373. *See, e.g.*, *In re* U.S. for an Order, 534 F. Supp. 2d at 612; *In re* Applications of the U.S. for Orders, 509 F. Supp. 2d at 74–75.

374. 509 F. Supp. 2d at 74 & n.6.

375. *See supra* Part I.A.2.

376. *See supra* notes 266–69 and accompanying text.

377. *See supra* Part I.B.3.

378. *See* COE, *supra* note 155, at 105–22; *see also, e.g.*, Peterson v. W. Union Tel. Co., 74 N.W. 1022, 1022 (Minn. 1898) (describing the process of sending a telegraph).

private and were outraged at the possibility of government or other private individuals reviewing their messages.[379]

b. *Information Reviewed by Third Parties*

Conversely, an individual may not prevail on a Fourth Amendment challenge where there is evidence demonstrating the provider or some other party did regularly review the information in question. When considering whether an individual has a privacy interest in electronic information on a computer used at work, courts have been heavily influenced by the employer's written policies regulating computer use.[380] For example, in *United States v. Mosby*,[381] the court found that, even though not enforced, a policy that informed employees that their computer use was not private and was subject to monitoring made any expectations of privacy the employees had unreasonable.[382] In *Warshak*, the panel recognized that if the government could demonstrate that it was the ISP's practice to review the users' messages, then the third-party doctrine would apply, and the government could access the messages with a subpoena.[383]

In situations where communications are regularly reviewed, and users are aware that their communications are not private, they may not have legitimate expectations of privacy.[384] However, even where an official policy instructs users not to expect privacy, courts still must engage in a fact-based inquiry to determine whether an employee could have a reasonable expectation of privacy in spite of such warnings.[385] In the case of electronic communications, even where a provider's use policy purports to limit an individual's privacy, courts still must consider what actually takes place in order to determine whether an individual's expectation of privacy is legitimate.[386] Where there is no use policy or other evidence demonstrating the third party reviewed the user's communications, as was the case in *Quon* and *Warshak*, these decisions hold that the third-party service provider's limited access is not enough to bring the communications

379. *See supra* notes 167–72 and accompanying text.

380. *E.g.*, United States v. Mosby, No. 3:08-CR-127, 2008 WL 2961316, at *5 (E.D. Va. July 25, 2008).

381. 2008 WL 2961316.

382. *Id.* at *5. However, in *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006), the use policy did not clearly indicate that employees should not expect privacy, and the court found that the other circumstances surrounding the use, including regularly changing passwords, contributed to a finding that the defendant did have an objectively reasonable expectation of privacy in the system. 64 M.J. at 64; *accord* Haynes v. Attorney Gen., No. 03-4209, 2005 WL 2704956, at *4 (D. Kan. Aug. 26, 2005) (discussing fact-specific inquiry to determine whether employee had legitimate expectation of privacy and collecting cases).

383. *See* Warshak v. United States, 490 F.3d 455, 475–76 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008) (finding claim was not ripe for judicial determination).

384. *E.g.*, *Haynes*, 2005 WL 2704956, at *4 (finding no expectation of privacy based on "splash screen" that warned "that information flowing through or stored on the computer could not be considered confidential").

385. *E.g.*, *Mosby*, 2008 WL 2961316, at *5.

386. *E.g.*, *Haynes*, 2005 WL 2704956, at *4.

within the purview of the third-party doctrine and find an individual's expectation of privacy is unreasonable.[387]

III. SECTION 2703 OF THE STORED COMMUNICATIONS ACT IS UNCONSTITUTIONAL AS APPLIED

As e-mail and other forms of electronic communications became more widely used, Congress recognized their tremendous importance and grew concerned that the existing statutory and constitutional framework was not robust enough to adequately protect them for two main reasons.[388] First, Congress was concerned about the unpredictability of which expectations of privacy courts would recognize as reasonable and, therefore, sufficient to satisfy the *Katz* test for determining the scope of Fourth Amendment protections.[389] Second, Congress was unsure how the third-party doctrine that evolved in Fourth Amendment analysis through the Supreme Court's decisions in cases like *Hoffa*, *Smith*, and *Miller* would be applied.[390] However, when considered in light of this precedent, electronic communications are still protected by the Fourth Amendment, as the *Warshak* and *Quon* courts recognized.[391]

The nature of the technology requires that electronic communications will frequently bounce between several different servers controlled by third parties during transmission, and these third-party servers may create backup or archival copies of messages.[392] However, these intermediaries are not parties to the conversations in the same way that the bank in *Miller* was, and *Quon* and *Warshak* recognize that merely retaining a copy of the message does not bring the communication within the purview of this exception.[393]

In this situation, the provider is a fundamental part of the communication process because it delivers the messages, but it is not an intended recipient.[394] The provider's relationship with the message is not akin to the situation in *Hoffa*, where Hoffa shared information with an associate believing he would keep it confidential.[395] Here, although the provider carries the message, the message is not directed to it.

This distinction between information carried by third parties and information directed to third parties for their use is consistent with the Supreme Court's decision in *Smith*, holding that individuals do not have reasonable expectations of privacy in the telephone numbers they dial,

387. *See supra* Part II.B.1–2.
388. *See supra* Part I.C.1.
389. *See supra* notes 20, 23–28, 200, 206 and accompanying text.
390. *See supra* Part I.A.
391. *See supra* Part II.B.1–2.
392. *See supra* notes 31–33 and accompanying text. In *Quon*, for example, the provider retained copies of all the text messages it carried. *See supra* note 335 and accompanying text.
393. *Supra* notes 315–22, 350–56 and accompanying text.
394. *See supra* notes 31–33, 81 and accompanying text.
395. Hoffa v. United States, 385 U.S. 293, 302 (1966).

thereby permitting the government to request copies of a user's call history from the phone company.[396] Dialing information is conveyed directly to the phone company so that it may complete the phone call, and for the purpose of this information, the phone company is the intended recipient and is—like Hoffa's associate—free to disseminate this information to whomever it chooses.[397] However, even though the content of the conversation that takes place after the phone company uses the number dialed to route and connect the call also passes through the phone company's network, it is strongly protected under the Fourth Amendment.[398] This is because the content is not like the phone number dialed and is not conveyed to the phone company for it to use. Additionally, there is a strong societal expectation that the conversation will be kept private.[399]

The Supreme Court also recognized this distinction earlier when it considered protections available for postal mail in *Ex parte Jackson*.[400] Like a telephone call, when an individual deposits a letter in the mail, the Postal Service has full control over the communication. Although postal agents could easily open up letters and read their contents, as was in fact widely done during the colonial period,[401] the Postal Service is not expected to do so, and the contents of letters are strongly protected by the Fourth Amendment.[402] The Postal Service is, however, expected to deliver letters and, in doing so, is expected to read the address and other information written on the exterior.[403] Similar to a phone number, because the address is directly communicated to the Postal Service for use in delivering the letters, it is not protected by the Fourth Amendment.[404] However, the content of the letter, like the content of the phone call, is not similarly directed and is strongly protected by the Fourth Amendment.[405]

This distinction is equally applicable to e-mail and other electronic communications. Some information, namely the recipient's address, is conveyed to the ISP for its use in routing the message.[406] The ISP is privy to this information and, for Fourth Amendment purposes, is analogous to Hoffa's associate—free to disseminate the information as it wishes.[407]

396. *See supra* Part I.A.1.

397. Providers and customers are, of course, free to contract for greater protections and require that the phone company not freely disclose this information. Additionally, although not protected under the Fourth Amendment to the U.S. Constitution, the analogous provision in the New Jersey State Constitution has been interpreted to cover this information. *See supra* notes 275–81 and accompanying text.

398. *See supra* notes 123–24 and accompanying text.

399. *See supra* notes 129–32 and accompanying text.

400. *See supra* Part I.B.2.

401. *See supra* notes 138–41 and accompanying text.

402. *See supra* notes 136–37 and accompanying text.

403. *See supra* notes 147–49 and accompanying text.

404. *See supra* notes 129–32, 147–49 and accompanying text.

405. *See supra* notes 136–37 and accompanying text.

406. *See supra* note 31.

407. Additional restrictions on disclosure can be enforced contractually.

However, like the substance of a telephone conversation or the text of a letter, the contents of e-mail messages are not directed to, nor expected to be read, by ISPs.[408] The ISP in this case is not truly a party to the communication, and the third-party doctrine does not apply as the Sixth Circuit panel concluded in *Warshak* and the Ninth Circuit suggested in *Quon*.[409]

Additionally, by analogy to postal mail and telephone conversations, the contents of e-mail messages should also be strongly protected by the Fourth Amendment.[410] As the Court recognized early on in *Ex parte Jackson*, "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[411] Electronic communications are similarly "closed" and not expected to be reviewed by the intermediaries merely charged with delivering the messages.

This analysis does not change merely because an ISP may retain backup or archival copies of messages in its database. This storage is fundamentally different from the storage of bank records in *Miller* because, in that instance, the information had been communicated to the bank for its use.[412] In this situation, the ISP merely has access to the information, but was never an intended recipient of the message. In *Miller*, the documents were shared with the bank on the assumption that it would not turn the information over to anyone else, and certainly not law enforcement.[413] However, like Jimmy Hoffa, that "misplaced reliance" eliminated the depositor's expectation of privacy in the documents.[414] There is no misplaced reliance in the case of the electronic communications at issue because, unlike the financial instruments in *Miller*, they are never directed to the provider. As such, users still maintain reasonable expectations of privacy in their communications even if archival copies are created and stored in the third party's electronic database.

Further bolstering the conclusion that the nature of the third-party service provider's use of, and interaction with, the communications does not work to bring it within the purview of the third-party doctrine is the immense importance of privacy in electronic communications.[415] In *Katz*, the Supreme Court recognized the tremendous importance of the telephone and corrected its earlier error in *Olmstead* by giving strong protection to

408. *See supra* notes 31–33, 81 and accompanying text.

409. *Supra* notes 315–22, 350–56 and accompanying text.

410. *See supra* Part I.B.1.b, I.B.2. Similarly, while considering the level of protection that should be afforded to telegrams, Judge Thomas M. Cooley remarked on the analogy between telegrams and postal mail, noting that the two types of communication should be similarly protected by the Fourth Amendment. *See supra* notes 179–83 and accompanying text.

411. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

412. *Cf. supra* notes 70–75 and accompanying text.

413. *See supra* notes 70–75 and accompanying text.

414. *See supra* notes 35–38, 70–75 and accompanying text.

415. *See, e.g.*, *supra* notes 216–19 and accompanying text.

telephone calls.[416] Similarly, in *Ex parte Jackson* the Court acknowledged the central role of the mail system and, in the face of widespread snooping, gave strong protection to the mails.[417] Although never discussed in a reported judicial opinion, the public even expected privacy in telegraph messages, where the technology required operators to actually read the contents of transmissions.[418] And, in attempting to enact protective legislation, congressional representatives noted the tremendous importance of the telegraph system and the problems that would flow if individuals could not be guaranteed some privacy in using it.[419]

Congress recognized that many of these same problems would exist if electronic communications were not adequately protected and attempted to enact strong protective legislation.[420] However, in the short period since the SCA was enacted, computer use has significantly changed.[421] The Ninth Circuit's decision in *Quon* and the Sixth Circuit panel's decision in *Warshak* recognize that electronic communications are protected by the Fourth Amendment and that the provision in § 2703 of the SCA that permits the government to access messages greater than 180 days old without first securing a warrant supported by probable cause is unconstitutional.[422] An individual's reasonable expectation of privacy and Fourth Amendment protections do not evaporate over time. Congress recognized that messages less than 180 days old would likely be protected under the Fourth Amendment,[423] and, now that individuals frequently store messages on servers for longer periods of time, the statute should be modified to recognize this.

Furthermore, this provision is also problematic because it allows government actors broad access to all of an individual's electronic communications without any meaningful restriction.[424] This unbridled access would in some cases permit law enforcement to engage in "fishing expeditions," one of the chief evils against which the framers of the Fourth Amendment sought to guard.[425]

At the same time, consistent with *Smith* and *Miller*, users do not have legitimate expectations of privacy in information turned over to third parties.[426] Therefore, the provision in § 2703(c)(2) of the SCA that allows government access to subscriber information is consistent with the Supreme Court's Fourth Amendment jurisprudence because this information is

416. *See supra* notes 126–27 and accompanying text.
417. *See supra* notes 143–46 and accompanying text.
418. *See supra* notes 160–62, 191–93 and accompanying text.
419. *See supra* notes 180–81 and accompanying text.
420. *See supra* Part I.C.1.
421. *See supra* Part I.C.3.
422. *See supra* Part II.B.1–2.
423. *See supra* notes 246–50 and accompanying text.
424. *See generally supra* Part I.C.2.
425. *Cf. supra* notes 14–16 and accompanying text.
426. *See supra* Part I.A; *supra* note 245 and accompanying text.

voluntarily turned over to the provider in order to establish an account.[427] However, particularly where the provider expressly states that it will not review a user's messages,[428] and where Congress itself recognized that mail less than 180 days old is likely protected under the Fourth Amendment,[429] subscriber information is significantly different from communications the provider stored in a database but was never a party to.

As the panel decision in *Warshak* concluded, because § 2703 of the SCA allows the government to access material protected by the Fourth Amendment without a warrant supported by probable cause, it is unconstitutional.[430] Although this Note argues that, irrespective of legislative action, electronic messages are protected by the Fourth Amendment, until the Supreme Court considers this issue the level of protection remains largely unknown, and lower courts could potentially reach divergent results. In the face of this uncertainty, Congress should revise the SCA to eliminate the distinction between mail greater and less than 180 days old and extend the same, high level of protection to all electronic communications, regardless of how long they have been in storage.

CONCLUSION

Information gleaned from e-mail messages will likely become an increasingly important tool for law enforcement agencies to use in combating crime, and they should be encouraged to rely on it going forward. However, law enforcement may not take advantage of the anomaly that has resulted where, although Congress attempted to legislate to protect electronic communications, evolving uses actually resulted in communications having less protection than is provided by the Constitution. Electronic communications do frequently pass through third parties, but the third parties are not parties to the transmissions. Their minimal interaction does not eliminate the sender or receiver's expectation of privacy in, or Fourth Amendment protections for, the messages. The same requirement that law enforcement obtain a warrant before searching e-mail messages less than 180 days old should also apply to mail greater than 180 days old. Users' expectations of privacy do not disappear over time, and the same rationale that led Congress to conclude that messages less than 180 days old are protected by the Fourth Amendment should be adopted to keep pace with technology and the current practice of storing messages for more than 180 days. Because all electronic messages, regardless of age, are protected by the Fourth Amendment, § 2703(b) of the SCA, which allows law enforcement to access communications greater than 180 days old without a warrant, is unconstitutional.

---

427. *See supra* Part I.A.2; *but cf. supra* notes 275–81 and accompanying text.
428. *See supra* note 81 and accompanying text.
429. *See supra* notes 246–50 and accompanying text.
430. *See supra* notes 322–24 and accompanying text.