2004

Surveillance Law Through Cyberlaw's Lens

Patricia L. Bellia
Notre Dame Law School, patricia.l.bellia.2@nd.edu

Surveillance Law Through Cyberlaw's Lens

Patricia L. Bellia*

Table of Contents

* Associate Professor of Law, Notre Dame Law School. A.B. Harvard College; J.D. Yale Law School. E-mail: pbellia@nd.edu. I thank A.J. Bellia, Bob Blakey, Susan Freiwald, Rick Garnett, Jim McAdams, and David G. Post for helpful comments on a prior draft of this article. Gretchen Heinze and Rabeh Soofi provided able research assistance.

Introduction

As Congress debated and passed the USA Patriot Act,[1] the popular news media carried story after story detailing the ways in which the statute enhanced the government's electronic surveillance capabilities.[2] Critics charged that, among other things, the Patriot Act authorized "unparalleled" acquisition of Internet communications;[3] gave officials the power to engage in "roving wiretaps" of unspecified telephone facilities; and unconstitutionally extended a foreign intelligence surveillance statute to permit the use of its procedures in ordinary criminal cases.[4]

As it happens, these objections each reflected profound misunderstandings about the state of surveillance law prior to the passage of the Patriot Act. For instance, although the Act did authorize the government to request a court order for the collection of certain Internet addressing and routing information,[5] the statute merely codified an existing government practice of

---

1 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. Throughout this Article this Act will be referred to interchangeably as either the "USA Patriot Act" or the "Patriot Act."

2 I explain how I am using the terms "electronic surveillance" and "Internet surveillance" in greater detail below. *See infra* text accompanying notes 17–19.

3 Jim Puzzanghera, *Uneasiness Over Drive to Monitor E-mail, Web*, SAN JOSE MERCURY NEWS, Sept. 27, 2001, at 1A.

4 *See, e.g.*, *Agreement on an Antiterrorism Bill*, N.Y. TIMES, Oct. 2, 2001, at B7 (describing surveillance changes in bill); Sonia Arrison, *New Anti-Terrorism Law Goes Too Far*, SAN DIEGO UNION-TRIB., Oct. 31, 2001, at B9 (calling the USA Patriot Act "labyrinth legislation" that compromises "basic rights that define the nation"); Susan Goering, *Anti-Terrorism Act Imperils Liberties*, BALT. SUN, Oct. 30, 2001, at 15A (claiming that the Act's investigative and surveillance provisions go "light years beyond what is necessary" to achieve its objectives); Bob Kemper & Jeff Zeleny, *President Signs Bill Widening Powers for Police*, CHI. TRIB., Oct. 27, 2001, at 1 (describing new surveillance powers); Jim McGee, *An Intelligence Giant in the Making: Anti-Terrorism Law Likely to Bring Domestic Apparatus of Unprecedented Scope*, WASH. POST, Nov. 4, 2001, at A4 (discussing public focus on new Internet surveillance capabilities); Serge Schmemann, *United Nations to Get a U.S. Antiterror Guide*, N.Y. TIMES, Dec. 19, 2001, at B4 (describing USA Patriot Act as granting "vast new powers of surveillance").

The USA Patriot Act changes have been equally controversial among academic commentators. For criticism of the surveillance-related changes, see Laurie Thomas Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUTER & TECH. L.J. 371, 377–403 (2003); Steven A. Osher, *Privacy, Computers and the Patriot Act: The Fourth Amendment Isn't Dead, but No One Will Insure It*, 54 FLA. L. REV. 521, 523–34 (2002); Marc Rotenberg, *Foreword: Privacy and Secrecy after September 11*, 86 MINN. L. REV. 1115, 1116–18 (2002). For arguments that the Patriot Act's surveillance provisions will have less impact on privacy than critics fear, see Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003); Nathan C. Henderson, Note, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179, 194–208 (2002); Stephen D. Lobaugh, Note, *Congress's Response to September 11: Liberty's Protector*, 1 GEO. J.L. & PUB. POL'Y 131 (2002); Michael T. McCarthy, *Recent Developments: USA Patriot Act*, 39 HARV. J. ON LEGIS. 435, 436–53 (2002).

5 USA PATRIOT Act § 216, 115 Stat. at 288.

seeking such an order.[6] In fact, the Patriot Act removed the real possibility that law enforcement officials were free to acquire at least some addressing or routing information without any legal process whatsoever.[7] The Patriot Act also granted law enforcement officials the power to request court approval for roving wiretaps, but it granted that power in connection with foreign intelligence investigations, not criminal investigations.[8] Indeed, a roving wiretap authority had already existed for criminal investigations for fifteen years.[9] Finally, although the Patriot Act's change to the scope of the foreign intelligence surveillance statute was the most substantively important of the electronic surveillance–related changes, it too was widely mischaracterized.[10]

---

6 *See* Kerr, *supra* note 4, at 633–34.

7 That possibility arose from the combination of the Supreme Court's case law holding that law enforcement officials' acquisition of the telephone numbers of an outgoing call did not constitute a search within the meaning of the Fourth Amendment, *see* Smith v. Maryland, 442 U.S. 735 (1979), and the narrow language of a subsequently enacted federal statute designed to protect the privacy of noncontent information such as telephone numbers, *see* Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, §§ 301–302, 100 Stat. 1848, 1868–72 (codified as amended at 18 U.S.C.A. §§ 3121–3127 (West 2000 & Supp. 2003)). *See infra* notes 306–09 and accompanying text. If neither the Fourth Amendment nor the statute protected the information, then law enforcement officials were free to acquire it without any legal process. As I discuss below, however, the constitutional issue is a difficult one. *See infra* notes 296–99 and accompanying text.

8 *See* USA PATRIOT Act § 206, 115 Stat. at 282.

9 *See* 18 U.S.C. § 2518(11) (2000) (authorizing application and order for interception of communications without specification of facilities to be subject to surveillance, where there is probable cause to believe suspect's actions will have the effect of thwarting interception from a specified facility). The provision was enacted in 1986. *See* ECPA § 106(d)(3), 100 Stat. at 1857.

10 News accounts both understated and overstated the significance of the change. In one example of understatement, *The New York Times* described the change as applying to "electronic surveillance of terrorists overseas." *See Agreement on an Antiterrorism Bill*, *supra* note 4. In fact, the underlying surveillance statute, the Foreign Intelligence Surveillance Act ("FISA"), deals not with *foreign* surveillance, but with *domestic* surveillance to acquire foreign intelligence information. *See* Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511, § 101(f), 92 Stat. 1783, 1785 (codified at 50 U.S.C. § 1801(f) (2000)) (defining "electronic surveillance" as the monitoring of persons or installation of surveillance devices "within" the United States). At the same time, some accounts suggested that the amendment authorized an end run around the strict surveillance regime that applies in ordinary criminal cases. *See, e.g.*, Scott Shane, *Secret U.S. Court Handed New Power to Fight Terror; But Some Observers Fear for Civil Liberties*, BALT. SUN, Oct. 29, 2001, at 1A (noting concern among civil libertarians that the change "weakens constitutional protections by enabling the FBI to circumvent the requirements for criminal wiretap warrants"). Before passage of the USA Patriot Act, FISA allowed surveillance to proceed only if a senior executive branch official in the area of national security or defense certified that "the purpose" of the surveillance was to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(7)(B) (2000). The Patriot Act amended the statute to permit surveillance to proceed upon certification that "*a significant* purpose" of the surveillance was to obtain foreign intelligence information. USA PATRIOT Act § 218, 115 Stat. at 291 (codified at 50 U.S.C.A. § 1804(a)(7)(B) (West Supp. 2003)) (emphasis added). The change clarified that FISA itself did not prohibit officials from using the statute's procedures where the primary purpose of the investigation was to obtain evidence for a criminal prosecution. But the change did not eliminate—and, indeed, could not eliminate—any independent Fourth Amendment constraint on the use of foreign intelligence surveillance procedures in ordinary criminal cases. The appeals court created by FISA has held that the Fourth Amendment does not prohibit use of the statute's procedures in cases where the primary purpose of the investigation is to prosecute a *foreign intelligence* crime. *See In re* Sealed Case, 310 F.3d 717, 736–46 (Foreign Int. Surv. Ct. Rev. 2002).

Without minimizing these objections to the USA Patriot Act's surveillance law changes, we can safely say that the public debate over those changes failed to account for many of the nuances and complexities of existing surveillance law. The Patriot Act debate is in fact illustrative of a more general problem with electronic surveillance law, and specifically with electronic surveillance law as it applies to communications carried over the Internet or other computer networks. Complaints that government investigatory techniques invade our privacy and calls to limit the government's ability to gather information about us strike a chord with the public. The laws regulating electronic surveillance generally, and particularly those governing acquisition of electronic evidence, however, are highly technical and poorly understood. And the problems and misperceptions are not confined to the lay public. Courts struggle with how to apply overlapping and seemingly conflicting statutory provisions;[11] scholars endorse problematic decisions and incorporate them into the (relatively small) body of materials from which surveillance law and related topics can be taught.[12] Indeed, so much confusion prevails that litigants, courts, and scholars cannot even agree on what to call the principal federal statute governing electronic surveillance.[13]

---

11 One of the best examples of courts' confusion over how to apply the surveillance statutes involves cases dealing with the intersection of the prohibition on interception of communications and the prohibition on the acquisition of communications from electronic storage. *See* Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1048 (9th Cir.) (concluding that unauthorized access to a secure web site constituted an interception), *withdrawn*, 262 F.3d 972 (9th Cir. 2001), *new opinion filed*, 302 F.3d 868 (9th Cir. 2002) (reversing in part and holding that unauthorized access to a secure web site did not constitute an interception); United States v. Smith, 155 F.3d 1051, 1059 (9th Cir. 1998) (concluding that a private acquisition of a stored voice mail message constituted an interception). The USA Patriot Act modified the statutory language that gave rise to much of the confusion, but the change is scheduled to expire in 2005. USA PATRIOT Act §§ 209, 224, 115 Stat. at 285, 295. For further discussion, see *infra* notes 114–21.

12 Two particularly problematic lines of cases are worth mentioning. First, courts have considered several claims that placement of "cookies" on users' hard drives violates surveillance statutes. Although courts generally have rejected such claims on the theory that the web site served by the advertiser "consents" to the placement of cookies, the cases reflect substantial confusion over statutory concepts such as "electronic communication service" and "electronic storage." *See, e.g.*, Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1158–63 (W.D. Wash. 2001); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001). Second, cases dealing with application of the surveillance statutes to claimed unauthorized access to web sites also reflect confusion over these concepts. *See, e.g.*, *Konop*, 302 F.3d at 894–81. For further discussion, see *infra* notes 114–21 and accompanying text. The absence of alternative materials makes it difficult to omit such cases from Internet law and privacy law case books.

13 By the principal federal surveillance statute, I mean the provisions appearing in chapter 119 of the criminal code, at 18 U.S.C.A. §§ 2510–2522 (West 2000 & Supp. 2003). The statute was enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211, and is most often referred to in criminal cases and within the government as "Title III." Because the statute was amended by the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, which added electronic communications to the statute's coverage, courts and commentators also refer to the statute as "ECPA." That reference is erroneous, because the statute covers far more than electronic communications, and confusing, because ECPA also added a separate chapter of the criminal code, *id.* §§ 201–202 (codified as amended at 18 U.S.C.A. §§ 2701–2709, 2711–2712 (West 2000 & Supp. 2003)), that some refer to as ECPA. Finally, some courts and commentators refer to 18 U.S.C. §§ 2510–2522 as the "Wiretap Act," even though the statute covers not only "wiretapping"—that is, acquisition of the

Several provisions of the USA Patriot Act that altered federal surveillance law will expire via a sunset provision in 2005 unless Congress acts.[14] Congress should use the approach of the sunset date as an opportunity to address Internet surveillance issues more broadly. That task is complicated, however, by the fact that surveillance law is undertheorized. First, much legal scholarship addressing electronic surveillance issues focuses heavily on the constitutional questions involved.[15] The value of such scholarship is obvious, but the constitutional focus is rarely integrated with a detailed analysis of the statutory aspects of surveillance. Although no surveillance law reform could proceed without an understanding of the constitutional backdrop, and there are certain areas in which the existing statutory scheme is premised on a flawed understanding of that constitutional backdrop,[16] many controversial surveillance law issues are purely statutory ones. Second, because a significant portion of the literature proceeds from a deep suspicion of surveillance activities, the literature gives less attention than it should to the normative principles that should guide Congress in balancing the privacy and law enforcement interests at stake. Taken together, these two scholarly trends give rise to two problems. Because the scholarship largely ignores statutory issues, or the interplay between the statutory and constitutional issues, courts do not receive needed guidance for applying the surveillance statutes. More important, to the extent that the literature focuses on the constitutional aspects of surveillance—and on the role of courts in applying the Fourth Amendment to guarantee privacy against assertions of law enforcement interests—it leaves Congress with the mistaken impression that courts are, or should be, the primary guarantors of privacy in this area. In other words, Congress is led to believe that it can safely overvalue law enforcement interests and undervalue privacy interests because courts will right the balance.

In this Article, I seek to contribute to the debate over the appropriate scope of Internet surveillance laws in two ways. The first is to explore the

---

contents of wire communications through use of a mechanical device—but also the acquisition of oral and electronic communications. *See infra* notes 92–95 and accompanying text. When describing provisions of the statute under which government officials seek court authorization to conduct surveillance activities, I generally refer to "Title III" orders, in keeping with government practice.

14 *See* USA PATRIOT Act § 224, 115 Stat. at 295.

15 *See, e.g.*, Chris J. Katopis, *"Searching" Cyberspace: The Fourth Amendment and Electronic Mail*, 14 TEMP. ENVTL. L. & TECH. J. 175, 191–205 (1995) (applying Fourth Amendment balancing tests to e-mail and pen registers); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1350–68 (2002) (arguing that use of new technologies such as Magic Lantern and Carnivore should be considered "searches" under the Fourth Amendment); Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 123–41 (2002) (applying Fourth Amendment principles from *Katz v. United States*, *Kyllo v. United States*, and *Smith v. Maryland* to e-mail searches and use of Carnivore); Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1343 (2002) (advocating that courts applying *Katz v. United States* to electronic communications use an approach focusing on results of search rather than method of search).

16 *See infra* notes 125–215 and accompanying text; *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1576–82 (2004).

intricacies of the constitutional and statutory frameworks governing electronic surveillance, and particularly surveillance to acquire electronic evidence. Such an exploration should help to clarify many of the poorly understood aspects of the surveillance framework, but my aims are broader—to provide guidance on how reforms of surveillance law should proceed. First, in a practical sense, I hope to identify the inconsistencies, gaps, and ambiguities that any reform of Internet surveillance law must address in the short term. Second, I will show how the development of surveillance law provides something of a cautionary tale for Congress as it legislates in this area. The inconsistencies, gaps, and ambiguities are in part a product of an assumption Congress made in 1986 that has not withstood the test of time: that electronic communications are sufficiently like telephone communications that application of a similar surveillance regime to both types of communications will adequately balance the privacy and law enforcement issues at stake. Third, I hope to disentangle the constitutional and statutory strands of surveillance law, with three audiences in mind: litigants and courts; Congress; and the public interest groups that seek to shape privacy legislation. Although much of surveillance law is statutory law, there are some statutory provisions that litigants and courts have not tested, but should test, against the Fourth Amendment. Disentangling the constitutional and statutory strands of surveillance law is also important for Congress, because doing so illustrates that uncertainty within the Fourth Amendment's coverage places additional responsibilities on Congress to protect privacy. Finally, for public interest groups that seek to shape privacy legislation, disentangling the constitutional and statutory strands of surveillance law provides the basis for a rhetorical shift. Claims questioning the constitutionality of certain surveillance techniques are powerful tools in the public debate, but deploying them too frequently threatens to dilute their force.

The second overarching goal of this Article is to take some steps toward reconceiving Internet surveillance law. We tend to view surveillance law as a relatively narrow and specialized field located at the outer boundaries of the domain of criminal procedure. Just as electronic surveillance generally is not a central focus of criminal procedure courses, Internet surveillance law is rarely given in-depth treatment within Internet law or "cyberlaw" courses. At most, such courses tend to focus on the significant cases illuminating the relationship between the Fourth Amendment's protection against warrantless searches and technological developments that enhance the government's surveillance powers. Within the growing body of Internet law scholarship, too, surveillance issues take a back seat to copyright, trademark, and free speech matters. The marginalization of Internet surveillance law is unfortunate in two respects: first, surveillance law issues can provide a rich illustration of some of the major themes that emerge in Internet law scholarship; and second, Internet law scholarship can illuminate and provide an organizing normative structure to some of the policy dilemmas Congress faces in updating surveillance law.

I. Understanding Internet Surveillance Law

In this Part, I explore the constitutional and federal statutory frameworks governing electronic surveillance. Before beginning that task, it is useful to define what I mean by "electronic surveillance" and to distinguish that concept from surveillance that yields electronic evidence. By "electronic surveillance," I mean techniques that historically have involved the use of certain electronic or mechanical *devices* to acquire the contents of communications and identifying data associated with them. The "electronic" in "electronic surveillance," then, refers to the technique used in the surveillance, not to the type of communication acquired through the technique. Wiretapping (that is, attaching a device to a telephone wire to acquire the contents of a telephone communication) and bugging (that is, installing a device to transmit or record a conversation) are two such techniques. The principal modern federal surveillance statute was initially drafted to prohibit these techniques, but to authorize law enforcement officials to engage in them in some circumstances.[17] As we shall see, the widespread use of electronic communications necessitated an expansion of that statute,[18] as well as the adoption of separate provisions protecting against unauthorized acquisition of communications held in storage by service providers.[19]

I use the term "Internet surveillance" as a shorthand for the various means by which government officials gain access to the contents of electronic communications transmitted over computer networks, and to noncontent data associated with such communications, although the term is something of a misnomer in two respects. First, such surveillance can involve retrieval of electronic communications from networks other than the Internet. Second, law enforcement officials can acquire electronic evidence through techniques that are not what we traditionally think of as "surveillance"—by using legal process to compel production of communications from service providers, rather than by using a device to extract such communications during their transmission. In the interest of providing more thorough coverage of the means by which law enforcement officials can gain access to electronic communications, this Article deals with the legal authorities governing both the extraction and the compelled production of communications.

In exploring the surveillance law framework, I address three categories of surveillance activities in turn: (1) the interception of communications during transmission; (2) the acquisition of stored communications and related records directly from a service provider; and (3) the acquisition of source, destination, and related information concerning a communication during transmission. As I will show, the lines between these categories have both constitutional and statutory significance,[20] but the categories do not encom-

---

17 *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801–804, 82 Stat. 211, 211–23 (codified as amended at 18 U.S.C.A. §§ 2510–2522 (West 2000 & Supp. 2003)).

18 *See* Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, §§ 101–111, 100 Stat. 1848, 1848–59.

19 *See* ECPA §§ 201–202, 100 Stat. at 1860–68 (codified as amended at 18 U.S.C.A. §§ 2701–2709, 2711–2712 (West 2000 & Supp. 2003)).

20 Concerning the constitutional significance, see *infra* Parts I.A.1, I.B.1, I.C.1. With re-

pass all of the relevant surveillance activities;[21] indeed, analyzing the existing legal framework reveals significant gaps in coverage.

Within the first category of surveillance activities—interception of communications—the Fourth Amendment standards governing traditional electronic surveillance techniques (that is, wiretapping and bugging) are relatively straightforward, and Congress designed the modern statute authorizing law enforcement surveillance to meet these standards. That statute initially governed the interception of "wire" and "oral" communications but was expanded in 1986 to cover the interception of electronic communications.[22] Although the statute's treatment of wire and oral communications differs in some respects from its treatment of electronic communications, the statute generally requires prior judicial authorization of surveillance activities. As a result, courts have not needed to assess how the Fourth Amendment applies to electronic communications intercepted in transit. The constitutional and statutory frameworks are far less clear for the second category of surveillance activities—acquisition of stored communications directly from a service provider. The main constitutional question is whether one retains a reasonable expectation of privacy in communications stored with a third party, such that acquisition of these communications constitutes a "search" within the meaning of the Fourth Amendment.[23] I call into question the prevailing assumption that an expectation of privacy is lacking when a service provider holds communications on a user's behalf. Because application of the Fourth Amendment is in doubt, the statutory rules for acquisition of communications are all the more important. Those provisions, however, reflect significant gaps and ambiguities.

Finally, with respect to the third category of surveillance activities—acquisition of source and destination information concerning communica-

---

spect to the statutory significance, there are two controversial issues. The first is whether the acquisition of a stored communication, such as a voice mail or e-mail message, is covered by the statute prohibiting interception of a communication, *see* 18 U.S.C. § 2511(1)(a) (2000), the statute prohibiting obtaining a communication from electronic storage, *see* 18 U.S.C. § 2701(a) (2000), or both. For a discussion of this issue, see *infra* notes 109–21 and accompanying text. The second controversial statutory line relates to what statutory authority governs the acquisition of certain addressing information in connection with Internet communications. For a discussion of this issue, see *infra* notes 306–17 and accompanying text.

21 Because I am primarily concerned with the legal authorities governing acquisition of information in criminal investigations, I do not discuss the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C.A. §§ 1801–1863 (West 2000 & Supp. 2003). That statute authorizes surveillance to gather "foreign intelligence information," defined in part to include information that relates to the ability of the United States to protect against an attack or other hostile acts by a foreign power; acts of sabotage or international terrorism; or clandestine intelligence gathering activities. *Id.* § 1801(e). The statute creates a special court to hear requests for orders approving electronic surveillance to gather foreign intelligence information. *Id.* § 1803. Rather than requiring a showing of probable cause that the surveillance will reveal evidence of criminal activity, however, the statute requires a showing of probable cause to believe that the target of the surveillance is a "foreign power" or "the agent of a foreign power." *Id.* § 1804(a)(4). Although several of the relevant definitions involve a showing of an imminent violation of criminal law, some do not. For further discussion, see 2 JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE §§ 9:7–9:8, at 9-12 to 9-14 (2003). *See also supra* note 10.

22 *See* ECPA, §§ 101–111, 100 Stat. at 1848–59.

23 *See infra* Part I.B.1.

tions—we can again distinguish between information associated with telephone conversations and information associated with electronic communications. The application of Fourth Amendment principles to source and destination information associated with telephone conversations is clear: one lacks an expectation of privacy in such information, and law enforcement officials need not seek a warrant to acquire it.[24] The question is whether source and destination information concerning an electronic communication reveals more about the substance or meaning of a communication than analogous information reveals about a telephone call, thereby calling into question the extension of this constitutional principle.

As the discussion will show, most of the difficult constitutional and statutory surveillance issues confronting courts and Congress involve electronic communications. The relevant constitutional and statutory categories developed at a time when electronic communications either did not exist or were not widely used, and subsequent technological developments have placed tremendous strain on those categories.

A. "Interception" of Communications in Transit

In this section, I discuss the constitutional and statutory frameworks governing the "interception" of communications while they are occurring, through the use of a device that transmits, records, or replicates such communications. Two key Supreme Court cases decided in 1967 outlined how the Fourth Amendment applies to wiretapping and eavesdropping activities,[25] and one year later Congress adopted detailed procedures regulating those activities.[26] Nearly two decades later, Congress extended much, but not all, of that statutory framework to electronic communications.[27] Because this layer of statutory protection requires prior judicial authorization of surveillance activities, courts seldom need to assess how, if at all, the Fourth Amendment protects electronic communications in transit. As will become clear, however, this relatively high degree of protection is afforded only to communications in transit, and a complete picture of legal protections for electronic communications emerges only when we consider the accessibility of such communications in storage.

1. The Constitutional Framework

a. Traditional Electronic Surveillance Techniques

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, sup-

---

24 *See* Smith v. Maryland, 442 U.S. 735, 744 (1979). For further discussion of *Smith*, see *infra* text accompanying notes 167–71.

25 *See* Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967); *infra* notes 32–46 and accompanying text.

26 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801–804, 82 Stat. 211; *see infra* notes 62–91 and accompanying text.

27 ECPA, §§ 101–111, 100 Stat. at 1848–59; *see infra* notes 92–108 and accompanying text.

> ported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[28]

The Supreme Court wrestled with the Fourth Amendment's application to electronic surveillance activities as early as 1928, holding in *Olmstead v. United States*[29] that a wiretap not effected through a trespass onto private property did not violate the Fourth Amendment.[30] In 1967, the Court decided two cases concerning the use of electronic listening devices that would shape both the constitutional and statutory frameworks for wiretapping and eavesdropping activities. In *Berger v. New York*,[31] the Court concluded that the capture of a conversation through the placement of an electronic listening device in an office constituted a "search" within the meaning of the Fourth Amendment.[32] The Court further held that the procedures under which New York law authorized courts to grant orders permitting such surveillance were constitutionally deficient.[33] As discussed below, the Fourth Amendment requirements identified in *Berger* provided a blueprint for the federal legislation authorizing applications for electronic surveillance orders.[34] For current purposes, *Berger* is relevant insofar as it holds that installation of an electronic listening device—at least within a private area—to capture a conversation requires a warrant.[35]

Katz v. United States[36] also involved the use of an electronic listening device to capture a conversation, but in that case, law enforcement officials placed the device in a public area—a telephone booth—rather than in a private home or office.[37] Prior Fourth Amendment case law, including the *Olmstead* and *Berger* decisions, had aligned the question of whether particular activities violated the Fourth Amendment with whether the officials' conduct would constitute a trespass at common law. The absence of a trespass in *Olmstead* led the Court to conclude that use of a wiretap did not violate the Fourth Amendment;[38] in *Berger*, the fact that the placement of the device in the office was effected through a "trespassory intrusion into a constitutionally protected area" led the Court to conclude that officials were required to comply with the Fourth Amendment.[39] In light of the traditional focus on whether a "trespassory intrusion" into a "constitutionally protected area" had occurred, the parties in *Katz* disputed whether the phone booth from which Katz placed his calls was a constitutionally protected area.[40] In an explicit shift from the trespass approach, the Court held that the Fourth Amendment does not simply protect against government intrusions into

---

28 U.S. CONST. amend. IV.

29 Olmstead v. United States, 277 U.S. 438 (1928).

30 *See id.* at 466.

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

32 *Id.* at 51.

33 *Id.* at 54–60.

34 *See infra* text accompanying notes 72–90.

35 *Berger*, 388 U.S. at 63.

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

37 *Id.* at 348.

38 Olmstead v. United States, 277 U.S. 438, 466 (1928).

39 *Berger*, 388 U.S. at 44.

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

physical areas in which an individual has a property interest: "[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[41] Because the government's activities "in electronically listening to and recording [Katz's] words violated the privacy upon which he justifiably relied while using the telephone booth," the government's conduct amounted to a search.[42] Law enforcement officials could not engage in such conduct without obtaining prior judicial authorization for it.

Although the Court did not explain the circumstances in which one might "justifiably" rely on privacy, Justice Harlan's concurrence described the appropriate inquiry as encompassing two questions: whether "a person [has] exhibited an actual (subjective) expectation of privacy," and whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[43] In subsequent cases, the Court adopted this now familiar "reasonable expectation of privacy" formulation.[44] Although both *Berger* and *Katz* involved installation of electronic listening devices rather than wiretapping—in *Berger*, the device was a freestanding bug,[45] and in *Katz*, the device was not attached to the telephone line, but was placed so as to pick up Katz's end of the telephone conversations[46]—the implication for wiretapping was clear: if a wiretap would invade a reasonable expectation of privacy, it ordinarily could not proceed without prior judicial authorization. *Berger* and *Katz* thus established that the Fourth Amendment generally requires law enforcement officials to obtain judicial authorization before engaging in wiretapping or electronic eavesdropping activities.

b. Electronic Communications

If we can reasonably expect privacy in telephone communications and in some other oral conversations, we might also assume that under *Katz* we can expect privacy in electronic communications transmitted over computer networks as well. Subsequent development of the *Katz* test makes the matter more complicated, however. If we take a personal e-mail communication as an example, we can assume that a user subjectively expects privacy in the communication. The question, then, is whether society is prepared to accept that expectation as reasonable. There are three arguments as to why the expectation might not be reasonable. First, once the user transmits the message, he or she has no control over what the recipient does with it: the recipient may print, forward, or otherwise disclose the message.[47] Second, a

41 *Id.* at 353.

42 *Id.*

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

44 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979).

45 Berger v. New York, 388 U.S. 41, 45 (1967).

46 *Katz*, 389 U.S. at 348.

47 *See, e.g.*, Andrew Ross Sorkin, *An E-Mail Boast to Friends Puts Executive Out of Work*, N.Y. TIMES, May 22, 2001, at C2 (describing a personal e-mail forwarded to "thousands," resulting in the sender losing his job).

user must rely on several third parties—including his or her Internet service provider and multiple other intermediaries—to transmit his or her message to the ultimate recipient.[48] Third, we are conditioned to presume the vulnerability of our electronic communications at various points on the Internet to hackers. If electronic communications are insecure, it might be unreasonable to expect privacy in them.

It should be clear, however, that the first two of these objections to the reasonableness of an expectation of privacy could have been made in *Katz* itself. The person with whom Katz conversed could have revealed the substance of his or her conversation with Katz to authorities, voluntarily or in response to law enforcement questioning. The fact that he or she *could* have done so, however, did not eliminate Katz's expectation of privacy as against the use of an electronic listening device by government officials.[49] *Katz* and subsequent cases implicitly recognize that one can expect privacy against government eavesdropping even when one cannot expect that a party to a communication will not reveal its contents.[50] Similarly, the involvement of Internet service providers and other intermediaries in the transmission of electronic communications is analogous to the involvement of telecommunications carriers in telephone conversations. Telecommunications carriers facilitate the connection over which the communication occurs and have limited rights to overhear the contents of the communications.[51] *Katz* found an expectation of privacy in Katz's portion of the telephone conversation despite this fact.[52]

The third argument, that electronic communications are vulnerable to hackers and that any expectation of privacy in them is therefore unreasonable, highlights a general problem with measuring society's willingness to accept an expectation of privacy as reasonable, particularly with emerging (and potentially insecure) communications technologies. *Katz* provides no satisfactory answer to this question, because it does not indicate the degree to which the reasonableness of an expectation of privacy depends on the function served by a mode of communication or the degree to which the reasonableness of the expectation depends on the security of the mode of communication against eavesdropping. Under a functional approach, one could argue that electronic communications have supplanted communica-

---

48 *See, e.g.*, Chris Gaither, *Google's E-Mail Strategy Criticized*, L.A. TIMES, Apr. 2, 2004, at C1 (noting Google's plan to scan all messages that pass through its free e-mail service).

49 *See Katz*, 389 U.S. at 353.

50 In a line of cases both pre-dating and post-dating *Katz*, for example, the Supreme Court has held that no Fourth Amendment violation occurs when a party to a conversation, at the behest of the government, reveals, records, or transmits by an electronic device the contents of the conversation. *See infra* notes 143–57 and accompanying text. This recognition that one who misplaces his or her trust in another participant in a conversation cannot expect privacy is consistent with *Katz* only if it is understood to mean that the speaker cannot expect privacy against the activities of the other party to the conversation, and not that the speaker cannot expect privacy against surveillance conducted by outsiders.

51 For example, federal law permits the employee of a communications provider to intercept a communication "in the normal course of his employment, while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i) (2000).

52 *See Katz*, 389 U.S. at 353.

tions by mail or telephone; and since the Fourth Amendment protects against the acquisition of the contents of a telephone conversation[53] and the contents of a letter[54] without a warrant, society should recognize an expectation of privacy in electronic communications as reasonable. Under an approach focusing less on functional characteristics and more on the actual security of communications, one could argue that societal perceptions that such communications are insecure should lead to the conclusion that any expectation of privacy is unreasonable. The problem is that the reasonableness of an expectation of privacy in electronic communications then turns on the extent of our understanding of the technical processes by which such communications are transmitted. That understanding is likely to be influenced not only by the facts about those technical processes, but by other forces that have nothing to do with the interests the Fourth Amendment seeks to protect. Our understanding of the "privacy" of our electronic communications, for example, is affected by information from companies seeking to promote network security products, by employers who announce monitoring policies to deter misuse of network access, and by service providers who seek to disclaim liability for security breaches.

The fact that federal (and state) law to some extent protects the privacy of electronic communications[55] further complicates the matter. It cannot be the case that statutory or common law protection is *required* for an expectation of privacy to be reasonable, for that would simply return the constitutional inquiry to something analogous to its pre-*Katz* state.[56] If positive law protects the privacy of communications, however, then it becomes more reasonable to expect privacy in such communications. The Supreme Court has never squarely addressed the extent to which statutory or common law protection of a communication contributes to the reasonableness of an expectation of privacy. In *California v. Greenwood*,[57] a case involving a state law, the Supreme Court suggested that statutory protection of privacy does not create a per se expectation of privacy and thereby ratchet up the constitutional protection.[58] Because the Court's treatment of the issue involved a

---

53 *Id.*

54 *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984).

55 *See infra* notes 92–122, 222–82 and accompanying text (describing statutory protections for electronic communications in transit and in electronic storage). In addition, the Computer Fraud and Abuse Act prohibits unauthorized access to a computer system in some circumstances. *See* 18 U.S.C.A. § 1030 (West 2000 & Supp. 2003). Avenues of state protection include state surveillance statutes, state computer crime statutes, and common law trespass actions. For discussion of state surveillance statutes, see Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971 (2003). For discussion of state computer crime statutes, see A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 639–1300 (2001). For discussion of state trespass actions, see Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. (forthcoming 2004).

56 Because pre-*Katz* case law tied the protection of the Fourth Amendment to activities that would constitute a trespass at common law, it simply linked Fourth Amendment law to existing common law protection. A rule under which the reasonableness of an expectation of privacy was determined wholly by reference to existing legal protection for privacy would have much the same effect.

57 California v. Greenwood, 486 U.S. 35 (1988).

58 In *Greenwood*, a warrantless search of a garbage bag, impermissible under California

state law rather than a federal law and was extremely brief,[59] *Greenwood* does not foreclose the argument that federal statutory privacy protections can contribute to the reasonableness of an expectation of privacy. In addition, one could argue that this layer of statutory protection constitutes evidence that society views an expectation of privacy in electronic communications as reasonable.

Perhaps the most that can be said is that statutory and common-law-based privacy protections cannot alone determine the scope of an expectation of privacy for constitutional purposes. In any event, Congress has, by statute, aligned the interception of electronic communications with the use of wiretaps to obtain wire communications and the use of electronic listening devices to obtain oral communications.[60] To engage in such conduct, officials generally must seek a court order.[61] Because such an order is sufficient to overcome an expectation of privacy, courts have not addressed the application of the Fourth Amendment to the interception of electronic communications during transmission. I explore the development of the statutory regime below.

2. *The Statutory Framework*

a. *Traditional Electronic Surveillance Techniques*

In response to the Supreme Court's decisions in *Berger* and *Katz*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[62] In Title III, Congress adopted a pattern that it followed in later surveillance-related statutes: it prohibited surveillance activities, whether conducted by private parties or government officials, and excepted certain law enforcement conduct from the prohibition.[63] Title III provides for criminal penalties and civil damages against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept" any covered communication.[64] To "intercept" a

---

state law, was upheld by the Court because of the bag's exposure to the public. *Id.* at 38–41. For other formulations of how an expectation of privacy relates to statutory or common law protection of property or privacy, see, e.g., Kyllo v. United States, 533 U.S. 27, 34 (2001) (arguing that "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*," and that use of a device revealing what goes on inside the home constitutes a search for Fourth Amendment purposes); United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) (arguing that expectations of privacy stem from "reflections of law that translate into rules the customs and values of the past and present").

59 *Greenwood*, 486 U.S. at 43–44.

60 *See* 18 U.S.C. § 2510(4) (2000) (defining "intercept" as acquisition of contents of any wire, oral, or electronic communication); *id.* § 2511(1)(a) (prohibiting interception of wire, oral, and electronic communications); *id.* § 2518 (authorizing application for court order permitting "interception of wire, oral, or electronic communications"). The statutory changes occurred in 1986, as part of a broader update of surveillance law with respect to electronic communications. The changes are discussed *infra* notes 92–122 and accompanying text.

61 18 U.S.C. § 2518.

62 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801–804, 82 Stat. 211.

63 *See infra* notes 80–81 and accompanying text.

64 18 U.S.C. § 2511(1)(a).

communication is to use "any electronic, mechanical, or other device" to acquire its contents.[65] Although the definition did not require that a communication be acquired during its transmission, at the time the statute was passed that was the only way to intercept the contents of a communication. Title III initially covered "wire" communications, generally understood to mean telephone conversations,[66] and "oral" communications, defined as communications "uttered by a person exhibiting an expectation that such a communication is not subject to interception under circumstances justifying such expectation."[67] The statute exempted certain activities undertaken by private parties, including conduct by a service provider that is incident to the rendition of service[68] and conduct undertaken with the consent of one party to the communication.[69]

The most significant exception to Title III's coverage is for court-ordered electronic surveillance.[70] For years, Congress had been attempting to develop a new statutory framework for electronic surveillance activities.[71] Because *Berger* explicitly catalogued the constitutional deficiencies in New York's eavesdropping statute, the case provided a useful road map for how Congress and state legislatures could authorize law enforcement officials to seek court orders for surveillance activities.

The statute at issue in *Berger* allowed court authorization of eavesdropping activities, but the Court found the statutory procedures deficient in several respects. First, the statute required a showing of reasonable grounds to believe that the surveillance would reveal evidence of criminal activity. Although the Court declined to consider whether the "reasonable grounds" standard was equivalent to the Fourth Amendment's probable cause stan-

---

65 *Id.* § 2510(4).

66 Omnibus Crime Control and Safe Streets Act, § 802, 82 Stat. at 212 (adding 18 U.S.C. § 2510(1)).

67 *Id.* (adding 18 U.S.C. § 2510(2)).

68 18 U.S.C. § 2511(2)(a)(i).

69 *Id.* § 2511(2)(c), (d). A person acting under color of law may intercept a communication with the consent of one of the parties; a person not acting under color of law may do so unless he or she has a criminal or tortious purpose. *Id.*

70 Title III allows law enforcement surveillance to proceed without a court order in an emergency situation, but it requires officials to request an order authorizing such surveillance within forty-eight hours. *Id.* § 2518(7).

71 Federal law had outlawed wiretapping—by private or governmental entities—since 1934, and many states also barred the practice. Act of June 19, 1934, ch. 652, § 605, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605 (2000)); *see* 1 CARR & BELLIA, *supra* note 21, § 2:8, at 2-10. These official proscriptions were widely disregarded. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. (forthcoming 2004). As for eavesdropping, the Court's reliance in *Olmstead v. United States*, 277 U.S. 438, 466 (1928), on a trespassory entry as the trigger for application of the Fourth Amendment led to a body of case law under which officials' choice of equipment for overhearing a conversation determined the permissibility of the conduct: a bug placed on an adjacent wall was held permissible, *see* Goldman v. United States, 316 U.S. 129, 135, 512 (1942), while a "spike mike" that penetrated property by less than an inch was not, *see* Silverman v. United States, 365 U.S. 505, 512 (1961). No federal statute regulated the practice. 1 CARR & BELLIA, *supra* note 21, § 2:25, at 2-21. For discussion of pre-Title III state laws regulating wiretapping and eavesdropping, see *id.* §§ 2:18–2:22, 2:28, at 2-17 to 2-20, 2-22.

dard,[72] the statute failed to satisfy the Fourth Amendment requirement that the crime to be investigated, the place to be searched, and the persons or things to be seized be particularly described.[73] Second, the statute imposed no limitations on which conversations could be seized[74] or the duration of the surveillance,[75] nor did it require termination of surveillance activities once the goals of the surveillance were met.[76] Third, the statute allowed law enforcement officials to secure renewal of a surveillance order on the basis of the initial showing.[77] Fourth, the statute did not provide for prior notice of the search to the subject of the surveillance and required no showing of exigency to justify the lack of notice.[78] Finally, the statute did not provide for a "return" on the warrant to a judge, "thereby leaving full discretion in the officer as to the use of seized conversations of innocent as well as guilty parties."[79]

With Title III, Congress sought to overcome each of these deficiencies. Under Title III, for federal investigations of certain serious crimes, an attorney for the government (after securing approval of a high-level official in the Department of Justice) may apply for a court order authorizing an interception.[80] Surveillance by state authorities is also permitted if it conforms with a state authorizing statute that is at least as restrictive as Title III.[81] In keeping with *Berger*'s requirements, Title III requires that the application specify the offense being investigated, the nature and location of the facilities where the communications are to be intercepted, and a particular description of the communications sought to be intercepted.[82] To grant the order, the court must find probable cause to believe that a particular enumerated offense is being committed and that targeting the specified facility will yield particular communications concerning that offense.[83] Congress dealt with *Berger*'s objection to the indeterminate length of surveillance under the New York statute by providing that orders may authorize surveillance only as long as necessary for achievement of the objective, up to thirty days.[84] A court may grant an extension, but only subject to the same showings and findings as the original order.[85] The statute also requires a court to order officials to "minimize" the interception of communications unrelated to criminal activity.[86] In light of *Berger*'s objection that the New York statute required no showing of exigency to justify the lack of notice, Title III requires a finding that normal

72 Berger v. New York, 388 U.S. 41, 55 (1967).
73 *Id.* at 55–56.
74 *Id.* at 59.
75 *Id.* at 59–60.
76 *Id.* at 59.
77 *Id.*
78 *Id.* at 60.
79 *Id.*
80 18 U.S.C.A. § 2516(1) (West Supp. 2003).
81 18 U.S.C. § 2516(2) (2000).
82 *Id.* § 2518(1) (specifying contents of application).
83 *Id.* § 2518(3) (specifying contents of order).
84 *Id.* § 2518(5).
85 *Id.*
86 *Id.*

investigative procedures are unlikely to be successful or are too dangerous[87] and generally requires notice to the target of the investigation within ninety days of the termination of the surveillance.[88] Finally, Congress required law enforcement officials to take a variety of steps that provide the functional equivalent of a return to a judge. For example, Title III requires law enforcement officials to record intercepted communications and to make the recordings available to the judge.[89] The statute also authorizes a judge to require periodic reports on the progress of the surveillance.[90] Oral and wire communications obtained in violation of the statute, whether by private parties or by the government, cannot be used as evidence.[91]

b. Electronic Communications

Because Title III, as enacted in 1968, covered only the interception of "wire" and "oral" communications rather than communications generally, the development of electronic communications created a gap in the statute. In 1986, Congress sought to fill this gap with the Electronic Communications Privacy Act ("ECPA").[92] Each of ECPA's three titles dealt with a different aspect of surveillance: the first updated Title III to cover electronic communications;[93] the second established a separate chapter of the federal criminal code setting forth privacy protections and government access rules for stored wire and electronic communications and associated data;[94] and the third established privacy protections and government access rules for telephone dialing and signaling information.[95] I explore the first set of changes here.

ECPA amended Title III to prohibit not only the interception of wire and oral communications but also the interception of electronic communications. Congress defined an electronic communication in part as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," but excluded wire and oral communications from the definition.[96] In addition to altering the substantive prohibition by adding electronic communications to the list of covered communications, Congress also altered the definition of "intercept." Previously, the statute defined "intercept" as the

87 *Id.* § 2518(3)(c).

88 *Id.* § 2518(8)(d).

89 *Id.* § 2518(8)(a).

90 *Id.* § 2518(6).

91 *Id.* § 2515 (barring use of wire and oral communications as evidence when disclosure of such communications would violate statute); *id.* § 2518(10)(a) (allowing aggrieved person to seek suppression of contents of wire or oral communications on grounds that interception was unlawful or failed to conform with terms of order). For a discussion of some of the court-created exceptions to these suppression provisions, see *infra* notes 105–06 and accompanying text.

92 Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848.

93 *Id.* §§ 101–111, 100 Stat. at 1848–59.

94 *Id.* §§ 201–202, 100 Stat. at 1860–68.

95 *Id.* §§ 301–302, 100 Stat. at 1868–72.

96 18 U.S.C. § 2510(12) (2000).

"aural acquisition" of the contents of a communication;[97] as amended, the statute defined "intercept" as "the aural or other acquisition" of the contents of a communication,[98] thereby clarifying that electronic communications need not be "aurally" acquired.

Although the inclusion of electronic communications in the statute had the effect of requiring law enforcement officials to seek a court order before intercepting electronic communications, Congress elected to treat electronic communications differently from wire and oral communications in several ways. First, § 2516(1) specifies the range of federal felonies for which government officials can seek orders to engage in surveillance of wire and oral communications.[99] Although that list has grown considerably since Title III's enactment in 1968, it does not encompass all federal felonies. Under § 2516(3), however, law enforcement officials are authorized to seek Title III orders for surveillance of electronic communications in connection with any federal felony.[100] Second, § 2516(1) also requires approval of certain high-level officials in the Justice Department before a request for surveillance of wire and oral communications can be sought from a court.[101] No similar statutory restriction exists in § 2516(3) for surveillance of electronic communications, although the Justice Department has abided by such a restriction as a matter of policy.[102]

Finally, §§ 2515 and 2518(10) bar the use in evidence of wire and oral communications obtained in violation of the statute or in violation of a Title III order.[103] On its face, the statute thus requires suppression of wire and oral communications even for Title III violations that do not also violate the Fourth Amendment, and even when the Fourth Amendment would not require exclusion because officials obtained the communications in good-faith reliance on a court order.[104] The force of these statutory exclusion provisions has been limited somewhat by a line of cases holding that suppression lies only for "substantial" violations of the statutory scheme,[105] and by courts' confusion regarding whether the good-faith exception to the Fourth Amendment's exclusionary rule should in fact apply to violations of Title III.[106] In

---

97 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 211, 212 (adding 18 U.S.C. § 2510(4)).

98 18 U.S.C. § 2510(4).

99 *Id.* § 2516(1).

100 *Id.* § 2516(3).

101 *Id.* § 2516(1).

102 *See* U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-7.100, http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/7mcrm.htm (last visited July 18, 2004). During negotiations over the legislation, the Justice Department and Congress apparently agreed informally that for three years the Department should apply the same review procedures for interception of electronic communications as for interception of wire and oral communications. After the three-year period, the Department rescinded the approval requirement for interception of electronic communications over digital display paging devices but retained it for all other electronic communications. *Id.*

103 18 U.S.C. §§ 2515, 2518(10).

104 *See* United States v. Leon, 468 U.S. 897, 916 (1984).

105 *See* United States v. Chavez, 416 U.S. 562, 568–69 n.2 (1974); United States v. Giordano, 416 U.S. 505, 527 (1974).

106 The text of Title III contains no indication that a good-faith exception should apply.

enacting ECPA in 1986, however, Congress did not authorize statutory suppression for interception of electronic communications in violation of Title III.[107] Accordingly, a court may only suppress improperly intercepted electronic communications if the contested actions rise to the level of a violation of the Fourth Amendment, and then only if officials did not act in good-faith reliance on a Title III order.

Apart from the fact that ECPA did not extend all of Title III's protections to electronic communications, Title III does not prohibit all methods by which electronic communications might be acquired. In particular, Title III only prohibits the *interception* of electronic communications. As noted earlier, at the time Title III was passed, wire and oral communications could only be intercepted as they occurred. Electronic communications, however, can be stored at various points on a computer network. The extension of Title III to electronic communications thus raised the question whether the prohibition on interception covered only the extraction of electronic communications during transmission, or whether it also covered the acquisition of such communications from storage. The development of voice mail services raised a similar question: would the acquisition of a stored wire communication constitute an interception?

Although Congress redefined the term "intercept" in 1986 to clarify that communications need not be "aurally" acquired,[108] it did not address this issue directly. Several other clues nevertheless led courts to conclude that, at

---

The report of the Senate Committee on the Judiciary accompanying the bill, however, indicated that Title III was intended to mirror the Fourth Amendment in its remedies. S. REP. NO. 90-1097, at 96 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185. Some courts have assumed that Title III's statutory exclusionary rule imports later developed changes to the Fourth Amendment's exclusionary rule, including the good-faith exception recognized in 1984 in *United States v. Leon*, 468 U.S. 897 (1984). *See, e.g.*, United States v. Moore, 41 F.3d 370, 376 (8th Cir. 1994). Other courts have relied on ECPA's amendments to Title III rather than Title III's legislative history. In particular, courts have focused on § 2518(10)(c), which ECPA added to Title III in 1986 and which states that "[t]he remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violation of this chapter involving such communications." 18 U.S.C. § 2518(10)(c). Because some courts have failed to note that § 2518(10)(c) applies only to *electronic* communications—and not to wire or oral communications—they have mistakenly interpreted § 2518(10)(c) as altering Title III's remedies for wire and oral communications as well, finding statutory suppression available for *nonconstitutional* violations of Title III, but importing Fourth Amendment principles, including *Leon*'s good-faith exception, for *constitutional* violations. *See* United States v. Gangi, 33 F. Supp. 2d 303, 307 (S.D.N.Y. 1999) (declining to suppress wiretap evidence on ground that probable cause was lacking and holding that even if probable cause showing was insufficient, interceptions were performed in good-faith reliance on judge's order); United States v. Ambrosio, 898 F. Supp. 117, 187 (S.D.N.Y. 1995) (holding that the good-faith exception applies to Title III); United States v. Ferrara, 771 F. Supp. 1266, 1273 (D. Mass. 1991) (denying a motion to suppress and holding that Title III incorporates *Franks v. Delaware*, 438 U.S. 154 (1978)); *see also* 2 CARR & BELLIA, *supra* note 21, § 6:40, at 6-99 to 6-100. For a useful discussion of these issues, see Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393 (1997).

107 18 U.S.C. § 2518(10)(a), (c); *see* United States v. Steiger, 318 F.3d 1039, 1050–52 (11th Cir. 2003); United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990); United States v. Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996).

108 *See supra* note 98 and accompanying text.

least for electronic communications, an interception occurs only when a communication is seized during its transmission.[109] In particular, ECPA created a separate chapter of the criminal code dealing with the acquisition of stored communications, with a prohibition on private and governmental conduct and exceptions for certain law enforcement activities.[110] If Title III already prohibited the acquisition of stored communications, then much of that statute would have been rendered redundant. In addition, Congress defined the terms "electronic communication" and "wire communication" differently. Congress specifically defined the term wire communication to include "any electronic storage of such communication," but did not define electronic communication to include electronic storage.[111] The purpose of including stored communications in the definition of wire communication was to make clear that law enforcement officials had to obtain a full Title III order to gain access to such communications.[112] Some courts concluded that Congress did not intend Title III to apply to the acquisition of stored electronic communications, because Congress included "electronic storage" within the definition of a wire communication, but excluded that phrase from the definition of an electronic communication. These courts held that to "intercept" an electronic communication meant only to acquire it during transmission.[113] In *Konop v. Hawaiian Airlines, Inc.*,[114] the United States Court of Appeals for the Ninth Circuit concluded otherwise, believing that an earlier Ninth Circuit decision with respect to *wire* communications, *United States v. Smith*,[115] compelled its decision.[116] In *Smith*, the Ninth Circuit had relied in part on the inclusion of "electronic storage" in the definition of a wire communication to state, in dictum, that Title III prohibits the acquisition of wire communications from electronic storage, not merely the acquisition of wire communications during transmission.[117] Because the *Konop* court reasoned that Title III's prohibition on interception should apply equally to wire and electronic

---

109 *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113–14 (3d Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Wesley Coll. v. Pitts, 974 F. Supp. 375, 388 (D. Del. 1997); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996); *Reyes*, 922 F. Supp. at 837.

110 *See infra* notes 216–82 and accompanying text.

111 *Compare* 18 U.S.C. § 2510(1) (2000), *with id.* § 2510(12).

112 That conclusion flowed not only from the inclusion of "any electronic storage of [a] communication" within Congress's definition of a "wire communication," *see id.* § 2510(1), but also from the fact that Title III was the only law enforcement avenue that applied to the acquisition of wire communications and that was exempted from the substantive prohibition on unauthorized access to stored communications, *see id.* § 2701(c) (exempting conduct authorized under 18 U.S.C. § 2518 and 18 U.S.C. § 2703 from substantive prohibition); *id.* § 2703 (setting forth procedures for government access to stored *electronic* communications).

113 *See supra* note 109 and accompanying text.

114 Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir.) (concluding that unauthorized access to a secure web site constituted an interception), *withdrawn*, 262 F.3d 972 (9th Cir. 2001), *new opinion filed*, 302 F.3d 868 (9th Cir. 2002).

115 United States v. Smith, 155 F.3d 1051 (9th Cir. 1998).

116 *Konop*, 236 F.3d at 1043–44.

117 *See Smith*, 155 F.3d at 1059. This case involved a voice mail message, obtained by a private party but turned over to law enforcement, that revealed criminal conduct. *Id.* at 1053–54. Even though the court characterized the question whether an interception had occurred as a threshold issue, its ultimate affirmance of the district court's conclusion that the

communications, the court concluded that the prohibition on interception must also cover the acquisition of electronic communications from electronic storage.[118] The court ultimately withdrew its opinion, and Congress soon clarified in the USA Patriot Act that Title III would no longer control law enforcement access to stored wire communications.[119] Over a dissent arguing that the USA Patriot Act did not affect the definition of the term "intercept,"[120] the superseding Ninth Circuit opinion followed other courts in holding that Title III only prohibits the interception of communications in transit.[121] In other words, although Congress never specifically defined "intercept" to mean acquisition of communications during transmission, the USA Patriot Act (in a provision scheduled to expire in 2005) removed the strongest argument that the term covers the acquisition of stored communications.

Congress's partial extension of the Title III framework to electronic communications in 1986 seemed to reflect the view that electronic communications are sufficiently similar to wire communications to warrant coverage in the same basic statutory surveillance scheme, but that electronic communications are nevertheless in some respects less deserving of protection than wire communications. I will argue later that there is no principled basis for the

---

admitted evidence was not derived from the voice mail message rendered its analysis of whether an interception had occurred unnecessary. *Id.* at 1063.

118 *Konop*, 236 F.3d at 1046. The *Konop* court was correct that the logic of the *Smith* court's reasoning compelled its holding, but the *Smith* court's reasoning was deeply flawed. A detailed discussion of the case is beyond the scope of this Article. Briefly, however, the court erroneously suggested that interpreting Title III to cover only interception of wire communications in transit would render meaningless the inclusion of "electronic storage" within the definition of a "wire communication." *Smith*, 155 F.3d at 1058 & n.12. The court ignored the fact that the inclusion of "electronic storage" within the definition of a "wire communication" in Title III served to emphasize the procedure that *law enforcement* officials had to follow to gain access to voice mail messages. In addition, to eliminate the overlap between Title III and the stored communications provisions that its reading created, the court essentially excised a portion of the substantive prohibition on unauthorized access to stored communications. *See id.* at 1058–59 (reading the substantive prohibition at 18 U.S.C. § 2701(a), which reaches one who "intentionally accesses" a facility "*and thereby obtains*" a wire communication, to prohibit the preliminary conduct by which one is in a position to acquire the contents of a communication (emphasis added)).

119 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 209, 115 Stat. 272, 285.

120 *Konop*, 302 F.3d at 891 & n.2 (Reinhardt, J., dissenting).

121 *Id.* at 878. While abandoning its problematic reading of Title III, however, the court adopted an equally strained reading of the Stored Communications Act ("SCA"). *See* Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, §§ 201–202, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C.A. §§ 2701–2709, 2711–2712 (West 2000 & Supp. 2003)). A detailed examination of the problem is beyond the scope of this Article. Briefly, the court ignored the fact that the SCA applies only to communications in "electronic storage." Because that term applies only to communications in "temporary, intermediate storage," and communications in "backup protection," it does not cover files maintained indefinitely on a web server. *See* 18 U.S.C. § 2701(a)(1) (2000); *id.* § 2510(17). The court also improperly accepted the parties' characterizations of Konop's web site as an "electronic communication service." *See Konop*, 302 F.3d at 879.

watered down protection of electronic communications.[122] The difficulties with respect to electronic communications, however, arise less from the inconsistencies in Title III's treatment of wire and electronic communications than from the fact that electronic communications tend to be stored far more frequently than wire communications. Because Title III covers only the interception of communications in transit, law enforcement officials have alternatives to the statute's relatively stringent procedures: compelling production of copies of stored communications from service providers. I discuss the rules for government acquisition of stored communications in the next section.

B. Acquisition of Stored Communications and Related Records

Although the protection against interception that federal law affords to electronic communications is not identical to the protection afforded wire and oral communications, the statutory rules are nevertheless clear. The constitutional and statutory questions are more difficult when, rather than using a device to extract or replicate a communication as it is being transmitted, officials seek to compel production of a copy of the communication that is stored with a third party. For example, a phone company may offer its customers a voice mail service with a password-protected voice mailbox; the mailbox may store copies of messages awaiting subscriber retrieval or old messages that the subscriber chooses to retain. Similarly, an Internet service provider that provides its users with the ability to send and receive e-mail will hold copies of incoming messages awaiting retrieval by a subscriber, copies of outgoing messages, and copies of messages the user chooses not to delete.

If law enforcement officials seek to acquire copies of a subscriber's communications from a third party such as a voice mail provider or an e-mail provider, the question is what kind of legal process such officials must present to the provider. If the communications were held only on a subscriber's computer inside of the subscriber's home, law enforcement officials generally could not view the communications without a warrant. Does the fact that a third party stores communications on a user's behalf change the inquiry, such that law enforcement officials could compel production of the communications without a warrant? The underlying constitutional question involved in such cases is whether one retains an expectation of privacy in copies of communications held by a third party. This question is a difficult one, in part because different lines of Fourth Amendment cases point in different directions. The prevailing view within the government is that the Fourth Amendment does not protect against warrantless access to such communications. I challenge the doctrinal and normative underpinnings of that view. In 1986, in the second title of ECPA, Congress adopted a layer of statutory protection for stored communications.[123] Stored communications have evolved in such

---

122 The differential treatment apparently represented the price of the Justice Department's support for extending Title III to electronic communications in 1986. *See* S. REP. NO. 99-541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

123 *See* ECPA, 100 Stat. at 1860–86 (codified as amended at 18 U.S.C.A. §§ 2701–2709, 2711–2712 (West 2000 & Supp. 2003)).

a way that these provisions, often referred to as the Stored Communications Act ("SCA"), are becoming increasingly outdated and difficult to apply. In addition, because the provisions were adopted amid uncertainty about whether the Fourth Amendment protects privacy in communications held by a third-party service provider, they allow law enforcement officials to compel production of some categories of communications without a search warrant.[124] As I will show, revision of the statutory framework is urgently needed.

1. The Constitutional Framework

a. Antecedents to United States v. Miller

To evaluate the claim that the Fourth Amendment does not protect the privacy of communications in the hands of a third-party service provider, it is necessary to understand two distinct lines of cases that converged—or, rather, were conflated—several years after the Supreme Court's decision in *Katz v. United States*.[125] One line of cases deals with the use of an administrative or grand jury subpoena to compel production of "business records" in the hands of a third party, over the objection of the documents' owner (or the person whom the documents incriminate) that the compulsion to produce the documents constitutes an unreasonable search and seizure. The second line of cases deals not with business records but with the contents of communications, obtained from an informant or a government agent who is a party to the communications. I explore the development of these lines of cases in turn.

Before its decision in *Katz*—holding, as discussed above, that whether a "search" occurs for purposes of the Fourth Amendment depends on whether the government's conduct invades a reasonable expectation of privacy—the Supreme Court had considered several claims that the compelled production of certain documents would violate the Fourth Amendment's prohibition on warrantless searches and seizures, as well as the Fifth Amendment's privilege against self-incrimination. In *Boyd v. United States*,[126] the Court held that, in an action for forfeiture of goods that the government claimed had been fraudulently imported by a company that failed to pay the requisite duty, both the Fourth and Fifth Amendments barred the government from issuing a subpoena compelling the claimed owners of the goods to produce relevant invoices.[127] The Court equated the compelled production of the invoices with a "search and seizure of a man's private papers."[128] After the Supreme Court held that a corporation and its officers could not invoke the Fifth Amendment privilege against the production of corporate records pursuant to lawful judicial process,[129] corporations continued to attempt to block enforcement of administrative and grand jury subpoenas by asserting Fourth

124 *See* 18 U.S.C.A. § 2703 (West Supp. 2003).

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

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

127 *Id.* at 638.

128 *Id.* at 622–23 (describing the predecessor to the statute at issue in *Boyd*).

129 *See, e.g.*, Hale v. Henkel, 201 U.S. 43, 70 (1906).

Amendment claims, relying on the language from *Boyd* quoted above.[130] The Court rejected such claims, but in doing so underscored the fact that the records involved were merely *corporate* records. In *Oklahoma Press Publishing Co. v. Walling*,[131] for example, the Court distilled prior case law as follows: "[I]n so far as [earlier cases] apply *merely to the production of corporate records and papers* in response to a subpoena or order authorized by law and safeguarded by judicial sanction," those cases establish that the Fourth Amendment "guards against abuse only by way of too much indefiniteness or breadth . . . if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant."[132]

Although pre-*Katz* case law thus established the constitutionality of the use of a subpoena to compel production of corporate records, the Court's decision in *Katz* supplied a new basis for Fourth Amendment challenges to such conduct: that the owner or subject of the records had an expectation of privacy in the documents. The Supreme Court first addressed such a claim in *Couch v. United States*.[133] There the IRS had issued a summons to compel an accountant to surrender certain records that Couch, a taxpayer, had provided to the accountant for use in preparing Couch's tax return.[134] When the accountant refused to produce the records and the IRS sought judicial enforcement of the summons, Couch intervened to assert that her Fifth Amendment privilege against self-incrimination barred the government from compelling the accountant to produce the records, arguing that the privilege should run with ownership rather than possession of the documents.[135] Couch also claimed that enforcement of the summons would violate her Fourth Amendment right to be secure from unreasonable searches and seizures.[136] Because the Court found that the Fourth Amendment claim was not well articulated, and "[did] not appear to be independent of [the taxpayer's] Fifth Amendment argument,"[137] the Court gave the claim only brief treatment in its opinion.[138] The Court nevertheless concluded that "the necessary expectation of privacy" under *Katz* "to launch a valid Fourth Amendment claim does not exist,"[139] reasoning that "there can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return."[140] Despite the fact that the *Couch* Court did not perceive the taxpayer to have offered an independent Fourth Amendment claim, *Couch* became the foun-

130 *See infra* notes 207–08.

131 Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208 (1946).

132 *Id.* at 208 (emphasis added). The Court explained that Congress can authorize access to corporate records by administrative subpoena in part because, when a corporation's activities affect interstate commerce, Congress possesses a wide investigative power over it, "analogous to the visitorial power of the incorporating state." *Id.* at 204 & nn.31–32.

133 Couch v. United States, 409 U.S. 322 (1973).

134 *Id.* at 323–24.

135 *Id.* at 325, 331.

136 *Id.* at 325 n.6.

137 *Id.* at 325–26 n.6.

138 *See id.* at 335–36.

139 *Id.* at 336 n.19.

140 *Id.* at 335.

dation for a series of cases involving business records turned over to third parties for the third parties to perform particular tasks with such records—with all of the cases rejecting claims that an individual can retain an expectation of privacy in the records. I return to those business records cases below.[141]

The second line of cases relevant to the protection of communications stored with a third party involves communications revealed, recorded, or transmitted to the government by a government informant or undercover agent who is a party to the communications. Prior to its decision in *Katz*, the Supreme Court had held on several occasions that the Fourth Amendment does not preclude a government informant from testifying about a conversation to which he was a party, and does not preclude the admission into evidence of a conversation surreptitiously recorded by a government informant. Two opinions handed down on the same day in 1966 illustrate the Court's approach. In *Hoffa v. United States*,[142] Hoffa sought to suppress testimony of a witness who had been present for several conversations in which Hoffa discussed bribing jurors to vote for his acquittal in a separate federal criminal trial.[143] The Court assumed that the witness in question was a government informant,[144] but concluded that "no interest legitimately protected by the Fourth Amendment is involved," because the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[145] Similarly, in *Osborn v. United States*,[146] Hoffa's attorney was charged with attempting to bribe jurors in another trial.[147] A local detective who had agreed to perform private investigative work for the attorney regarding potential jurors, but who in fact was acting as a government informant, taped a conversation with the attorney.[148] Osborn challenged the admissibility of the tape recording in his jury-tampering trial.[149] The Court concluded that the tape was admissible.[150] The Court emphasized that the government informant was a party to the conversation: "We thus deal here not with surreptitious surveillance of a private conversation by an outsider, but . . . with the use by one party of a device to make an accurate record of a conversation about which that party later testified."[151] In *Osborn*, the conclusion that the Fourth Amendment did not preclude a government informant from testifying about a conversation to which he was a party was not critical to the Court's holding, because a district court judge had authorized the use of the recorder.[152] The Court nevertheless acknowl-

141 *See infra* notes 158–66, 178 and accompanying text.

142 Hoffa v. United States, 385 U.S. 293 (1966).

143 *Id.* at 294–95.

144 *Id.* at 299.

145 *Id.* at 302.

146 Osborn v. United States, 385 U.S. 323 (1966).

147 *Id.* at 324.

148 *Id.* at 325–26.

149 *Id.* at 326.

150 *Id.* at 331.

151 *Id.* at 327 (citations omitted).

152 *Id.* at 329–30.

edged that it had previously held, in *Lopez v. United States*,[153] that evidence derived from a conversation surreptitiously recorded by a government agent was admissible, even though law enforcement officials had not sought prior judicial authorization for use of the recording device.[154] Nothing in *Osborn* cast doubt upon that conclusion.

Just as *Katz* spurred new (though ultimately unsuccessful) challenges to the use of subpoenas to compel production of business records, so too did the decision lead to renewed challenges to the admissibility of evidence concerning conversations to which a government informant was a party. In particular, defendants argued that *Katz*'s recognition that the Fourth Amendment guards against invasion of an expectation of privacy without a warrant disturbed the holdings of *Lopez*, *Hoffa*, and *Osborn*, because one has an expectation of privacy that a party with whom one is conversing will not reveal the contents of the conversation to law enforcement officials. The Supreme Court first faced such a claim in *United States v. White*.[155] There, a district court had allowed admission of the contents of a conversation transmitted to law enforcement officials by a government informant wearing an electronic listening device.[156] Although no opinion of the Court commanded a majority, a plurality of the Court distinguished *Katz* as follows:

> *Katz* involved no revelation to the Government by a party to conversations with the defendant nor did the Court indicate in any way that a defendant has a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police.[157]

Within a few years of the Supreme Court's decision in *Katz*, then, two rules emerged. First, the Fourth Amendment does not preclude use of a summons or subpoena to compel production of business records in the hands of a third party; and second, the Fourth Amendment does not prevent a government informant or undercover agent who is a party to a conversation from revealing, recording, or transmitting the contents of the conversation to law enforcement officials.

b. Miller *and Its Progeny*

The Supreme Court linked together these two lines of cases in *United States v. Miller*.[158] There, the Court considered whether an individual had a reasonable expectation of privacy in checks, financial statements, and deposit slips that banks held concerning his accounts.[159] The government had subpoenaed the records from the banks, which complied without objection.[160] The Court rejected Miller's claim that the Fourth Amendment required the

153 Lopez v. United States, 373 U.S. 427 (1963).

154 *Id.* at 439.

155 United States v. White, 401 U.S. 745 (1971) (plurality opinion).

156 *Id.* at 746–47.

157 *Id.* at 749; *see also* United States v. Caceres, 440 U.S. 741, 750–51 (1979) (following *White*).

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

159 *Id.* at 438.

160 *Id.* at 442.

government to present a warrant to obtain the information, concluding that Miller had no legitimate expectation of privacy in the contents of the documents.[161] The Court first drew upon the reasoning of *Couch* to examine the type of records involved and the independent interest of the persons receiving the documents in the documents' contents: "We must examine the *nature of the particular documents* sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[162] The records involved in *Couch* were business records containing information that the accountant needed in order to complete a tax return.[163] Similarly, the checks at issue in *Miller* were "not confidential communications but negotiable instruments to be used in commercial transactions," and the other documents obtained, "including financial statements and deposit slips," contained only "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[164]

Although initially focusing, as the *Couch* Court did, on the nature of the documents involved and the relevance of their contents to the bank's activities, the Court shifted its analysis and drew upon the government informant and undercover agent cases. Citing *Lopez*, *Hoffa*, and *White*, the Court reasoned:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[165]

Miller was similar to *Couch*, in that, first, it dealt with a subpoena for production of documents rather than involvement of a government agent; and second, the subpoena sought documents that had been conveyed to the bank to complete particular transactions, and the contents of which were independently relevant for the bank to do so. The outcome in *Couch* did not depend on the conclusion that one who conveys documents to a third party, expecting the third party to hold them in confidence, *assumes the risk* that the third party will reveal the documents' contents to authorities. The documents at issue in *Couch* themselves contained information required to be disclosed by law.[166] In other words, it was the nature of the documents and the tasks for which the taxpayer expected the accountant to use the documents, not the mere fact that the taxpayer had conveyed them to a third party, that eliminated any expectation of privacy. The Court could have taken the same approach with respect to the documents at issue in *Miller*. By

---

161 *Id.* at 440.

162 *Id.* at 442 (citing Couch v. United States, 409 U.S. 322, 335 (1973)) (emphasis added).

163 *Couch*, 409 U.S. at 323.

164 *Miller*, 425 U.S. at 442.

165 *Id.* at 443 (citations omitted).

166 *Couch*, 409 U.S. at 335.

relying on *Lopez*, *Hoffa*, and *White*, however, the *Miller* Court introduced an assumption-of-risk analysis not previously present in the business records cases. Read broadly, *Miller* suggests that the mere fact that documents are conveyed to a third party, without regard to the type of documents at issue or the purpose for which the documents were provided, eliminates any expectation of privacy.

Three years later, in *Smith v. Maryland*,[167] the Court relied on *Miller* in holding that one lacks an expectation of privacy in the telephone numbers one dials.[168] The Court reasoned that one necessarily conveys such information to the phone company, knowing that the phone company uses it for a variety of legitimate purposes.[169] As in *Miller*, however, the Court used broader language than necessary to resolve the case, stating that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[170] As in *Miller*, the Court cited not only the business records approach of *Couch*, but also the series of government informant cases, including *Hoffa*, *White*, and *Lopez*.[171]

What do these cases tell us about the circumstances in which the government can compel a service provider to produce the contents of communications maintained on its system on behalf of a user? The broad language of *Miller* and *Smith*, and in particular the *Miller* Court's statement that one "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government,"[172] provides the basis for arguments that a subscriber lacks an expectation of privacy in communications held by a service provider, and that, in the absence of statutory protection, such communications are subject to subpoena.[173] In Part I.B.2, I explain how the current statutory framework governing access to stored communications appears to be premised on this approach;[174] here, I call the broader constitutional argument into question.

---

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

168 *Id.* at 743–44.

169 *Id.* at 744.

170 *Id.* at 743–44.

171 *Id.* at 744.

172 United States v. Miller, 425 U.S. 435, 443 (1976).

173 COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § III.A (2002), http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (last visited July 18, 2004) [hereinafter CCIPS MANUAL] ("[T]he Fourth Amendment generally permits the government to issue a subpoena to a network provider ordering the provider to divulge the contents of an account."); 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, 1210 & n.11 (2004) [hereinafter Kerr, *A User's Guide to the Stored Communications Act*]; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1135 (2002) ("Individuals . . . probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network system administrators."); *see also* Brief of Amicus Curiae Professor Orin S. Kerr at 8–11, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), 2000 WL 33986512.

174 *See infra* notes 238–82 and accompanying text.

c. The Limits of Miller *and Its Progeny*

The conclusion that *Miller*, *Smith*, and like cases foreclose any claim of an expectation of privacy in communications held by a service provider fails to acknowledge the factual contexts of *Miller* and *Smith* themselves, as well as the doctrinal and normative underpinnings of those decisions. A broad reading of *Miller* and *Smith* is also fundamentally inconsistent with *Katz*.

First, it should be clear that the factual scenarios in *Miller* and *Smith* differ dramatically from those involved when an individual engages a communication service to facilitate the transmission and receipt of communications. There are at least four differences that are relevant to an assessment of an expectation of privacy: (1) the *type of information* at issue; (2) the *individual's purpose* in placing information in the hands of the third party; (3) the *relevance of the substance* of the information to the third party's activities; and (4) the limitations on the third party's *ability to gain access to or use the substance* of the information.

Neither *Miller* nor *Smith* involved the substance of personal communications. In both *Miller* and *Smith*, the defendants conveyed information so that the recipient would do something with that information. Miller's purpose in revealing information to the bank was for the bank to complete his transactions. Smith's purpose in dialing the number was for the telephone company to complete his call, and the telephone number was necessary for the telephone company to do so. In both cases, the substance of the information at issue was not only relevant to the recipient, it was essential for the recipient to conduct the transactions in question. In neither case was the recipient limited in his or her ability to gain access to the substance of the information.

Miller and *Smith* differ from the situation of a subscriber who uses a service provider to facilitate the transmission and receipt of his or her electronic communications. Although there are, of course, a range of service providers with different sorts of relationships with their users—from commercial providers offering service to the general public for a fee, to private providers, such as employers, offering service to their employees for business purposes—it is useful to consider the relationship between a commercial provider and a user. First, unlike the relationship between a customer and a bank, the subscriber's relationship with the service provider does not dictate the type of information the subscriber seeks to transmit or receive, and the information therefore will not necessarily be a business record. The subscriber simply acquires individual storage space on a provider's system, ordinarily segregated from others' space by a password or analogous access control. Second, the subscriber conveys communications to the service provider not because the contents of the communications are relevant to any transaction with the service provider, but because the subscriber wants the service provider to process them, much as a carrier transports a sealed package,[175] and to store them, much as a storage facility holds personal property.[176] While a service provider may need to access certain subscriber data and other information to provide and bill for its services, the particular *con-*

175 *See infra* note 186 and accompanying text.

176 *See infra* note 185 and accompanying text.

tents of communications the user stores with the service provider are not necessary or relevant for the service provider to transmit the communication. Indeed, the provider may be contractually barred from inspecting contents of communications except to maintain the service and prevent intrusions.[177]

If a provider has no reason to access communications to effect a purpose of a subscriber in providing them, then *Miller*, *Smith*, and like cases—where the sole purpose of providing information is to complete a transaction—are distinguishable.[178] In maintaining storage space on a provider's system, a user is not "revealing his affairs to another" in the sense the Court contemplated in *Miller*,[179] let alone "knowingly expos[ing]" his communications "to the public."[180] That *Miller* and its progeny provide minimal guidance for cases involving service providers holding communications on another's behalf becomes even clearer when the relationship between the subscriber and the service provider is analyzed in light of *Miller*'s doctrinal underpinnings. The relationship between a subscriber and service provider is not a relationship in which the subscriber merely conveys business records, and *Couch* is therefore inapposite. I made the case earlier that *Miller* wrongly relies on the government informant cases.[181] Even if those cases are relevant in *Miller*, however, they do not point to the conclusion that one lacks an expectation of privacy in communications held by a service provider. In *Lopez*, *Hoffa*, *Osborn*, and *White*, the informant was a *party* to the relevant communications, and that fact defeated any Fourth Amendment claim.[182] A service provider is

---

177 *Compare, e.g.*, AOL Legal Dept., America Online, Privacy Policy, *at* http://legal.web.aol.com/aol/aolpol/privpol.html#1 (last visited July 3, 2004) (stating that "AOL does not read or disclose private communications except to comply with valid legal process . . . to protect the company's rights and property, or during emergencies when we believe physical safety is at risk"), *with* Microsoft, MSN Website Terms of Use and Notices, *at* http://privacy.msn.com/tou/default.asp (last visited July 3, 2004) ("To the maximum extent permitted by applicable law, Microsoft may monitor your e-mail, or other electronic communications and may disclose such information in the event it has a good-faith reason to believe it is necessary for purposes of ensuring your compliance with this Agreement, and protecting the rights, property, and interests of the Microsoft Parties or any customer of a Microsoft Party.").

178 Other cases sustaining the use of a subpoena to compel the production of records in the hands of a third party are also distinguishable from situations in which a service provider receives and maintains potentially personal communications on behalf of, and solely for the use of, an individual. *See* Donovan v. Lone Steer, Inc., 464 U.S. 408, 415 (1984) (sustaining enforcement of a subpoena of restaurant-motel's payroll and sales records and emphasizing that "[i]t is now settled that, when an administrative agency subpoenas *corporate books or records*, the Fourth Amendment requires that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome" (internal quotation omitted) (emphasis added)); SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) (rejecting a Fourth Amendment challenge to officials' failure to provide notice of a third-party subpoena to the target of an investigation, when the subpoena sought financial records in the hands of firms with whom target had engaged in transactions); Fisher v. United States, 425 U.S. 391, 401 n.7 (1976) (noting the absence of arguments of a Fourth Amendment nature in a case involving the subpoena of accountants' records from taxpayers' attorneys, and observing that "[s]pecial problems of privacy which might be presented by subpoena of a personal diary are not involved here" (citation omitted)).

179 United States v. Miller, 425 U.S. 435, 443 (1976).

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

181 *See supra* pp. 1401–02.

182 *See* Lopez v. United States, 373 U.S. 427, 439 (1963) (distinguishing cases requiring

not a party to the communications its subscribers send. Moreover, even in the government informant cases, the intended recipients of the communications—the would-be co-conspirators who were actually government agents—had an independent interest in the *contents* of the communications, and the speakers intended to convey the substance of the communications to the listeners. The same cannot be said for the involvement of a service provider in the transmission, receipt, or storage of a communication. The ultimate *recipient* of the communication, not the service provider, stands in the shoes of the government informants and agents in *Lopez*, *Hoffa*, *Osborn*, and *White*.

This point illustrates how a broad reading of *Miller* and its progeny, as holding that any reliance on a third party to retain a communication eliminates an expectation of privacy in the contents of the communication, is inconsistent with *Katz* itself. In *Katz*, the phone company necessarily carried the defendant's telephone call, and the phone company no doubt had the technical ability to hear the contents of that call. That technical ability, however, was no impediment to the Court's conclusion that Katz had an expectation of privacy in the conversation.[183] Moreover, *Katz*'s co-conspirator could have revealed the contents of the communication at any time to police. His mere ability to do so was not thought to eliminate Katz's expectation of privacy.[184] Similarly, with respect to Internet communications, neither the service provider's technical ability to gain access to the contents of a communication, nor the ability of the communication's recipient to reveal the contents of the communication, should, without more, eliminate a subscriber's expectation of privacy in communications stored with a service provider. Therefore, we should reject any broad reading of *Miller* and its progeny that would point to this conclusion.

The conclusion that users lack an expectation of privacy in communications merely because a third party holds them on the users' behalf is inconsistent with the doctrinal underpinnings of *Miller* and *Smith* (as well as with *Katz*). Moreover, we can draw on other, more closely analogous bodies of case law to resolve the problem of how to treat stored communications for Fourth Amendment purposes. First, cases involving personal property maintained on the premises of another indicate that the owner of the personal property retains an expectation of privacy in it, so long as the property is secured against others' access and the owner of the premises has only a limited right of access to the premises.[185] Second, when an individual contracts

---

judicial authorization for electronic surveillance on the ground that when a government agent was a party to the conversation, "[t]he Government did not use an electronic device to listen in on conversations it could not otherwise have heard"); *see also* United States v. White, 401 U.S. 745, 751 (1971); Osborn v. United States, 385 U.S. 323, 327 (1966); Hoffa v. United States, 385 U.S. 293, 302 (1966).

183 *See Katz*, 389 U.S. at 353.

184 *See id.*

185 *Compare* Stoner v. California, 376 U.S. 483, 489 (1964) (concluding that a search of a hotel room without a warrant violated the Fourth Amendment, despite the implied permission that one who engages a hotel room gives to personnel, such as maids, janitors, or repairmen, to enter to perform their duties), *and* Chapman v. United States, 365 U.S. 610, 616–18 (1961) (concluding that a search of a house occupied by a tenant violated the Fourth Amendment, despite the landlord's authority to enter the house for some purposes), *and* United States v. Johns, 851

for a third party to transmit or carry a communication or sealed package on his or her behalf, the individual does not lose his or her expectation of privacy in the communication or the contents of the package.[186] Analogously, as noted above, the telephone company's technical ability to gain access to the contents of a customer's communications does not mean that law enforcement officials can intercept those contents without judicial authorization; indeed, that is the premise of *Katz* and Title III.

Far from pointing to a blanket rule that one lacks an expectation of privacy in communications stored by a third party, these cases illustrate the factors that distinguish the use of a service provider to carry and store communications from the scenarios at issue in *Miller* and *Smith*. Whether one retains an expectation of privacy despite having conveyed some item to a third party depends upon the user's purpose in conveying the item to the third party; the relevance of what the item is to the third party's completion of the transaction; and the limitations (technical or legal) on the third party's ability to gain access to the item itself. One who maintains personal property on the premises of another for the purpose of storing the item—not for the third party to use the item—will not lose an expectation of privacy, as long as the third party's access to the item is limited and the item is secured against the access of others. Just as physical property, whether on rental premises, in a hotel, or in a storage facility, is "locked" against unwanted access, e-mail, segregated in an electronic mailbox and password protected, is likewise locked against unwanted access.

The most difficult aspect of assessing whether one retains an expectation of privacy in communications stored with a third party is what weight to give contractual terms—or, to sidestep the question of when such terms are enforceable, terms of service—allowing a service provider to gain access to the contents of communications for some purposes. Here, the case law is of limited assistance. On the one hand, cases dealing with maintenance of personal property in a hotel or storage facility suggest that an individual loses any expectation of privacy if the rental period expires or the individual storing the property fails to pay, thereby triggering the lessor's unfettered right of

---

F.2d 1131, 1133–35 (9th Cir. 1988) (implicitly recognizing a reasonable expectation of privacy in rented storage unit), *with* United States v. Rahme, 813 F.2d 31, 34 (2d Cir. 1987) (concluding that when a hotel guest failed to pay rent and the rental period had expired, the hotel could lawfully take possession of the items in the room and the guest had no reasonable expectation of privacy), *and* United States v. Poulsen, 41 F.3d 1330, 1336–37 (9th Cir. 1994) (reaching same conclusion where a defendant failed to pay rent on a storage unit and the manager therefore had unlimited access to the unit and the property stored therein).

186 *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable. Even when government agents may lawfully seize such a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package." (footnotes omitted)); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. 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.").

access.[187] On the other hand, one may retain an expectation of privacy against government inspection of the contents of a sealed package transported by common carrier,[188] even though nongovernmental carriers generally claim an unfettered right to inspect the packages they carry.[189] The first point suggests that by failing to adhere to contract terms, an individual can forfeit an expectation of privacy; the second point suggests that terms of service alone cannot defeat an expectation of privacy.

Of course, permitting the terms of service—in particular, the scope of the third party's right of access—to define the contours of an expectation of privacy in the carriage or storage of property or communications would create difficulties for law enforcement officials, who would be unable to anticipate those terms in every case. Perhaps more relevant than the terms of service themselves are the purposes that such terms implicitly serve. A provider's purpose will affect whether it is reasonable for the user to maintain an expectation of privacy in spite of those terms. In retaining a right to inspect packages, a carrier seeks to protect its property and its service, by ensuring that it does not transport items that are hazardous or likely to damage other goods.[190] Similarly, one who rents out a storage space might bar a renter from storing certain dangerous goods and might reserve a right of access to protect its property. Focusing on the purpose of retaining a right of inspection suggests a possible approach to dealing with storage of electronic communications. A provider that offers service to the general public most likely retains a right to inspect communications in order to protect its equipment and service. An employer that provides its employees with Internet and e-mail access may have the additional purpose of ensuring that employees are not misusing employer resources, transmitting trade secrets, or otherwise violating limitations on personal use. If a user knows that the employer not only has the right to monitor his or her communications, but also a broader purpose in doing so than to protect its system, the user has less reason to expect that his or her communications will remain private.[191]

As this discussion suggests, the argument that, under *Miller*, the mere fact that a subscriber places his or her communications with a third-party service provider eliminates any expectation of privacy in those communications is doctrinally and normatively unsound. Broad statements in *Miller* and *Smith* suggesting that one forfeits an expectation of privacy against government inspection merely by conveying an item to a third party arise from the

---

187 *Rahme*, 813 F.2d at 34; *Poulsen*, 41 F.3d at 1336–37.

188 *See* cases cited *supra* note 186.

189 *See, e.g.*, FedEx, FedEx Express Terms and Conditions, *at* http://www.fedex.com/us/services/express/termsandconditions/us/inspection.html?link=4 (last visited July 3, 2004) ("We may, at our sole discretion, open and inspect any shipment without notice.").

190 *See, e.g., id.* (discussing transport of dangerous goods).

191 Against this approach of imputing a particular purpose to a provider's preservation of a right to inspect property or communications, one might argue that a provider need not (attempt to) retain such rights by contract, because the provider has a property right to protect its property and service. That argument, however, cuts in favor of, not against, the conclusion that one can reasonably expect privacy in property and communications in the hands of a third party, for it suggests that one's reasonable expectation of the circumstances in which a carrier or provider will inspect property or communications can be independent of terms of use.

Court's conflation of two different strands of case law. Neither line of cases points to the conclusion that subscribers always lack an expectation of privacy in communications held on their behalf by service providers, and the premises underlying such a conclusion are in any event inconsistent with *Katz*. Finally, case law that bears more directly on the status of communications held by a service provider—namely, cases addressing an expectation of privacy in property held by a carrier or lessor—suggests that merely placing an item with a third party does not eliminate an expectation of privacy.

In light of the different possible analogies that a court could use, it is perhaps unsurprising that current case law does not clearly resolve whether one retains an expectation of privacy in electronic communications stored on a service provider's system. Courts have held that a user retains no expectation of privacy in subscriber information supplied to a provider.[192] That holding is consistent with a narrow reading of *Miller* and *Smith*, for subscriber information is information necessary for the provider to engage in a variety of legitimate activities in the normal course of its operations, such as billing and routing communications. As for the contents of communications, courts have held that a user lacks any expectation in communications conveyed in public forums such as chat rooms, when one of the communications' recipients is a government informant.[193] That result, of course, is consistent with the line of cases including *Lopez*, *Hoffa*, *Osborn*, and *White*.[194] As for contents of communications segregated in private areas, one court has recognized an expectation of privacy in stored e-mail messages, when the service provider neither reads nor monitors such messages.[195] Other courts have rejected such claims where an employer acted as the service provider, imposed

---

192 *See, e.g.*, Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that users lack expectation of privacy in subscriber information communicated to bulletin board system operators); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (holding that defendant lacked expectation of privacy in subscriber information communicated to Internet service provider); United States v. Hambrick, 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999) (defendant had no expectation of privacy in name, address, credit card number, and telephone number because he knowingly revealed that information to service provider for use in its normal course of business), *aff'd*, No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. Aug. 3, 2000) (rejecting expectation of privacy in subscriber information, but stating in dicta that "under certain circumstances, a person may have an expectation of privacy in content information"); State v. Evers, 815 A.2d 432, 443 (N.J. 2003) (holding that defendant had no expectation of privacy in subscriber information communicated to America Online).

193 *See* United States v. Charbonneau, 979 F. Supp. 1177, 1184–85 (S.D. Ohio 1997) (holding that the defendant had no expectation of privacy in communications made in chat rooms where FBI agents were among recipients, nor in e-mails sent or forwarded to agents); *Evers*, 815 A.2d at 440 (no expectation of privacy in communications transmitted to fifty-one chat room recipients, one of whom was an undercover police officer); State v. Moller, No. 2001-CA-99, 2002 WL 628634, at *5 (Ohio Ct. App. Apr. 19, 2002) (defendant had no expectation of privacy in communications in chat room, where undercover officer posing as fourteen-year-old girl was among recipients); Commonwealth v. Proetto, 771 A.2d 823, 831, 832 (Pa. Super. Ct. 2001) (no expectation of privacy in communications forwarded to law enforcement officials by recipient or made directly to law enforcement agent posing as fifteen-year-old girl), *aff'd*, 837 A.2d 1163 (Pa. 2003).

194 *See supra* notes 143–57 and accompanying text.

195 United States v. Maxwell, 45 M.J. 406, 412, 419 (C.A.A.F. 1996) (finding reasonable expectation of privacy in files held by AOL).

specific limitations on the system's use, and reserved the right to monitor the communications.[196] Although these cases provide limited guidance, they are not inconsistent with the approach I advocated above.

d. Legal Process for Material in the Hands of a Third Party

I argued above that *Miller* and like cases should not be read broadly as eliminating any expectation of privacy in communications held by a third party. *Miller*, of course, stands for the proposition that when no expectation of privacy exists, the government may use a properly drawn subpoena—one that is issued by an entity with appropriate legal authority, seeks relevant information, and is not unduly broad[197]—to compel production of documents. *Miller* does not, however, resolve the question of what legal process can be used to compel production of material in the hands of a third party when one retains an expectation of privacy in that material. Ordinarily, law enforcement officials cannot invade an expectation of privacy without a warrant. There are nevertheless a handful of cases that appear to sustain the government's use of subpoenas to compel the production of personal property in the hands of third parties, even when that property is protected by (or is assumed to be protected by) a reasonable expectation of privacy. The Department of Justice[198] and some commentators[199] rely on such cases to conclude that the Fourth Amendment offers only weak protection to the contents of electronic communications, and that a properly drawn subpoena is constitutionally sufficient to compel production of communications from a service provider. I argue here that the cases sustaining use of a subpoena where an expectation of privacy exists are not persuasive, and they do not

196 *See* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (holding that an employee had no expectation of privacy in copied files when government employer's Internet usage policy imposed limitations on system's use); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (holding that an employee had no expectation of privacy in e-mail messages when employer reserved right to monitor messages); United States v. Geter, No. NMCM 9901433, 2003 WL 21254249 (N-M. Ct. Crim. App. May 30, 2003) (holding that a government employee had no expectation of privacy in a government-operated e-mail system in which individual e-mail accounts were provided for official use only); *see also* United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (declining to resolve the question; suggesting in dictum that "it is less clear that an . . . expectation of privacy [in e-mail files] derives from the Constitution"). In arguably analogous contexts, courts have held that employees lack an expectation of privacy in files stored on their office computers, where employers warn employees about possible monitoring activities. *See, e.g.*, United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002); United States v. Bailey, 272 F. Supp. 2d 822, 835 (D. Neb. 2003); *see also* United States v. Butler, 151 F. Supp. 2d 82, 84–85 (D. Me. 2001) (no expectation of privacy in files stored on shared university computers); United States v. Bunnell, No. CRIM.02-13-B-S, 2002 WL 981457, at *5 (D. Me. May 10, 2002) (following *Butler*). Courts have also declined to find an expectation of privacy in such cases for purposes of state law privacy torts. *See* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002); Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *2 (D. Mass. May 7, 2002); Wasson v. Sonoma County Junior Coll., 4 F. Supp. 2d 893, 905–06 (N.D. Cal. 1997), *aff'd on other grounds*, 203 F.3d 659 (9th Cir. 2000).

197 *See supra* text accompanying note 132.

198 *See* CCIPS MANUAL, *supra* note 173, § III.A & n.14.

199 *See, e.g.*, Brief of Professor Orin S. Kerr in Support of Appellant at 17–19, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), 2000 WL 33986512; Kerr, *A User's Guide to the Stored Communications Act*, *supra* note 173, at 1211–12.

call into question the conclusion that law enforcement officials must ordinarily use a warrant to compel production of communications in which one has an expectation of privacy.

The argument that officials can use a subpoena to compel production of information in the hands of a third party even when an individual retains an expectation of privacy in that information may seem counterintuitive, because it cuts against the body of case law dealing with subpoenas. Courts addressing Fourth Amendment challenges to the use of a subpoena do so because the challenging party claims that use of the subpoena constitutes a search or seizure that is impermissible without a warrant. If a subpoena were sufficient legal process to compel production of items in the hands of a third party regardless of whether one has an expectation of privacy in the items, cases such as *Couch* and *Miller* need not have considered the expectation-of-privacy issue at all: the Court could simply have said that *assuming* an expectation of privacy exists, a subpoena is sufficient to overcome it. Even though the subpoena cases indeed suggest that the argument lacks merit, commentators rely on two cases that appear to allow officials to use a subpoena to compel production of property in which an individual is assumed or acknowledged to have an expectation of privacy. In *United States v. Palmer*,[200] the court of appeals held that the government did not violate the Fourth Amendment when, by subpoena, it compelled a defendant's attorney to produce property of the defendant in the attorney's possession.[201] The court explained that, even assuming that the defendant had a reasonable expectation of privacy in the property in his lawyer's possession, "a properly limited subpoena does not constitute an unreasonable search and seizure under the fourth amendment."[202] Similarly, in *United States v. Barr*,[203] a district court held that the government did not violate the Fourth Amendment when it compelled, by subpoena, a company that performed the service of receiving telephone messages and mail on behalf of the defendant to produce the defendant's mail.[204] "[A] subpoena which compels production of evidence," the court explained, "is generally not considered to be a 'seizure' within the meaning of the Constitution."[205]

Both of these cases suggest that use of a subpoena does not constitute a search or seizure. *Palmer* sustained use of a subpoena even on the explicit assumption that the defendant maintained an expectation of privacy in property in the hands of a third party.[206] *Barr* does not make this explicit assumption, but if my argument above that a user can maintain an expectation of privacy in communications held by a third party is correct, then Barr presumably would have had an expectation of privacy in the contents of the mail the answering service held on his behalf. A closer analysis of these cases, however, shows that they do not stand for the broad proposition that the govern-

200 United States v. Palmer, 536 F.2d 1278 (9th Cir. 1976).

201 *Id.* at 1282.

202 *Id.*

203 United States v. Barr, 605 F. Supp. 114 (S.D.N.Y. 1985).

204 *Id.* at 116.

205 *Id.*

206 *Palmer*, 536 F.2d at 1281–82.

ment can use a subpoena to compel production of materials in the hands of a third party even when the target of an investigation maintains an expectation of privacy in such materials.

In reaching the conclusion that a properly limited subpoena can overcome an expectation of privacy in property in a third party's possession, *Palmer* relied on cases rejecting Fourth Amendment objections to grand jury and administrative subpoenas.[207] The cases on which *Palmer* relied, however, dealt not with personal property or personal communications held by third parties for a limited purpose, but rather with corporate and other records necessary to carry out particular transactions or required to be retained by law.[208] In other words, the cases on which *Palmer* relied were the precursors to *Couch* and *Miller*, which clarified that there is no expectation of privacy in records of the sort at issue in those cases. Indeed, *Palmer* was decided within six weeks of *Miller* and did not cite that decision. Because *Palmer* relied exclusively on cases that the *Miller* Court clarified involved no expectation of privacy, we cannot place great weight on the *Palmer* court's conclusion that a subpoena can overcome a reasonable expectation of privacy.

In stating that a subpoena is not considered to effect a "seizure" within the meaning of the Fourth Amendment, the *Barr* court relied principally on the Supreme Court's decision in *United States v. Dionisio*.[209] In that case, the Court examined whether execution of a subpoena compelling individuals to appear before a grand jury and give voice exemplars violated the Fourth Amendment.[210] The Court considered the question in two distinct parts: whether the *order that the individuals appear* before the grand jury violated the Fourth Amendment;[211] and whether, once the individuals were lawfully before the grand jury, the further *direction to make voice recordings* violated the Fourth Amendment.[212] On the first question, the Court concluded that

---

207 *Id.* at 1282; *see* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208 (1946) (affirming courts' enforcement of administrative subpoenas compelling production of various corporate records and papers); United States v. Bausch & Lomb Optical Co., 321 U.S. 707, 727 (1944) (discussing cases upholding compelled production of corporate records); Hale v. Henkel, 201 U.S. 43, 77 (1906) (recognizing Fourth Amendment limitations on subpoenas, but rejecting the view that a subpoena can never compel documentary evidence).

208 In *Hale*, for example, the Court considered a Fourth Amendment challenge to a subpoena compelling production of various corporate documents. *Hale*, 201 U.S. at 74. In its Fourth Amendment discussion, the Court observed that "we are of the opinion that there is a clear distinction . . . between an individual and a corporation, and that the latter has no right to refuse to submit its books and papers for an examination at the suit of the state." *Id.* Though the Court acknowledged that a corporation is protected by the Fourth Amendment, the Court took the view that the corporation was entitled only to assert that the subpoena was unreasonably broad. *Id.* at 76. Similarly, in *Walling*, the Court considered whether a district court could enforce an administrative summons compelling production of business records. *Walling*, 327 U.S. at 189. The Court noted that "the records and papers sought are of a corporate character" and reasoned that, insofar as the case law applies "merely to the production of corporate records and papers . . . the Fourth [Amendment], if applicable, at the most guards against abuse only by way of too much indefiniteness or breadth." *Id.* at 208. The papers at issue in *Bausch & Lomb* were likewise corporate papers. *Bausch & Lomb*, 321 U.S. at 725 & n.6.

209 United States v. Dionisio, 410 U.S. 1 (1973); *see Barr*, 605 F. Supp. at 116.

210 *Dionisio*, 410 U.S. at 3.

211 *Id.* at 9–10.

212 *Id.* at 13–15.

the subpoena to appear before the grand jury did not amount to a "seizure," because it involved neither the threat of force nor the social stigma that typically accompany an arrest.[213] Having held that the individuals were properly before the grand jury, the Court then considered whether they were properly required to provide voice exemplars. On this point, the Court reasoned that the requirement to make voice recordings infringed no expectation of privacy since the Fourth Amendment provides no protection for physical characteristics, such as the sound of one's voice, that an individual knowingly and necessarily exposes to the public.[214]

As this discussion reveals, the *Dionisio* Court's statement that a subpoena generally does not amount to a "seizure" dealt with an issue entirely irrelevant in *Barr*—the compulsion to physically appear before a grand jury. *Barr* was a third-party subpoena case; the only individual arguably compelled to appear before the grand jury in *Barr* was the defendant's mail processing company, which apparently did not contest the subpoena. Put another way, had the grand jury subpoenaed Barr *himself* to appear and produce various documents, the district court might properly have disposed of Barr's Fourth Amendment objection *to his appearance* by relying on the cited language in *Dionisio*. As the remainder of *Dionisio* makes clear, however, that an individual is properly before the grand jury does not resolve the question of what the grand jury may properly require the individual to provide. Interestingly, in *Barr*, the government in fact obtained a search warrant before examining the contents of Barr's mail.[215] Accordingly, the case cannot be read to stand for the proposition that a subpoena is sufficient to overcome an expectation of privacy simply because a third party holds the materials the government seeks.

In sum, *Palmer* and *Barr* are not persuasive authority on the question of how the government might compel production of communications in the hands of a third party. They do not cast doubt upon the conclusion that, if an individual retains an expectation of privacy in communications in the hands of a service provider, law enforcement officials generally must present a warrant to gain access to such communications.

e. Conclusion

As the discussion above shows, the question of what constitutional framework governs access to stored communications is extremely complex. Broad language in *Miller* and *Smith* could be taken to suggest that a subscriber lacks an expectation of privacy in communications a service provider stores on his or her behalf, on the theory that one loses an expectation of privacy in any item conveyed to a third party. We should resist this reading of *Miller* and *Smith*, however, because it is fundamentally inconsistent with *Miller*'s doctrinal underpinnings, with *Katz*, and with case law in analogous areas. In the next section, I turn to the statutory framework governing access to stored communications. That statutory framework is also quite complex,

213 *Id.* at 10.

214 *Id.* at 14.

215 *See* United States v. Barr, 605 F. Supp. 114, 116 (S.D.N.Y. 1985).

and it appears to allow law enforcement officials to compel production of certain categories of communications without a search warrant.

2. The Statutory Framework

With the passage of ECPA, Congress provided a layer of statutory protection for stored communications. In keeping with the structure of Title III, these provisions, often referred to as the Stored Communications Act ("SCA"), not only prohibit all parties from gaining access to certain kinds of communications, but also identify a range of circumstances in which law enforcement officials are authorized to do so.[216] The legislative reports accompanying ECPA suggest conflicting views of whether subscribers retain an expectation of privacy in communications held by third-party service providers. For example, the report of the Senate Committee on the Judiciary relies on *Miller* to suggest that communications in the hands of a third party "may be subject to no constitutional privacy protection."[217] The report of the House Committee on the Judiciary, in contrast, states that "[i]t appears likely . . . that the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required."[218] As ultimately passed, the stored communications access provisions allow for compelled production of the contents of communications without a search warrant in some circumstances.[219] As I argued above, the view that a subscriber always lacks an expectation of privacy in the contents of communications held by a third party is erroneous. The significance of Congress's choice to allow compelled production of some communications without a search warrant depends on how one interprets several statutory categories the SCA creates. The prevailing view within the government is that the only communications to receive warrant protection under the SCA are "unopened" communications, held for 180 days or less.[220] I show that while that interpretation is plausible, and perhaps even the best interpretation of the statutory text, it illustrates that changes in how we communicate have placed a tremendous strain on the existing statutory categories. The current statutory framework reflects choices that are questionable as a constitutional matter and as a policy matter.

In the sections that follow, I describe the statute in extensive detail. I do so in part because the statute is complex and poorly understood. In addition, in light of the relationship between the SCA and Title III, the scope of the

---

216 18 U.S.C.A. §§ 2701–2709, 2711–2712 (West 2000 & Supp. 2003).

217 S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

218 H.R. REP. NO. 99-647, at 22 (1986); *see also id.* at 23 (suggesting that subscriber has limited rights in connection with subscriber or customer records maintained with services that process and store data, but that the contents of customer data enjoy a higher degree of Fourth Amendment protection).

219 *See* 18 U.S.C.A. § 2703(b) (West Supp. 2003); *see infra* notes 265–68 and accompanying text.

220 *See* CCIPS MANUAL, *supra* note 173, at 88–89 (explaining difference in statutory treatment of unopened and opened communications). That view is also reflected in Professor Kerr's contribution to this volume. *See* Kerr, *A User's Guide to the Stored Communications Act*, *supra* note 173, at 1216. Kerr was the principal author of the 2001 version of the CCIPS Manual, on which the cited 2002 version is largely based. *See* CCIPS MANUAL, *supra* note 173, at vi.

SCA takes on heightened importance. Recall that prospective surveillance under Title III is only appropriate when other investigative methods have been tried and have failed.[221] In other words, Title III essentially requires the "exhaustion" of other avenues of investigation before officials invoke its procedures. Because most electronic communications are stored in various places, the procedures of the SCA will be those of first resort, and the procedures of Title III those of last resort.

a. Statutory Terms

To understand the SCA, it is necessary to introduce three distinctions that determine its scope. The statute is based on the premise that individuals' stored communications will in many circumstances be held in the hands of a third-party service provider. The statute first divides providers who might store communications into two categories: those that offer an "electronic communication service"—that is, a service that "provides to users thereof the ability to send or receive wire or electronic communications"[222]—and those that offer a "remote computing service"—that is, "the provision to the public of computer storage or processing services by means of an electronic communications system."[223] As we will see, the level of protection certain communications receive under the statute depends on whether the provider holding them is a provider that offers the ability to send and receive communications or instead merely offers storage and processing services.[224] Second, the statute distinguishes between communications that are "in electronic storage" and those that are not. Not all communications that we might intuitively regard as "stored" are in fact "in electronic storage" for purposes of the statute, because electronic storage is narrowly defined. Electronic storage describes "any *temporary, intermediate* storage of a wire or electronic communication *incidental* to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of *backup protection* of such communication."[225] As I discuss below, what precisely "electronic storage" covers is a matter of dispute.[226] Because portions of the statute only protect communications that are in electronic storage, there are gaps in coverage for communications that a third party may "store," but that nevertheless are not "in electronic storage." Finally, the statute distinguishes between providers that offer services "to the public" and those that do not; some provisions grant greater protection to communications held by providers that offer services to the public.[227]

With that background, we can examine the statute's prohibitions and authorizations.

---

221 18 U.S.C. § 2518(3)(c) (2000).

222 *Id.* § 2510(15); *see* 18 U.S.C.A. § 2711(1) (West Supp. 2003) (cross-referencing definitions in § 2510).

223 18 U.S.C.A. § 2711(2) (West Supp. 2003).

224 *See infra* notes 238–58 and accompanying text.

225 18 U.S.C. § 2510(17) (emphasis added).

226 *See infra* notes 248–58 and accompanying text.

227 *See infra* text accompanying notes 272–75; *see also* 18 U.S.C. § 2702(a)(2) (prohibiting disclosure of communications held by provider of remote computing service to the public).

b. Substantive Prohibition

Section 2701(a) provides for criminal penalties[228] and civil damages[229] against one who:

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . .[230]

From the discussion of statutory terms, two limitations are evident. First, the provision applies to one who accesses a facility through which an *electronic communication service* is provided; it does not cover one who accesses a facility through which a *remote computing service* is provided. By definition, then, the substantive prohibition is limited to the facilities of an entity that provides users with the ability to send or receive wire or electronic communications. The provision would likely cover, for example, access to a telephone provider's voice mail system to retrieve a voice mail message, or access to an Internet service provider's system to retrieve an e-mail message from storage.

Second, the provision applies only to communications in *electronic storage*—that is, communications in temporary, intermediate storage incidental to their transmission, or communications in storage for purposes of backup protection.[231] As discussed below, the distinctions between an electronic communication service and a remote computing service, and between communications in electronic storage and communications not in electronic storage, are critical not only to the scope of the substantive provision, but also to the rules for government access.[232] Briefly, the prevailing interpretation of the term "electronic storage" within the Department of Justice, which both prosecutes violations of the statute and must obtain appropriate legal process for acquiring communications in connection with federal investigations, is that the term electronic storage refers to communications not yet retrieved by a subscriber, such as unopened e-mail and not-yet-accessed voice mail messages.[233] I evaluate that interpretation more fully below. For now, it is sufficient to note that the prevailing government interpretation dramatically narrows the scope of the SCA's substantive prohibition. Under that interpretation, § 2701(a) does not prohibit access to communications held by service providers unless those communications have not yet been accessed by the intended recipient.[234]

---

228 18 U.S.C. § 2701(b).

229 18 U.S.C.A. § 2707 (West 2000 & Supp. 2003).

230 18 U.S.C. § 2701(a).

231 *See supra* note 225 and accompanying text.

232 *See infra* notes 248–58 and accompanying text.

233 *See infra* notes 249–54 and accompanying text.

234 Of course, even with respect to communications accessed by the user and retained for further action, it is possible that other laws would bar access. *See supra* note 55.

The substantive prohibition of the SCA, like that of Title III, contains exceptions for conduct authorized by the service provider[235] and conduct authorized "by a user of that service with respect to a communication of or intended for that user."[236] In addition, the statute sets up procedures through which law enforcement officials can gain access to stored communications.[237] I explore those procedures in the next section.

c. Government Access

Section 2701(c) of the SCA exempts from the SCA's substantive prohibition both surveillance under § 2518 of Title III and actions taken under the SCA's government access provisions, set forth in § 2703. Until passage of the USA Patriot Act, these provisions applied only to electronic communications;[238] to acquire wire communications in electronic storage, law enforcement officials had to obtain a full Title III order.[239] The USA Patriot Act eliminated this requirement, and, at least until the sunset date, the statute's government access provisions apply both to electronic and to wire communications.[240] As with the substantive prohibition, application of the government access provisions of § 2703 turns on statutory distinctions between providers of electronic communication services and providers of remote computing services, and communications in electronic storage and communications that are not.

As relevant here, the statute distinguishes between three types of communications: (1) communications held "in electronic storage" with the provider of an "electronic communication service" for 180 days or less; (2) communications held "in electronic storage" with the provider of an "electronic communication service" for more than 180 days; and (3) communications held by a "remote computing service."[241] The SCA grants the most protection to communications in the first group.[242] Under § 2703(a) of the SCA, the government can compel production of such communications only by presenting a provider with a search warrant.[243] For communications in the remaining two categories, § 2703(b) provides the government with a number of options. The government can use a full search warrant and need not give notice to the subscriber if it does so.[244] Alternatively, if it provides notice to the subscriber, the government can compel a service provider to produce communications by presenting the provider with an administrative or grand jury subpoena, or by securing a court order under § 2703(d) of the statute.[245]

---

235 18 U.S.C. § 2701(c)(1).

236 *Id.* § 2701(c)(2).

237 18 U.S.C.A. § 2703 (West Supp. 2003).

238 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283. This provision is scheduled to expire in 2005. *Id.* § 224, 115 Stat. at 295.

239 *See supra* note 112 and accompanying text.

240 USA PATRIOT Act § 209, 115 Stat. at 283.

241 18 U.S.C.A. § 2703.

242 *Id.* § 2703(a).

243 *See id.*

244 *Id.* § 2703(b)(1)(A).

245 *See id.* § 2703(b)(1)(B).

A 2703(d) order is not equivalent to a search warrant: a court may issue a 2703(d) order if the government offers "specific and articulable facts showing reasonable grounds to believe" that the communications sought are "relevant" to an ongoing criminal investigation.[246]

To understand the significance of the different standards for these categories of communications, we must determine what the term "electronic storage" covers. As mentioned, the prevailing government interpretation, which I evaluate more fully below, is that only "unopened" communications are entitled to the full search warrant protection of § 2703(a); other communications are protected, if at all, only under § 2703(b). In examining the constitutional framework governing stored communications, I challenged the doctrinal and normative bases for the view that a subscriber cannot have an expectation of privacy in the contents of communications.[247] If my constitutional argument is correct, then the application of § 2703(b) to allow the government to compel production of electronic communications without a warrant will be unconstitutional in some circumstances. Even if my constitutional analysis is not correct, policy considerations counsel in favor of requiring a search warrant in a broader range of circumstances than the statute is currently understood to require. In either case, Congress should revise the SCA.

The Government's Interpretation of § 2703(a). Since § 2703(a) of the SCA affords search warrant protection only to communications in "electronic storage," we must determine what that term covers. Recall that the term "electronic storage" describes "any *temporary, intermediate* storage of a wire or electronic communication *incidental* to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of *backup protection* of such communication."[248] The first prong of the definition would clearly cover communications held by a service provider and not yet retrieved by a subscriber, such as an unopened e-mail or a new voice mail message. So long as a user has not yet retrieved a communication, its storage by the service provider is "temporary," "intermediate," and "incidental" to its transmission. The second prong of the definition would cover copies of unopened communications that the service provider retains in the event of a service disruption.

The difficulty is how to deal with a variety of other communications that a service provider holds on a user's behalf. For example, a voice mail subscriber might listen to a message and then instruct the service provider to save it. For e-mail, the circumstances under which the service provider continues to hold a message on a subscriber's behalf will depend on the options the service provider offers and the configuration of the user's e-mail client. The software that my university provides for sending and receiving e-mail, for example, has multiple configurations—one configuration that permits me, upon checking my account, to have copies of my e-mail "pushed" down from the mail server to my computer's hard drive (or a portion of the network

246 *Id.* § 2703(d).

247 *See supra* Part I.B.1.

248 18 U.S.C. § 2510(17) (2000) (emphasis added).

allocated to my use) and purged from the university's mail server; another configuration that allows me to maintain the e-mail in the mailboxes I have set up on the mail server; and another configuration that allows me to have copies of my e-mail pushed to my computer's hard drive or my network space but retained on the mail server for a specified time period, such as twenty days. Accordingly, depending on how I configure my mail client, the university's mail server may hold only those unopened messages that have not been "pushed" to my hard drive or network space, may hold those unopened messages plus all of the messages I have chosen not to delete from the server, or may hold all of unopened and opened the messages that are up to twenty days old. A similar range of options applies with respect to outgoing mail. Depending on how I configure my mail client, the mail server may or may not retain copies of my sent messages.

Which of the messages a service provider holds on a user's behalf fall within the SCA's definition of "electronic storage"? The prevailing government interpretation, as set forth in the Department of Justice's manual on searching and seizing electronic evidence, is that the term "electronic storage" covers only the unopened messages.[249] As I will show, the government's interpretation is a textually plausible one, offers a fairly clear rule for law enforcement officials to follow, and gives content to other portions of the SCA that would otherwise be outdated. The problem with the interpretation is that it requires drawing constitutionally questionable distinctions among classes of communications, and makes very little sense from a policy perspective.

With respect to the first prong of the electronic storage definition, the textual basis for the government's argument that only communications not yet retrieved by a subscriber are in electronic storage is that once a user retrieves a communication, the "transmission" of the communication to its addressee is complete, and any copy of the message then stored by the service provider is not for a "temporary" purpose associated with transmission.[250] Consider a voice mail message. If upon hearing a message a user decides to retain the message, the storage of the message is no longer "intermediate," because the communication has already reached the recipient. Nor is the storage "temporary," because the subscriber could retain the message indefinitely. Nor is the storage "incidental to transmission," because the transmission is complete. The handful of courts to have considered what electronic storage is have concluded that the first prong of the electronic storage definition covers only communications stored for a limited time in the middle of a transmission—"when an electronic communication service temporarily stores a communication while waiting to deliver it."[251]

---

249 *See* CCIPS MANUAL, *supra* note 173, at 88–89 (explaining difference in statutory treatment of unopened and opened communications).

250 *Id.*

251 *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001); *see also* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) ("Retrieval of a message from post-transmission storage is not covered by the Stored Communications Act. The Act provides protection only for messages while they are in the course of transmission."), *aff'd on other grounds*, 352 F.3d 107 (3d Cir. 2003).

The Justice Department's manual on searching and seizing electronic evidence does not address in any detail what the "backup protection" prong of the electronic surveillance definition covers, but the manual implicitly rejects the possibility that communications already retrieved by a user but still held by a service provider are in backup protection.[252] The SCA offers no guidance on what constitutes "backup protection." The Ninth Circuit, in construing the substantive prohibition of § 2701(a), has suggested that communications retrieved by a subscriber but not deleted from the service provider's system satisfy the "backup protection" prong of the definition,[253] and the United States Court of Appeals for the Third Circuit has left that possibility open.[254] The Ninth Circuit's interpretation of the statutory text, however, is awkward. The definition of electronic storage implies that, in a determination of whether a communication is in backup protection, the relevant perspective is that of the *service provider*, not the user. The provision covers storage *by* the electronic communication service *for purposes* of backup protection. Moreover, the term "backup" presupposes the creation of a second copy of a communication. A user who simply chooses not to delete a communication may wish to continue to store the communication, but he or she is not actually "backing up" the communication. To the extent that the Ninth Circuit's approach suggests that any communication a service provider holds on a user's behalf is in backup protection, then, it relies on a strained reading of the text.

The legislative reports accompanying the SCA are consistent with the government's narrow reading of "electronic storage." In discussing the substantive prohibition of § 2701(a), which, as mentioned, only covers communications in electronic storage,[255] the report of the House Committee on the Judiciary states:

> Section 2701(a) generally prohibits any person from intentionally accessing a wire or electronic communication system without authorization or in excess of authorization, and thereby obtaining access to a wire or electronic communication while it is in electronic storage in the system. An "electronic mail" service, which permits a sender to transmit a digital message to the service's facility, *where it is held in storage until the addressee requests it*, would be subject to Section 2701. A "voice mail" service operates in much the same way, except that the stored message takes the form of the sender's voice, usually in digital code. It would likewise be subject to Section 2701.[256]

The report's reference to an e-mail held in storage until its retrieval suggests that the Committee understood § 2701(a) to protect wire and electronic communications only *until the subscriber requests such communications*, be-

---

252 *See* CCIPS MANUAL, *supra* note 173, at 88–89 (emphasizing that "opened" communications are not included under § 2703(a) of the SCA).

253 Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004).

254 *Fraser*, 352 F.3d at 114.

255 *See* 18 U.S.C. § 2701(a) (2000).

256 H.R. REP. NO. 99-647, at 63 (1986) (emphasis added).

cause after that point such communications are no longer in "electronic storage." Extending the same reasoning to the government access provisions of § 2703 would mean that only communications not yet retrieved by a subscriber are in electronic storage. The report's discussion of § 2702(a)(2) reinforces this approach. That provision, which governs the circumstances under which a service provider can disclose communications, suggests that a communication's status under the statute changes once a user retrieves it. The report states that § 2702(a)(2), which prohibits voluntary disclosure of communications "carried or maintained" on a "remote computing service," applies to a communication that an addressee retrieves and subsequently stores: "Sometimes the addressee, having requested and received a message, chooses to *leave it in storage on the service for re-access at a later time.* The Committee intends that . . . such communication should continue to be covered *by section 2702(a)(2).*"[257] Of particular significance is that § 2702(a)(2) does not protect communications in electronic storage.[258] In other words, in stating that a communication retrieved by a user but left in storage is protected by § 2702(a)(2) against voluntary disclosure, the report implicitly suggests that such a communication is not in electronic storage—for if it were, § 2702(a)(1) would have covered it.

In sum, under the government's approach, only communications not yet retrieved by a subscriber are in "electronic storage" for purposes of the SCA. This interpretation is textually plausible, and perhaps stronger than that offered by the Ninth Circuit. But what are the consequences of such an interpretation? I have already noted one consequence: the interpretation severely curtails the protection of the substantive prohibition of § 2701(a). The interpretation also has significant constitutional and policy consequences for the SCA's government access provisions.

Consequences of the Government's Approach. In Part I.B.1, I argued that a blanket conclusion that one lacks an expectation of privacy in communications held by a third party is doctrinally and normatively problematic. If the Justice Department's interpretation of the term electronic storage is correct, however, only a narrow category of communications—a category including unopened e-mail or not-yet-accessed voice mail—is entitled to search warrant protection. The Justice Department's reading thus has significant constitutional and policy implications.

It should be noted that even for the communications the government agrees cannot be acquired without a search warrant—unopened communications 180 days old or less—the inclusion of a search warrant requirement does not eliminate all constitutional inquiry. It is not clear whether law enforcement officials presenting a warrant for the retrieval of communications from a service provider must provide notice to the subscriber, either as a statutory matter or as a constitutional matter. With respect to the statutory issue, portions of § 2703 specify when the government must provide notice that it has compelled production of documents and when such notice may be

257 *See id.* at 65.

258 *See* 18 U.S.C.A. § 2702(a)(2) (West Supp. 2003); *cf. id.* § 2702(a)(1).

withheld, but § 2703(a) is silent on the question.[259] The statute merely requires that the government follow "the procedures described in the Federal Rules of Criminal Procedure,"[260] which generally require notice to the person "from whom or from whose premises" property was taken.[261] The difficulty is that when officials compel production of information from a service provider, one could argue that the provider itself, and not the subscriber, is the searched entity. The Department of Justice has taken the position that the SCA does not require the government to notify a subscriber when it obtains information from a provider using a search warrant, but it bases that conclusion on a section of the SCA that does not apply to communications in electronic storage.[262] As for the constitutional question, as discussed in Part I.A.1, the lack of notice, or of a showing of exigency to justify the absence of notice, was among the constitutional deficiencies the Supreme Court identified in the New York statute at issue in *Berger v. New York*.[263] Although courts have sustained the failure to provide notice to a searched party in several contexts, they have done so in circumstances when notice would undermine the object of the search.[264] Section 2703(a) thus complies with constitutional requirements insofar as it mandates that law enforcement officials produce a search warrant to retrieve unopened communications, but the ambiguity in the statute regarding notice raises a constitutional question.

The constitutional questions are obviously more significant for communications that the government treats as being outside of § 2703(a)'s search warrant protection. Section 2703(b) establishes government access standards for communications that are held in electronic storage for more than 180 days,[265] and for communications that are held by the provider of a "remote computing service."[266] The government may, but need not, use a search warrant to compel production of such communications; with notice to a subscriber, a subpoena or § 2703(d) order will suffice. For the sake of discussion, we can assume that the statute treats all "opened" communications as communications held by a "remote computing service" and thus within the coverage of § 2703(b). (I show below, however, that the assumption that all such

---

259 *Compare id.* § 2703(a), *with id.* § 2703(b)(1)(A) (stating that notice to the subscriber is not required when law enforcement officials present a warrant).

260 *Id.* § 2703(a).

261 FED. R. CRIM. P. 41(f)(3) (requiring officer to give person "from whom or from whose premises the property was taken" a copy of the warrant and a receipt for the property taken).

262 *See* CCIPS MANUAL, *supra* note 173, § II.D.5 (relying on § 2703(b)(1)(A)).

263 *See supra* note 78 and accompanying text.

264 *See, e.g.*, Dalia v. United States, 441 U.S. 238, 247–48 (1979) (rejecting the claim that Title III violates the Fourth Amendment because it allows surveillance without prior notice); United States v. Donovan, 429 U.S. 413, 429 n.19 (1977) (holding that Title III's requirement of notice once surveillance operation is completed is a constitutionally adequate substitute for advance notice); Katz v. United States, 389 U.S. 347, 355 n.16 (1967) (noting that "officers need not announce their purposes before conducting an otherwise authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence").

265 *See* 18 U.S.C.A. § 2703(a) (West Supp. 2003) (making § 2703(b) applicable to communications held more than 180 days).

266 *Id.* § 2703(b).

communications are held by a remote computing service is clearly wrong in some cases and is questionable in others.)[267]

With respect to these two categories of communications, the statute's authorization of a subpoena or a 2703(d) order rather than a full search warrant necessarily reflects a premise that a subscriber retains no reasonable expectation of privacy in such communications. For unopened communications held for more than 180 days, the theory appears to be that such communications have been abandoned. For opened communications held by a service provider, the theory appears to be that one forfeits an expectation of privacy by maintaining communications with a third-party service provider. That approach, of course, is inconsistent with the Fourth Amendment analysis in Part I.B.1. As I argued there, a blanket conclusion that one lacks an expectation of privacy in communications held by a third party is doctrinally and normatively problematic. A more nuanced approach would distinguish between circumstances in which a service provider, such as an employer, reserves the right to monitor communications, not only to protect its system, but also to ensure that employees do not misuse their network access, and circumstances in which a provider does not do so.[268] If one has an expectation of privacy in communications held by a service provider, however, it is unclear why one should lose that expectation by virtue of choosing not to delete a communication. Insofar as the SCA allows officials to use a subpoena or a court order under § 2703(d) to gain access to communications that are held by a service provider but that are not in "electronic storage"—regardless of whether one might have an expectation of privacy in such communications—its application will be unconstitutional in some circumstances.

This point raises the question of whether courts could, consistent with the constitutional avoidance canon,[269] construe the definition of electronic storage more broadly, to include all e-mail held by service providers for 180 days or less, without regard for whether a subscriber has retrieved the e-mail. While treating all stored communications as being in "electronic storage" would resolve many of the problems the current statute raises, it would require rewriting, not merely construing, the statutory text. The constitutional avoidance canon allows a court to adopt one of two plausible alternative interpretations of a statute. Reading the term electronic storage to encompass all communications held indefinitely on a service provider's system, however, would make the "temporary, intermediate" and "incidental to transmission" requirements meaningless. In addition, the term "electronic storage" appears in multiple places in the statute, and in only one place does its scope raise potential constitutional issues. Courts applying the language outside of the context of the government access provisions would either have to adopt the broad definition of electronic storage, even though no constitutional question compelled that adoption, or accept that the term had different meanings in different portions of the statute. Finally, the avoidance canon is designed to give effect to congressional intent, based on the presumption that

267 *See infra* note 275 and accompanying text.

268 *See supra* note 191 and accompanying text.

269 *See, e.g.*, Jones v. United States, 526 U.S. 227, 239 (1999).

Congress would not intend to violate the Constitution. In the case of the SCA, however, adopting a broad interpretation of electronic storage would not amount to using the avoidance canon to choose one of two plausible interpretations of vague language where Congress did not consider the underlying constitutional question. Rather, adopting the broad interpretation would amount to correcting Congress's erroneous constitutional interpretation—that is, its apparent reliance on *Miller* to conclude that users always lack an expectation of privacy in communications held by third parties. In that sense, courts' use of the canon to arrive at a broad interpretation of electronic storage would not be consistent with Congress's intent. From a constitutional perspective, then, the current interpretation of "electronic storage" is problematic, but congressional action will be required to correct it.

Even setting these constitutional questions aside, as a policy matter an approach that permits only "unopened" messages transmitted to a subscriber to qualify for the highest level of protection under the statute is out of step with the way that many people use e-mail today. The choice to maintain a message in storage indefinitely with a provider need not reflect a conscious decision to transmit the message back to a service provider for further storage; the user simply "leaves" the message in a particular mailbox, perhaps planning to process or purge it later. If the reading of electronic storage proffered above is correct, however, then such "opened" e-mail messages become vulnerable not only to private acquisition, but to government acquisition with a mere subpoena. Similarly, a subscriber may opt to have the service provider retain copies of any sent messages. These sorts of copies are not likely to qualify as copies in "temporary, intermediate" storage, nor are they copies made by the service provider "for purposes of backup protection." Other architectural choices by providers or decisions by users may also have unexpected legal consequences under the regime. Recall the multiple options that my university's e-mail system offers: an option to keep messages on the server only until they are "pushed" onto my hard drive or network space; an option to keep all messages, unopened and opened, on the server indefinitely; and an option to have messages pushed to my hard drive or network space but to remain on the server for a specified time period. The last two options frequently prove more convenient, because they allow me to view my e-mail from my work, home, or notebook computers. If I were to choose the option to have copies of my e-mail pushed to my hard drive and purged from the server, my messages would not be held by a service provider, and law enforcement officials would need a warrant to search my computer to retrieve those messages. If I were to choose to maintain my e-mail on my service provider's server, however, the SCA would allow officials to subpoena the contents of any opened e-mail message.[270] In other words, under the government's approach, seemingly trivial choices by a subscriber among dif-

270 As I discuss below, this example is based on the assumption that an opened e-mail that one continues to maintain with a service provider is held by a "remote computing service." *See infra* notes 276–79 and accompanying text. In the university example, this is probably not the case, because a remote computing service by definition must provide services to the public. *See* 18 U.S.C.A. § 2711(2) (West Supp. 2003).

ferent technical options a service provider offers have tremendous legal consequences.

Finally, it is worth noting that the government's interpretation of "electronic storage" also drives a particular interpretation of the term "remote computing service." Although the interpretation has the benefit of making sense of portions of the statute that would otherwise be outdated, it is textually awkward and creates other anomalies. I assumed above that virtually all messages that a user "stores" but that are not technically held in "electronic storage" by the provider of an electronic communication service fall under § 2703(b), which permits access to such messages through a subpoena or court order, with notice to the subscriber.[271] As it turns out, § 2703(b) does not cover all messages stored with a service provider. First, § 2703(b) covers only messages held by the provider of a "remote computing service."[272] Recall the distinction between the provider of an "electronic communication service" and the provider of a "remote computing service": the former refers to "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[273] while the latter describes "the provision *to the public* of computer storage or processing services by means of an electronic communications system."[274] Under the remote computing service definition, only entities that provide services *to the public* qualify.[275] The term does not describe, for example, an employer whose system stores and processes e-mails for its employees, or a university that stores and processes e-mails on behalf of students. Thus, although the SCA requires law enforcement officials to present a warrant before compelling production of unopened e-mails stored by entities that offer services other than to the general public, because such providers are providers of an electronic communication service with respect to communications that are in "electronic storage," the statute is entirely silent on what process officials must use to compel production of communications that are neither in "electronic storage" nor held by a "remote computing service."

Even for providers that do offer services to the general public, the conclusion that opened e-mails no longer held in "electronic storage" are subject to § 2703(b) is questionable. That interpretation, again, requires treating a message that is not in electronic storage, but that is nevertheless maintained in storage by a service provider, as a communication held by a "remote computing service." To understand this approach, consider a communication received by AOL intended for one of its users. As long as the communication has not been retrieved by the user, AOL holds it in "electronic storage" and § 2703(a) applies. Once the user retrieves the communication, however, it is no longer in electronic storage; if the user does not delete the communica-

271 *Id.* § 2703(b).

272 *Id.*

273 18 U.S.C. § 2510(15) (2000).

274 18 U.S.C.A. § 2711(2) (West Supp. 2003) (emphasis added).

275 There is, however, an inconsistency in the statute on this point. Section 2711(2) defines a "remote computing service" as the provision of services to the public, but § 2702(a)(2) speaks redundantly of a person or entity "providing a remote computing service to the public." *Id.* §§ 2702(a)(2), 2711(2).

tion, AOL merely stores or maintains it on behalf of the user, and thus acts as a "remote computing service" with respect to that communication. AOL is the provider of an electronic communication service and the provider of a remote computing service at the same time, depending on the communication at issue.

The approach of treating opened e-mail communications as communications held by a remote computing service is the prevailing approach within the Justice Department,[276] but it is far from clearly correct. A passage quoted earlier from the report of the House Committee on the Judiciary does support this reading of the statute.[277] The passage deals with § 2702(a)(2) of the SCA, which limits the ability of a provider of a "remote computing service" to disclose communications held on its system.[278] The Committee stated that it intended communications that an addressee requests and receives, but chooses to "leave . . . in storage on the service for re-access at a later time" to be protected by § 2702(a)(2).[279] In other words, the Committee indicated that communications stored after a subscriber's access are communications held by a remote computing service.

The text of the statute, and other portions of the committee reports, however, suggest that Congress had something different in mind when it used the term "remote computing service." First, it is textually awkward that a user's failure to delete a communication converts a provider from an electronic communication service to a remote computing service with respect to that communication. Congress could have easily excluded communications held by an electronic communication service that are not in electronic storage from § 2703(a), much as it excluded those held in electronic storage for more than 180 days. Second, the reports accompanying ECPA suggest that Congress, in using the term remote computing service, mainly contemplated the circumstances in which a customer would outsource data processing and storage functions, not situations in which a subscriber to an electronic communication service would choose not to delete a communication. Consider the following passage in the report of the Senate Judiciary Committee on ECPA:

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data in-house on the user's own computer or on someone else's equipment. Over the years, remote computer [sic] service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement,

---

276 *See* CCIPS MANUAL, *supra* note 173, § III.B.

277 *See supra* note 257 and accompanying text.

278 18 U.S.C.A. § 2702(a)(2) (West Supp. 2003).

279 H.R. REP. NO. 99-647, at 65 (1986).

> or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer.[280]

The services described here are quite different from storage services in connection with e-mail transmissions.

As this discussion suggests, it is questionable that merely opening a communication shifts it from § 2703(a)—covering communications in electronic storage with the provider of an electronic communication service—to § 2703(b)—covering communications held or maintained by a remote computing service on a user's behalf. To the extent that the Justice Department embraces and applies this reading, however, this approach may be more privacy protective than other approaches. If opened communications are neither in electronic storage nor held or maintained by a remote computing service, then such communications—like opened communications held by an entity other than a public provider—fall entirely outside of the SCA. The Fourth Amendment would provide the sole limitation on officials' access to such communications. Without revisiting the earlier discussion of the applicability of the Fourth Amendment to stored communications, we can safely say that the scope of Fourth Amendment protection is unclear. Communications held by nonpublic providers, which are clearly outside of § 2703(b), are the least likely to involve an expectation of privacy.[281] A subpoena would likely be sufficient to compel production of the communications. A reasonable expectation of privacy may also be lacking for communications held by public providers where the provider retains a broad right to access the contents of communications.[282] Here, in other words, the Fourth Amendment rule would be close to the rule triggered by the Justice Department's interpretation of the SCA, in the sense that a subpoena would suffice to compel production of the communications.

For communications held by public providers where a user retains an expectation of privacy, however, the Justice Department's interpretation of § 2703(b)—treating opened communications as held or maintained by a remote computing service and thus subject to a subpoena or 2703(d) order—raises constitutional questions, because the Fourth Amendment would require a warrant.

3. Summary

As this discussion suggests, the extent to which the Fourth Amendment and the SCA protect stored communications is unclear. In light of the widespread use and storage of electronic communications, these constitutional and statutory questions have far greater urgency today than they did in 1976, when the Court decided *United States v. Miller*, or in 1986, when Congress, with an eye toward *Miller*, constructed multiple categories of communications and offered search warrant protection only to one category. Although many factors counsel against reading *Miller* broadly, the prevailing interpre-

---

280 S. REP. No. 99-541, at 10–11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564–65; *see also* H.R. REP. No. 99-647, at 23 (1986).

281 *See supra* text accompanying note 191.

282 *See supra* notes 187–91 and accompanying text.

tation of the SCA assumes that *Miller* supplies the appropriate constitutional framework. Under that reading, the SCA offers far less protection for electronic communications than we might expect. The narrow definition of "electronic storage" drastically limits both the communications covered by the prohibition on private acquisition and the communications given the most robust protection against government acquisition. Some communications—such as opened communications held by nonpublic providers—fall entirely outside of the SCA. The outdated "remote computing service" concept may or may not capture some communications that fall outside of the "electronic storage" category, but the protections offered against governmental acquisition are so low as to raise constitutional questions. Even if the SCA did not raise constitutional questions, however, it raises significant policy questions, in that it attaches tremendous legal significance to seemingly trivial choices about how to construct and use an e-mail system. I return to the weaknesses of the SCA in Part II, where I offer suggestions for reform.

C. *Gathering of Source and Destination Information*

Having discussed the constitutional and statutory frameworks governing the interception of communications in transit and the acquisition of communications in storage, I now turn to the third category of relevant electronic surveillance activities: the acquisition of source and destination information in connection with the transmission of a communication. For wire communications, such information would include the numbers associated with an outgoing or incoming call. As with the interception of the contents of wire communications, the constitutional rules here are relatively clear: there is no expectation of privacy in this information, and law enforcement officials therefore do not need a warrant to acquire it. In 1986, as part of ECPA, Congress added a layer of statutory protection for such information; to obtain the information, law enforcement officials must acquire a court order, although the standard for obtaining such an order is extremely low and the scope of a judge's review in granting the order is limited. For electronic communications, the constitutional and statutory questions are once again more complicated, because the acquisition of source and destination information concerning electronic communications reveals more about the contents of the communications than a phone number reveals about the contents of a telephone call. I discuss the constitutional and statutory issues in turn.

1. *The Constitutional Framework*

a. *Traditional Electronic Surveillance Techniques*

The Supreme Court addressed the application of the Fourth Amendment to the use of a device to extract the telephone number of an outgoing call in 1979 in *Smith v. Maryland*.[283] In that case, law enforcement officials had requested that a telephone company install a "pen register"—understood at the time of the case to mean a device that records the numbers dialed on a telephone by monitoring electrical impulses caused when the dial

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

is released—at its central office to record the numbers dialed from Smith's home telephone.[284] Smith was a suspect in a recent robbery, and the data the pen register gathered indicated that Smith was making phone calls to the robbery victim.[285] Officials used the information revealed by the pen register to request a search warrant for Smith's home.[286] Once indicted for robbery, Smith sought to suppress the evidentiary fruits derived from the use of the pen register on the ground that such use violated the Fourth Amendment.[287]

The Court concluded that use of the pen register did not constitute a "search" within the meaning of the Fourth Amendment.[288] Following the reasoning of Justice Harlan's concurrence in *Katz v. United States*, the *Smith* Court considered whether the defendant had an actual expectation of privacy that the telephone numbers he dialed would remain private, and whether that expectation was one that society was prepared to accept as reasonable.[289] The Court reasoned that it was unlikely that *Smith* had an actual expectation of privacy in the numbers he dialed: "Telephone users . . . 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."[290] In these circumstances, the Court concluded, "it is too much to believe" that telephone users harbor an actual, subjective expectation that the numbers they dial will remain secret.[291] Even assuming that Smith did harbor some subjective expectation that his phone numbers would remain private, however, the Court found that such an expectation is not one that society is prepared to recognize as "reasonable."[292] Drawing upon *United States v. Miller* and similar cases,[293] the Court reasoned that, by using his phone, Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[294] Although *Smith* involved only the use of a pen register to detect numbers dialed from Smith's phone, the same theory would presumably apply to the use of a "trap and trace" device to detect the source of an incoming call.

b. Electronic Communications

The question is how this principle—that acquisition of source or destination information concerning telephone calls is not a "search"—might apply

284 *Id.* at 736–37 & n.1.
285 *Id.* at 737.
286 *Id.*
287 *Id.*
288 *Id.* at 746.
289 *Id.* at 740.
290 *Id.* at 743.
291 *Id.*
292 *Id.*
293 *Id.* at 744 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)). I explained above how *Smith* compounds *Miller*'s error of conflating the business records and government informant cases. *See supra* notes 167–71 and accompanying text.
294 *Smith*, 442 U.S. at 744.

to information identifying the source or destination of an electronic communication. The *Smith* Court's theory in holding that the Fourth Amendment does not require law enforcement officials to obtain a warrant before installing a pen register was that the defendant necessarily conveyed the number he dialed to a third party to complete his call. By analogy, a user necessarily conveys some information in order to transmit or receive a communication. For an e-mail, of course, destination information is necessary for the communication to be routed properly. When a user seeks information from a particular web site, he or she must type the "address" of the page in order for his or her browser to contact the destination server to transmit the relevant file for display on the user's screen. The Court in *Smith* found it irrelevant that Smith's local call might have been completed through automatic processes; Smith was nevertheless deemed to have disclosed information, even if only to the phone company's computers.[295] A similar line of argument would suggest that even though the transmission of a communication or the request for a web page involves computer-to-computer contact, a user necessarily reveals the source or destination information.

The issue is more complicated than that, however. First, information that ostensibly identifies the location of the relevant file on a web server may embed certain clues as to content. Consider, for example, a user searching the Barnes & Noble web site for a book on breast cancer.[296] The address—known as the universal resource locator, or URL—of the page displaying the search results will likely contain the search terms, as in the example http://search.barnesandnoble.com/booksearch/results.asp?WRD=breast+cancer&userid=2TJNS0YMEW. Though the URL only represents the location on Barnes & Noble's server of a file generated in response to the search and containing the results of the search, it gives significant clues as to what that file contains. In contrast, a telephone number alone reveals little, if anything, about the content of a telephone conversation. Moreover, even when a URL reveals nothing at all about content, when a publicly available web site is involved, the address information is all that law enforcement officials need to determine what information a user has viewed. In other words, address information may not reveal content in the abstract, but in the case of a URL, it directs law enforcement officials to publicly available sites where that content can be found. The same cannot be said for the vast majority of telephone numbers; only when a telephone number connects one to a prerecorded message can a telephone number alone direct a law enforcement official to content.

Although the analogy between telephone numbers and the source or destination of an electronic communication works well for information necessary to route an e-mail, the analogy is imperfect when address information may reveal or direct law enforcement officials to content. With respect to such information, we must return to the analysis of *Katz* and cases following it, and ask whether a user has an actual expectation of privacy in the ad-

295 *Id.* at 744–45.

296 This example is drawn from PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 256 (2003).

dresses of sites the user views, and whether society is prepared to view that expectation as reasonable. We can assume that users expect privacy with respect to their Internet surfing activities. Determining whether society is prepared to accept that expectation as reasonable, however, raises some of the difficulties discussed in connection with the application of *Katz* to the acquisition of contents of communications.[297] Society's perceptions about the technical processes involved in the transmission of communications are difficult to measure and are shaped by a variety of inputs that may not reflect the truth of the matter. One factor, however, cuts against the conclusion that users retain an expectation of privacy in URLs: in various contexts URLs are passed to web servers other than the server providing the particular page the user views. For example, a web site may have an arrangement with a third-party advertiser for the advertiser to serve banner ads to the site; the user's browser will transmit the URL of the page the user is viewing to the advertiser's server.[298] Similarly, when a user transmits a request to view a particular web page, the server hosting that page typically can log the URL of the preceding page the user viewed.[299] In light of this exposure of URLs not only to the server holding the page the user requests, but also to other servers, it seems likely that a court would deem a user's expectation of privacy in URLs of the pages the user views to be unreasonable. If so, the sole protection against law enforcement officials' acquisition of such information is that provided by the statutory framework.

---

297 *See supra* Part I.A.1.b.

298 *See, e.g., In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502–06 (S.D.N.Y. 2001).

299 When a web browser contacts a server to retrieve a particular page, the browser conveys several pieces of information, such as the media types the browser will accept in response, the address to which the web server should respond, and information about the browser that sent the request. Among the pieces of information the browser conveys is the contents of the "Referer" variable—a variable the user's browser typically sets to contain the address of the previously accessed web page. *See* R. FIELDING ET AL., HYPERTEXT TRANSFER PROTOCOL—HTTP/1.1: REQUEST FOR COMMENTS 2616, § 14.36, at 140–41 (1999), *available at* http://www.ietf.org/rfc/rfc2616.txt (last visited July 18, 2004). ("Referer" is a misspelling of "Referrer." *See id.*) Referer variables are useful to web server owners, because they allow the server to identify pages with links to the server, to optimize caching, and to trace obsolete or mistyped links. The HTTP/1.1 standards recognize the privacy concerns involved when a browser conveys the address of the previously viewed site, and therefore recommend that a browser allow users to determine whether or not the browser transmits the contents of the Referer variable. *See id.* § 15.1.3, at 152 ("Because the source of a link might be private information or might reveal an otherwise private information source, it is strongly recommended that the user be able to select whether or not the Referer field is sent. For example, a browser client could have a toggle switch for browsing openly/anonymously, which would respectively enable/disable the sending of Referer and From information."). Most browsers, however, do not afford users this option. Browsers do sometimes control the sending of Referer information when there is a danger of passing secure information to a nonsecure server. For discussion of how Internet Explorer 4.0 and later versions work in this regard, see Microsoft, Microsoft Knowledge Base Article–178066, Info: Internet Explorer Does Not Send Referer Header in Unsecured Situations, *at* http://support.Microsoft.com/default.aspx?scid=KB;EN-US;Q178066& (last visited July 18, 2004).

2. *The Statutory Framework*

Following the *Smith* Court's conclusion that one lacks an expectation of privacy in telephone numbers dialed, Congress passed a statute providing minimal protection for such information. Although this statute was enacted as the third title of ECPA, the statutory language dealt more directly with wire communications than with electronic communications. As a result, its application to electronic communications proved controversial.

a. Traditional Electronic Surveillance Techniques

The third title of ECPA regulated the use of two kinds of devices: pen registers and trap and trace devices. As the Supreme Court explained in *Smith v. Maryland*, a pen register was understood at the time of that case to mean a device used to detect the number of an outgoing call; the device registered the impulses generated as the dial was released.[300] A trap and trace device was a device designed to detect the originating number of an incoming call.[301] Again following the pattern established in Title III, Congress outlawed the use of pen registers and trap and trace devices in the "pen/trap statute,"[302] subject to the standard exceptions for activities of a provider to maintain its service or for use with the consent of a party to the communication.[303] The most significant exception from the prohibitions of the pen/trap statute is for court-authorized surveillance. The court order provisions, however, differ significantly from those in other areas of surveillance law. Under the pen/trap statute, a government official need only certify that information likely to be obtained by use of a pen register or trap and trace device "is relevant to an ongoing criminal investigation."[304] Upon that certification, the court "*shall* enter an ex parte order."[305] In other words, the statute does not appear to require the judge to independently assess the factual predicate for the government's certification.

b. Electronic Communications

The pen/trap statute differed from Title III and the SCA in that its prohibition was written in terms of the use of particular devices rather than acquisition of particular information. Because the statute's prohibition was couched in terms of the use of pen registers and trap and trace devices, the applicability of the pen/trap statute to identifying information associated with electronic communications was unclear. In several ways, the statute seemed to focus exclusively on telephone numbers, pointing to the conclusion that the statute did not apply to identifying information associated with electronic communications. For example, the statute required the court order to specify the number of the "telephone line" to which the pen register or trap and

300 Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979).
301 *See* 18 U.S.C. § 3127(4) (2000).
302 *Id.* § 3121(a).
303 *Id.* § 3121(b).
304 *Id.* § 3122(b)(2).
305 18 U.S.C.A. § 3123(a)(1), (2) (West Supp. 2003) (emphasis added).

trace would be attached,[306] as well as the subscriber of that telephone line.[307] The statute also defined a pen register as a device that "records or decodes electronic or other impulses which identify the *numbers dialed* or otherwise transmitted on the telephone line to which such device is attached."[308] On the other hand, the statute defined a trap and trace device as a device to capture the "originating number" from which "a wire *or electronic* communication was transmitted,"[309] tending to suggest that the statute covered at least some identifying information in connection with electronic communications. It was thus unclear whether the statute limited the use of devices analogous to pen registers and trap and trace devices to obtain addressing information with respect to electronic communications, and whether law enforcement officials could invoke the statute's procedures to acquire origin and destination information concerning electronic communications.

As noted earlier in the constitutional discussion, as the Internet developed, the matter became more complicated because some addressing information—in particular, URLs associated with certain pages on a web server—might reveal content, or provide law enforcement officials with all the information they needed to discern that content.[310] For wire communications, the division between prospective access to content information, controlled by Title III, and prospective access to noncontent information, governed by the pen/trap statute, is relatively clear. Title III defines the contents of a communication as information "concerning the substance, purport, or meaning of the communication";[311] in the vast majority of cases, use of a pen register or a trap and trace device to obtain a phone number would reveal no content. As electronic communications developed, however, the narrow focus in the pen/trap statute on the two covered devices left law enforcement officials and the courts to wrestle with several possibilities. The first possibility was that the pen/trap statute neither prohibited nor authorized the acquisition of source or destination information associated with an electronic communication, and that the information was neither "content" for purposes of Title III nor subject to an expectation of privacy for purposes of the Fourth Amendment. Under this theory, acquisition of the information without legal process would not violate Title III or the Fourth Amendment. The second possibility was that the statute neither prohibited nor authorized acquisition of such information, but some of the information was properly treated as "content" in which one retained an expectation of privacy. Under this theory, law enforcement officials could not acquire the information without a Title III order. Finally, the third possibility was that the statute covered such information, and the information was neither content within the meaning of Title III nor subject to an expectation of privacy for purposes of the Fourth Amendment. Under this theory, although acquisition of the information would neither violate Title III nor be a search within the meaning of the

306 18 U.S.C. § 3123(b)(1)(C).

307 *Id.* § 3123(b)(1)(A).

308 *Id.* § 3127(3) (emphasis added).

309 *Id.* § 3127(4) (emphasis added).

310 *See supra* notes 296–99 and accompanying text.

311 18 U.S.C. § 2510(8) (2000).

Fourth Amendment, the statute required law enforcement officials to seek a court order to gain access to the information.

The Justice Department took the last position, and sought pen/trap orders authorizing the use of devices to extract information in connection with electronic communications.[312] Congress essentially codified this interpretation in the USA Patriot Act. The Act expanded the "pen register" and "trap and trace device" definitions to clarify that the terms cover not only dialing information, but also addressing information in connection with electronic communications.[313] As amended, the statute defines a "pen register" as a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted";[314] a "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication."[315] Each definition provides that the information retrieved by such devices "shall not include the contents of any communication."[316] This qualification was unnecessary, because any acquisition of the contents of a communication in transit would of course constitute an interception and could not proceed without a full Title III order.[317] The main difficulty with Congress's approach is that it resolves next to nothing about the status of URLs and similar information; it simply shifts to the courts the question of whether such information is "content" and thus warrants heightened statutory and constitutional protection.

D. Summary

As this discussion has shown, electronic surveillance law, and in particular surveillance law as it applies to communications over the Internet, is extraordinarily complex. It did not start out that way. In 1968, Congress followed a relatively clear road map offered by the Supreme Court to create a Fourth Amendment–compliant framework for court authorization of prospective electronic surveillance to acquire wire and oral communications. When the growing use of electronic communications prompted a broadening of the initial statutory framework, Congress declined to extend all of the statute's protections to electronic communications. Moreover, Congress adopted statutory protections for stored wire and electronic communications against a backdrop of Fourth Amendment uncertainty that still persists today. As I argued, the Fourth Amendment uncertainty stems in part from the Supreme Court's error in conflating two lines of Fourth Amendment case law. In adopting a statutory framework for stored communications, Congress

312 Kerr, *supra* note 4, at 633–34.

313 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288.

314 18 U.S.C.A. § 3127(3) (West Supp. 2003).

315 *Id.* § 3127(4).

316 *Id.* § 3127(3)–(4).

317 18 U.S.C. §§ 2511(1)(a), 2518(4) (2000).

erred in assuming that cases dealing with business documents held by a third party could readily be applied to circumstances involving personal communications temporarily stored by a service provider. As a result, the statutory provisions offer robust protection only to a relatively small subset of stored communications. Finally, although statutory protections granted to source and destination information in connection with telephone calls exceed Fourth Amendment requirements, the recent extension of those same protections to source and destination information in connection with electronic communications raises complicated constitutional issues.

In the next Part, I propose some important statutory changes to address inconsistencies and gaps in the current statutory framework. As I will argue, however, even those changes leave many difficulties of Internet surveillance law unresolved, and the pressures that electronic communications place on our surveillance framework are unlikely to subside. Accordingly, I draw upon Internet law scholarship in an attempt to bring an organizing normative structure to some of the policy dilemmas Congress faces in updating surveillance law.

II. Rethinking Internet Surveillance Law

With the constitutional and statutory frameworks for Internet surveillance in place, we can begin the task of rethinking surveillance law. I argued earlier that surveillance law is undertheorized. By that I meant not only that the law as it exists is poorly understood—by courts, litigants, and policy advocates—but also that scholars have directed insufficient attention to questions surrounding what this law ought to be.[318] A focus on constitutional issues at the expense of statutory ones and a starting premise that surveillance activities are largely illegitimate have limited the normative guidance provided to courts and particularly Congress in this area. Throughout Part I, I offered some guidance to courts concerning constitutional and statutory questions that have arisen with respect to the existing statutory framework. In this Part I seek to do three things: first, to identify short-term measures Congress could take to address the statutory ambiguities, gaps, and inconsistencies; second, to identify several sets of broader questions that Congress must consider in approaching any surveillance law reform; and third, to illustrate how Internet law scholarship can contribute to consideration of those questions.

A. Resolving Statutory Ambiguities, Gaps, and Inconsistencies

Part I catalogued several statutory problems that Congress could address in the short term, and I highlight some of the possible responses here.

1. Interception of Communications in Transit

Reconciling Title III's Treatment of Electronic Communications with Its Treatment of Wire and Oral Communications. Although application of Title III's general framework to electronic communications requires law enforcement officials to obtain a court order before extracting such communications,

318 For important exceptions, see *infra* note 344.

thus overcoming any Fourth Amendment concerns, there is no justification for providing less protection under Title III for electronic communications. Congress's restriction of the availability of Title III orders to a subset of federal crimes—albeit an ever-expanding subset—reflected its view that electronic surveillance techniques should be employed in limited circumstances. In functional terms, electronic communications have increasingly supplanted telephone communications, and reconciling the treatment of wire and oral communications with electronic communications would acknowledge that fact. Finally, a statutory suppression rule would both deter wrongful conduct by law enforcement officials and provide courts with a broader opportunity to interpret the statutes in cases involving governmental rather than private conduct.[319]

Clarifying the Relationship Between Title III and the SCA. Congress should also clarify the relationship between Title III and the SCA. Prior to the passage of the USA Patriot Act, there was confusion within the courts over which statute governed the acquisition of wire and electronic communications in storage.[320] If the USA Patriot Act's changes to Title III and the SCA—bringing wire communications in electronic storage within the ambit of the SCA and eliminating the requirement that law enforcement officials seek a Title III order to acquire these communications—are permitted to expire via sunset, confusion over the relationship between Title III and the SCA is likely to arise again. Although that confusion was initially confined to the wire communication context,[321] it carried over into the electronic communication context,[322] where it persists to some extent.[323]

The best way for Congress to approach this problem is to specify that the definition of "intercept" covers only acquisition of communications in transit. Acquisition of communications in transit raises fundamentally different questions from compulsion to a service provider to produce copies of communications from storage. Prospective surveillance is potentially invasive and can persist for an extended period of time without the subject's knowledge. Title III's heightened standards reflect that fact. Compulsion to a service provider

---

319 For a related argument with respect to the Stored Communications Act, see Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003).

320 *See supra* notes 20, 109–21 and accompanying text.

321 *See* United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

322 *See* Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1042 (9th Cir.), *withdrawn*, 262 F.3d 972 (9th Cir. 2001), *new opinion filed*, 302 F.3d 868, 874 (9th Cir. 2002).

323 *See Konop*, 302 F.3d at 891 (Reinhardt, J., dissenting). The original *Konop* decision and the *Konop* dissent on rehearing reflect overexpansive views of Title III at the expense of the SCA; on occasion courts adopt an overexpansive view of the SCA at the expense of Title III. The United States Court of Appeals for the First Circuit's recent decision in *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004), for example, interpreted Title III not to prohibit a service provider from capturing subscribers' communications with third parties contemporaneously with their transmission. The court reasoned that the communications were transmitted and stored simultaneously, and that they were therefore outside of the ambit of Title III. Since the communications were in fact captured contemporaneously with their transmission, Title III should have governed. As this Article went to press, the First Circuit voted to grant rehearing en banc in the *Councilman* case. United States v. Councilman, No. 03-1383, 2004 WL 2230823 (1st Cir. Oct. 5, 2004).

to produce the preexisting contents of a subscriber's mailbox is much more like a conventional search; as I will argue below, it is appropriate to require law enforcement officials to present a warrant to compel such communications, but the basis for applying Title III's detailed procedural requirements is weaker.

2. *Acquisition of Stored Communications*

Expanding the Scope of the SCA. With respect to stored communications, Congress should dramatically revise the current statute. First, the concept of a remote computing service is outdated. The Department of Justice has strained to give the phrase any content and currently appears to treat a remote computing service as an entity that holds wire or electronic communications already viewed by a subscriber, but maintained on the voice mail system or the e-mail server, as long as the entity provides services to the general public. Second, the definition of electronic storage is too narrow. The narrow definition guts the substantive prohibition and the government access provisions: only those communications not yet retrieved by a subscriber qualify as communications in electronic storage. Retrieval of an "opened" communication would not violate § 2701(a), and the government can compel production of such a communication based on a subpoena or a 2703(d) order. The government access provisions are to this extent constitutionally questionable. Congress should apply a uniform search warrant standard to all stored communications and should require notice of the search in most cases.

Adding a Suppression Remedy. Title III contains a suppression remedy for wire and oral communications obtained in violation of the statute. I argued above that the relevant provisions should be extended to cover wrongfully intercepted electronic communications as well, because such communications are not functionally different from wire and oral communications. Congress should also include a statutory suppression remedy in the SCA. A suppression remedy would deter abuses of the statute by law enforcement officials. In addition, because the SCA contains only criminal and civil remedies for violation of its provisions, cases addressing the SCA—and giving content to its terms—involve violation of the substantive prohibition of § 2701(a) by private parties, not violation of the government access provisions. A defendant could, of course, claim that law enforcement officials' use of a particular procedure to compel production of communications violated the Fourth Amendment. Such a claim, however, would do little to clarify the meaning of terms such as "electronic communication service," "remote computing service," and "electronic storage," because the claim would depend on the invasion of a reasonable expectation of privacy rather than a violation of the statutory terms.

3. *Gathering of Source and Destination Information*

Providing for Substantive Review of All Pen Register and Trap and Trace Device Applications. Congress should consider altering what is now a purely ministerial function of a court in approving a pen register or trap and trace order. The ostensible purpose of requiring a court to enter a pen register or

trap and trace order is to protect privacy, but the legitimacy of the process is threatened by the fact that the order must be entered upon the government's certification, creating the illusion of judicial scrutiny when in fact there is none. In connection with telephone calls, one clearly has no expectation of privacy in the information the government seeks. But if the privacy of the information is sufficiently important to require the government to articulate the basis for seeking it, it is sufficiently important to require a court's evaluation of the reasonableness of that basis.

Altering the Standard for Source and Destination Information in Connection with Electronic Communications. As discussed earlier, the interplay of the pen/trap statute and Title III with respect to addressing of Internet communications is complicated. The pen/trap statute defines the covered devices to include devices that detect addressing and routing information in connection with electronic communications, but provides that such information shall not include the contents of communications.[324] As I suggested earlier, this exclusion of contents was unnecessary, because Title III requires a full Title III order for interception of the contents of communications.[325] The exclusion of contents from the pen/trap statute does not necessarily resolve the problem with web communications. Even if a URL does not itself reveal anything about the contents of a page an individual views, and is thus not "information concerning the substance" of the page,[326] the URL is all that law enforcement officials need to gain access to the contents of the page.

Here, the problem is not necessarily a constitutional one, because, in light of the ways in which the URLs of the pages a user visits are exposed to other web servers, it seems unlikely that a court would hold that a user retains an expectation of privacy in such information. In other areas of the law, however, Congress has been sensitive to the problem of law enforcement officials gaining access to information that leads to the contents of what an individual views, and thus reveals the individual's thoughts or associations. For example, Congress has by statute limited governmental access to records indicating a cable subscriber's pay-per-view selection.[327] The Cable Communications Policy Act provides that a government official must obtain a court order to acquire cable records, by offering "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case."[328] It might be argued that a similar standard with respect to web-surfing activities would be inappropriate, because cable-viewing records are not exposed to third parties in the way that URLs are. Even if access to URLs that are not content, because by themselves they contain no information regarding the substance of a communication, does not need to be placed within Title III's framework, there is a strong argument that some standard over the current requirements for a pen register or trap and trace device should be adopted. For example, Congress could require officials to demon-

---

324 *See* 18 U.S.C.A. § 3127(3)–(4) (West Supp. 2003).

325 *See supra* text accompanying note 317.

326 18 U.S.C. § 2510(8) (2000).

327 *See* 47 U.S.C.A. § 551(h) (West 2000 & Supp. 2003).

328 *Id.* § 551(h)(1).

strate specific and articulable facts showing reasonable grounds to believe that the information is relevant to an ongoing investigation.[329]

B. Four Challenges of Internet Surveillance Law

The short-term measures discussed above are all necessary to close statutory gaps, resolve inconsistencies, and reconcile the statutory and constitutional frameworks for acquisition of electronic communications. But they are stop-gap measures, and they leave many difficulties of Internet surveillance law unresolved. In particular, the discussion brings to light four sets of overlapping questions that are likely to present challenges for Congress as it reconsiders the surveillance law framework, and that should be the focus of further scholarly discussion.

1. Technical/Architectural Questions

The first set of questions deals with the technical aspects of how communications are transmitted—or, put another way, the "architecture" of the network over which communications occur, and onto which a surveillance law regime must map. Even with respect to wire communications, network architecture has been a significant concern for Congress; the enactment of the Communications Assistance for Law Enforcement Act ("CALEA")[330] in 1994, for example, was designed to preserve surveillance capabilities that law enforcement officials feared would erode as the development of digital telephony altered the technical accessibility of communications lawfully authorized to be intercepted.[331]

The development of our current Internet surveillance law regime in fact reflects particular views about the architecture by which electronic communications are transmitted. Recall that with respect to prospective acquisition of the contents of communications during transmission, Congress simply extended much, but not all, of the existing regime covering wire and oral communications to electronic communications.[332] With respect to stored communications, Congress provided similar protection for wire and electronic communications, although it initially required a higher standard for government acquisition of wire communications.[333] For prospective acquisition of source and destination information in connection with communications in transit, Congress adopted a regime that initially covered wire communications, but was ambiguous with respect to electronic communications, and then explicitly brought electronic communications within the statutory ambit.[334] The picture that emerges is that wire communications are in some respects more deserving of protection than electronic communications,

---

329 *See* 18 U.S.C. § 2703(d) (2000) (setting out requirements for a court order under the SCA).

330 Communications Assistance for Law Enforcement Act (CALEA), Pub. L No. 103-414, 108 Stat. 4279 (1994).

331 *See infra* note 355 and accompanying text.

332 *See supra* notes 96–122 and accompanying text.

333 *See supra* notes 222–82 and accompanying text.

334 *See supra* notes 306–16 and accompanying text.

but that electronic communications are sufficiently similar to wire communications that it is appropriate to apply the same basic surveillance framework.

Congress's assumptions in this regard have become increasingly questionable over time. Taking stored wire and electronic communications as an example, the statutory alignment of the two kinds of communications fails to take into account that wire communications stored with a third party service provider constitute a relatively small fraction of wire communications, while a high percentage of electronic communications are stored with a third-party service provider, whether upon transmission or upon receipt. To the extent that the SCA exposes such communications to law enforcement officials on a lower standard than that required for most wire communications, it raises significant policy concerns. The assumption that electronic communications are sufficiently similar to wire communications to warrant application of the same statutory regime is one that must be reevaluated in connection with any Internet surveillance law reform.

These technical considerations are relevant not only across categories of communications, but also within those categories. I have already described how the configuration of an e-mail program can affect the accessibility of electronic communications to law enforcement officials. The difference between the transmission of ordinary e-mail communications and instant messaging provides another useful example. Instant messaging allows electronic communications to be transmitted through a peer-to-peer model; the direct connection between the sender and recipient may eliminate stored copies, and law enforcement officials will have fewer intermediaries from whom they can compel production of communications. To the extent that surveillance law treats these sorts of communications differently, it may drive subscriber choices about what services to use.

The technical aspects of how communications are transmitted raise other policy concerns as well. The trends toward convergence of voice and data transmission suggest that the architecture that currently applies to transmission of wire communications will become more like the architecture that currently applies to electronic communications. Quite apart from the difficult questions of statutory interpretation that will flow from this convergence, the resulting changes in the communications network can reduce the effective level of protection for wire communications. To the extent that our current surveillance law model was developed for the architecture that traditionally applied to wire communications, and was further extended to electronic communications—without reevaluating the differences in network architecture—the fact that wire communications will be carried in the same manner as electronic communications may be cause for concern.

2. *Substantive Questions*

The second set of questions that must be considered in connection with any Internet surveillance law reform relate to what substantive standards governing law enforcement access to communications would best balance the privacy and law enforcement interests at stake. Current Internet surveillance law consists of a hodgepodge of standards: Title III requires a heightened probable cause showing, coupled with a showing that other investigative

methods have failed or are too dangerous;[335] § 2703(a) of the SCA requires probable cause;[336] § 2703(d) of the SCA requires "specific and articulable facts showing reasonable grounds to believe" that the communications sought are "relevant" to an ongoing criminal investigation;[337] the pen/trap statute requires relevance to an ongoing criminal investigation;[338] and the subpoena provisions of § 2703(b) tie the standard to the specific authorizing statutes.[339]

The problem is that, save for those standards based on the Fourth Amendment's probable cause requirements, the substantive standards reflect a congressional view of the law enforcement and privacy interests at a particular moment in time. Even if law enforcement interests remain fairly constant, the competing privacy interests will change as the underlying technology changes, and as the functions communications serve change. In providing statutory protection for electronic communications, then, Congress has two choices: to set a standard that presumes Fourth Amendment protection for all communications, or to constantly reevaluate the law enforcement/privacy balance for particular categories of communications. Since enactment of ECPA in 1986, Congress has done neither.

3. Procedural Questions

The third set of questions that demand further consideration concern the procedural features of surveillance law that supplement the substantive standards. Part I's discussion of the legal framework revealed several difficult procedural questions; the answers to these questions can have important (constitutional and nonconstitutional) privacy implications. Should a suppression remedy apply for purely statutory surveillance law violations? Such a remedy applies with respect to the contents of wire communications acquired in transit, but not with respect to the contents of electronic communications acquired in transit, stored communications, or source and destination information. Second, when should the law require a judicial finding that a particular substantive standard has been met, and when is mere certification on the part of law enforcement officials sufficient? Third, when should the law require that law enforcement officials notify investigative targets that they have acquired communications or associated data? Title III requires after-the-fact notice (subject to certain exceptions).[340] The SCA is unclear as to law enforcement officials' obligations to notify subscribers in connection with the retrieval of some categories of stored communications, and notice is clearly not required as to other categories when law enforcement officials use certain kinds of legal process.[341] The pen/trap statute does not require notice.

---

335 18 U.S.C. § 2518(3) (2000).

336 18 U.S.C.A. § 2703(a) (West Supp. 2003).

337 *Id.* § 2703(d).

338 18 U.S.C. § 3122(b)(2).

339 18 U.S.C.A. § 2703(b)(1)(B)(i).

340 18 U.S.C. § 2518(8)(d).

341 *See* 18 U.S.C.A. § 2703(a)–(b); *see also supra* notes 259–62 and accompanying text.

Apart from the procedural features that emerged from the discussion in Part I, there are other procedural questions lurking. One that I return to below is the extent to which the various statutes permit cross-jurisdictional surveillance activities.[342]

4. Institutional Questions

The final set of questions that we must consider with respect to surveillance law reform are questions of institutional competence. If the primary task of a surveillance law framework is to moderate an appropriate balance between law enforcement interests and privacy interests, are the courts or is Congress in the best position to accomplish this task? The discussion in Part I of the interplay between the constitutional and statutory frameworks highlights some areas in which Congress has not adequately considered privacy issues. From that premise we might conclude that, at least with respect to constitutional considerations, courts are best able to apply Fourth Amendment principles to surveillance law, as the Supreme Court did in *Katz*. The issues are more complicated than that, however. Congress can act (and has acted) in various ways that make it less likely that courts will in fact resolve, or resolve appropriately, some of the critical constitutional surveillance law issues.[343] In approaching surveillance law reform, then, Congress must recognize its role as an important guarantor not only of law enforcement interests, but also of privacy interests.

C. Situating Surveillance Law Within Internet Law Scholarship

These challenges of Internet surveillance law—technical/architectural, substantive, procedural, and institutional—have not been adequately addressed in the scholarly literature. Surveillance law sits on the fringes of two areas of study. At least with respect to traditional surveillance techniques, it fits to some extent under the rubric of criminal procedure. In light of the highly technical nature of the statutory framework, however, mainstream criminal procedure courses typically give minimal attention to it. Moreover, viewing Internet surveillance law through the lens of criminal procedure can lead us to assume that surveillance of electronic communications is simply a natural outgrowth of surveillance of wire communications and that the same framework should apply. Just as Internet surveillance law is not viewed as being within the mainstream of criminal procedure, it is rarely given significant treatment within "Internet law" or "cyberlaw" courses. Internet law scholarship deals far more with copyright, trademark, and free speech issues than with surveillance issues. The marginalization of Internet surveillance law[344] is unfortunate, because Internet-related legal scholarship can illumi-

342 *See infra* notes 368–408 and accompanying text.

343 *See infra* p. 1447.

344 My point is not that important works on Internet surveillance law do not exist. Major contributors to the field include Jim Dempsey, Susan Freiwald, Orin Kerr, Raymond Ku, Tracey Maclin, Deirdre Mulligan, Paul Schwartz, Daniel Solove, and Peter Swire, among others. *See, e.g.*, James X. Dempsey and Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459 (2004); Freiwald, *supra* note 71; Kerr, *A User's Guide to the Stored Communications Act*, *supra* note 173; Kerr, *supra* note 4; Kerr, *supra* note 319; Ku, *supra* note 15;

nate some of the policy dilemmas that Congress faces in updating the statutory framework. At the same time, drawing Internet surveillance issues into Internet law scholarship can add a new dimension to that scholarship.

Attempting to bring Internet law scholarship to bear on surveillance issues necessarily conjures up questions about whether it is appropriate to view cyberlaw as a distinct field of study.[345] My bias on that point is clear,[346] but I hope to sidestep the debate. One need not view Internet law as a distinct field of study to recognize the richness of the developing theoretical literature on Internet issues. I focus on three (necessarily overlapping) themes within that literature: first, the importance of network architecture in supplementing or supplanting law as the primary force in regulating Internet activities; second, the pressures that the Internet places on a legal framework that presupposes regulation and enforcement by a geographically based sovereign; and third, the role of intermediaries, such as service providers, as points of "control" upon which states can act to secure certain policy outcomes.

My focus on the literature reflecting these themes may seem odd, because that literature is often concerned with one central question that is only tangential to my inquiry. In particular, most of the scholarship is concerned with the appropriate role of the state in regulating Internet activities. Scholarship addressing the relationship between geography and sovereignty examines whether state attempts to regulate Internet activities are unworkable or illegitimate because the Internet severs the link between the geographic location where acts occur and the geographic location where the acts' effects are felt. Scholarship addressing the relationship between law and technology suggests, in part, that governments can achieve some of their objectives by hard-wiring policy choices into the network architecture (or backing with the force of law the choices that private parties embed in digital content) rather than relying on enforcement of legal prohibitions.[347] Similarly, scholars addressing the role of service providers in the regulatory mix suggest that states can achieve regulatory outcomes by imposing substantive obligations or liability on service providers.[348]

Internet surveillance law is not concerned with government power to regulate Internet activities, except to the extent that it presupposes state power to protect the privacy of Internet communications. A link to these

---

Maclin, *supra* note 15; Mulligan, *supra* note 16; Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 751 (2003); Solove, *supra* note 173; Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264 (2004); Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV. (forthcoming 2004). My point, rather, is that surveillance issues are often overlooked in the broader context of *Internet law* scholarship, despite the contributions that such scholarship could make to understanding and resolving some of the dilemmas surveillance issues present.

345 *See, e.g.*, Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 206 (arguing that Internet law is not a distinct field of study); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (arguing that Internet law is a distinct field of study).

346 *See* BELLIA ET AL., *supra* note 296, at 12.

347 *See infra* note 350 and accompanying text.

348 *See infra* notes 409–13 and accompanying text.

bodies of literature is nevertheless instructive for several reasons. First, the architectural features that motivate concern about state regulation also motivate concern about surveillance capabilities. Second, although Internet surveillance law presupposes the power of the government to protect the privacy of Internet communications, the jurisdictional legitimacy questions involved with state regulation of Internet activities are similar to those involved with application of surveillance law, because the power to conduct a search and the procedural rules governing a search are typically tied to geography in the same way that (if not more so than) substantive regulation is.[349] Finally, just as service providers offer an attractive point for regulation, they also provide an attractive point for government extraction of communications.

1. Law, Technology, and Regulatory Outcomes

A significant body of Internet law scholarship addresses the relationship between law and technology. Two threads within that literature are particularly illuminating for Internet surveillance law. The first thread focuses on the government's difficulties in regulating Internet activities through standard mechanisms of passing and enforcing substantive prohibitions, and on how the government can, instead, work to alter the network architecture to reflect an underlying policy choice.[350] The second thread focuses on the bidirectional, destabilizing changes that technology can have on the outcomes the state seeks to legislate.[351] The first thread illuminates the technical/architectural challenges Congress faces in updating Internet surveillance law; the second thread illuminates the substantive and institutional questions.

In response to claims that states will have difficulty regulating Internet activities, some scholars argue that states in fact have a broad array of tools to achieve their regulatory objectives, and that a particularly attractive option with respect to the Internet will be for states to shape the network architecture to make regulation easier, and even to embed certain substantive policy choices into the architecture itself.[352] The development of the Platform on Internet Content Selection ("PICS"), although not government mandated, provides a useful example of how architectural changes can affect policy outcomes. PICS is simply a technical specification that facilitates filtering of Internet content along categories established by third parties and according to ratings supplied by any number of sources, including content providers themselves, companies that supply filtering software, and others. Such filtering is for some a particularly attractive alternative to direct regulation of sexually explicit content.[353] Though PICS is seemingly a neutral, technical solution—

---

349 For discussion of the international dimensions of this problem, see Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 47–57.

350 *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997).

351 *See generally* Yochai Benkler, *Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1238–49 (2000).

352 *See* Boyle, *supra* note 350, at 188.

353 Regulation of sexually explicit material is difficult because, even if one could settle in the abstract upon a constitutionally acceptable category of material that should be withheld from

it allows rating along any criterion and from any source—scholars have argued that the existence of this sort of technical specification will have the effect of curtailing some Internet content.[354] In other words, the fact that efforts to regulate sexually explicit content directly will encounter difficulties does not mean that Internet content will be unrestricted, because we will see a push toward solutions, such as PICS, that hard-wire policy choices into Internet architecture.

A surveillance-related example, although not directly concerning the Internet, provides a second illustration of this point. Law enforcement officials have traditionally conducted court-authorized surveillance of wire communications by attaching equipment to the "local loop"—the wires running from a telephone company's switching equipment to an individual subscriber's home. With the development of digital telephony, law enforcement officials claimed that they were unable to execute court-ordered wiretaps. In CALEA, Congress mandated that telecommunications carriers develop their systems in such a way as to facilitate surveillance both of the contents of telephone communications and of the dialing and signaling information associated with those communications.[355] Although CALEA does not directly expand the government's surveillance capabilities, in the sense that it does not affect the underlying legal authorities that authorize surveillance activities—Title III and the pen/trap statute—CALEA provides a ready example of the government's attempt to respond to the manner in which "digital technologies enlarge our space for living, both conceptually and practically," by demanding that surveillance "be hardwired into the 'technologies of freedom.'"[356] Similar dilemmas exist with respect to Internet communications, and although they have thus far been dealt with in different ways,[357] it is not

---

children, the geographic variation within the United States among standards for assessing such material, and the fact that so much covered material originates abroad, make efforts to regulate such material suspect as a constitutional and as a policy matter. These arguments were among the many leveled against the Communications Decency Act of 1996 (CDA), Pub. L. No. 104-104, 110 Stat. 133, and the Child Online Protection Act (COPA), Pub. L. No. 105-277, 112 Stat. 2681 (1998) (codified as 47 U.S.C. § 231 (2000)). *See* Reno v. ACLU, 521 U.S. 844, 874 (1997) (invalidating CDA on First Amendment overbreadth grounds); Ashcroft v. ACLU, 535 U.S. 564, 585 (2002) (rejecting facial challenge to COPA under First Amendment based on statute's contemporary "community standards" test for whether material is "harmful to minors"); ACLU v. Ashcroft, 322 F.3d 240, 266 (3d Cir. 2003) (invalidating COPA on overbreadth grounds on remand), *aff'd*, 124 S. Ct. 2783 (2004). For analogous challenges to state laws under First Amendment and dormant commerce clause theories, see Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168–83 (S.D.N.Y. 1997) (invalidating state regulation of sexually explicit communications).

354 Boyle, *supra* note 350, at 194 (noting that PICS' "technological goal—to facilitate third- and first-party rating and blocking of content—helps to weaken the Internet's supposed resistance to censorship at the same moment that it helps provide a filter for user-based selection").

355 47 U.S.C. § 1002(a)(1)–(2) (2000); *see* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996).

356 Boyle, *supra* note 350, at 204.

357 Consider, for example, the fact that law enforcement officials may have difficulty tracing the source of an electronic communication, because the relevant information will be held by different providers. The USA Patriot Act responded to this problem in part by allowing a single pen/trap order to be served on multiple providers. *See infra* notes 394–98 and accompanying text.

difficult to imagine the government seeking to preserve its surveillance capabilities by shaping the technical architecture of the Internet.

This attention to the interplay between law and architecture is largely lacking in discussions of Internet surveillance. I highlighted above several issues that warrant further consideration, including whether a legal regime developed for wire communications is appropriately applied to electronic communications; how, even within the category of electronic communications, technical features can drive policy outcomes; and how convergence of modes of voice and data transmission will map onto the existing surveillance law framework. To these we can add the more general concern that seemingly neutral, technical choices about network architecture can have significant consequences for surveillance law, insofar as they may increase or reduce the accessibility of communications to law enforcement officials.

The CALEA example highlights a second point about the relationship between law and technology that bears on the substantive and institutional considerations relevant to any surveillance law update: technology can have a bidirectional, destabilizing effect on the protection of rights that the law aims to achieve. The Fourth Amendment provides a degree of protection for the privacy of communications. But the Fourth Amendment's *legal* protection of privacy is not the sole determinant of the privacy one receives against surveillance. Technology destabilizes that protection in two ways. As the digital telephony example shows, technological developments can expand privacy by making communications technically inaccessible to law enforcement. More generally, digital technology increases the likelihood that communications will extend beyond the jurisdictional reach of law enforcement officials.[358] Encryption provides another useful example; to the extent that it makes surveillance technically more difficult, even when that surveillance is lawful, it provides a layer of technical protection over and above the constitutional and statutory protection. At the same time, technological developments can enhance surveillance capabilities. That trend is most easily observed with the use of sense-enhancing devices, such as thermal imaging devices and concealed weapons detection technology.[359] With respect to Internet communications, the development of tools such as Carnivore—a tool the FBI developed to overcome difficulties service providers had in isolating and delivering the contents of electronic communications or addressing or routing information in response to court orders—can have a destabilizing effect.[360] Similarly, because electronic communications must pass through various points of the network and copies of electronic communications are retained

358 *See* Bellia, *supra* note 349, at 55–57; *infra* notes 371–408 and accompanying text.

359 *See* Kyllo v. United States, 533 U.S. 27, 36 & n.3 (2001) (discussing sense-enhancing technologies).

360 Carnivore, renamed DCS1000 in the wake of controversy over its development and use, was designed to assist the government in intercepting and collecting communications and addressing information that "are the subject of a lawful order." *Internet and Data Interception Capabilities Developed by the FBI, Before the Subcomm. on the Constitution, House Comm. on the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Dir., Lab. Div., FBI), *available at* http://www.fbi.gov/congress/congress00/kerr072400.htm. For a brief discussion of the constitutional, statutory, and prudential concerns about use of the device, see BELLIA ET AL., *supra* note 296, at 263–65.

for a variety of legitimate reasons, more communications can be exposed to surveillance.

The destabilization raises both substantive and institutional issues. Substantively, what should we make of the fact that technology, and not merely law, determines the level of privacy that we enjoy with respect to our communications? When technology threatens law enforcement capabilities, as in the case of encryption, the government has taken the controversial position that the law must right the balance—that the Fourth Amendment provides a certain level of privacy protection, and that the law must overcome technical limitations on authorized access to communications. When advancements in surveillance threaten privacy, the question is whether the Fourth Amendment is the appropriate moderating force.

This theme of technology destabilizing legal protections emerges in Internet law scholarship primarily in connection with copyright law.[361] The federal copyright regime grants protection to the author of an original work in the form of certain exclusive rights.[362] At the same time, copyright law reserves certain rights to the public, including the right to make fair use of the copyrighted work[363] during the copyright term and the right to use the work once it passes into the public domain. Technology and its limitations profoundly affect the balance of the authorial and public use rights. To the extent that copies are not exact or are costly to distribute, a copyright holder receives an additional layer of protection. At the same time, the fact that it is difficult for a copyright owner to discover infringing acts and to identify and pursue individual infringers gives additional space to the public's rights.[364]

Digital technology destabilizes this regime in two directions. First, digital copies are perfect copies. Those who distribute such copies via the Internet do not bear the costs of distributing them. At the same time, digital technology gives a copyright holder a greater ability to control the uses to which his or her work will be put.[365] To the extent that a copyright holder can embed limitations into the code of a digital work on the manner in which the work can be used, the copyright holder can appropriate rights beyond those that copyright law grants (for example, by blocking uses that the law would treat as fair).

Though the merits of Congress's responses to the destabilization of copyright law are certainly debatable, the point is that the destabilization and the appropriate response, from a policy perspective, have been extensively explored within the Internet law literature—where scholars have examined whether the pre- and postdigital statutory regimes strike an appropriate balance between the rights of copyright holders and the rights of the public. The trends of destabilization with respect to government surveillance have not

---

361 *See* Benkler, *supra* note 351, at 1242–43.

362 17 U.S.C § 106 (2000).

363 *Id.* § 107.

364 LESSIG, *supra* note 350, at 125.

365 *Id.* at 127–30. For opposing perspectives on this trend, compare Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41 (2001), with Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998).

been a major focus of scholarship, despite significant parallels with copyright law. There are differences in the copyright and surveillance examples, especially since copyright law is largely viewed as statutory law[366] and surveillance law has constitutional and statutory components. A broader focus within Internet law scholarship on the role of the Internet in the destabilization of Fourth Amendment protection would nevertheless be useful. Is the Fourth Amendment the appropriate mechanism for moderating the balance between law and technology in protecting privacy rights while preserving government surveillance capabilities? Or must statutory law fill the gap? These questions, of course, raise an institutional concern: whether Congress or the courts are in a better position to strike the appropriate balance.

The discussion in Part I of this Article might suggest a preference for accommodation of the competing privacy and law enforcement interests in the courts; I argued that with respect to stored communications, the statutory framework has not been, but should be, tested against the Fourth Amendment.[367] The evolution of Internet surveillance law, however, shows the difficulty in relying on the Fourth Amendment as the main mechanism to moderate the balance between privacy and law enforcement interests. Courts obviously *can* deal with the constitutional dimension of Internet surveillance law, but Congress has already made choices that affect the likelihood of courts doing so in any effective way.

First, existing statutory protections may have the effect of "freezing" the application of the Fourth Amendment to surveillance issues. As discussed earlier, Congress sought to meet the Supreme Court's objection to the New York permissive eavesdropping statute at issue in *Berger* through Title III, which responded to the conclusion in *Berger* and *Katz* that eavesdropping constitutes a search within the meaning of the Fourth Amendment. The extension of Title III's framework to electronic communications largely pretermits any resolution in the courts of whether an expectation of privacy in electronic communications is reasonable. Second, Congress's passage of a layer of statutory protection is a crucial data point in constitutional interpretation. The notion that law enforcement officials can compel production of messages held by a third party without meeting Fourth Amendment requirements, for example, has gone largely unchallenged; and the fact that Congress has legislated on that premise has no doubt reinforced the perception that such techniques are permissible. In other words, even if courts *should*

366 There is, however, a growing body of scholarship on the relationship between copyright law and the First Amendment, and on the limitations the Copyright Clause imposes on Congress's power. *See, e.g.*, Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354 (1999); Paul J. Heald & Suzanna Sherry, *Implied Limits on the Legislative Power: The Intellectual Property Clause as an Absolute Constraint on Congress*, 2000 U. ILL. L. REV. 1119 (2000); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147 (1998); Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1 (2001); William Patry, *The Enumerated Powers Doctrine and Intellectual Property: An Imminent Constitutional Collision*, 67 GEO. WASH. L. REV. 359 (1999); Diane Leenheer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665 (1992).

367 *See supra* Part I.B.1.

have the primary responsibility for moderating the balance between law enforcement and privacy interests, congressional action can affect their ability to exercise that responsibility effectively. The perception that courts have that role, however, can prompt Congress to overvalue law enforcement interests, on the theory that the Fourth Amendment provides courts a mechanism for checking the weight Congress gives to privacy interests. Law enforcement interests will be overvalued if Congress perceives its role to be to empower law enforcement under the assumption that courts can function as a backstop on the privacy issues, because Congress's actions can have the practical effect of limiting dialogue within the courts on these issues.

These observations are necessarily preliminary. My point is that the existing Internet law literature offers some insights into the technical/architectural, substantive, and institutional questions that surveillance law raises, and that analysis of these issues could benefit from a further integration of surveillance law into Internet law scholarship.

2. *Surveillance and Geography*

A second major theme within the Internet law literature explores the pressures that the Internet places upon a legal framework that presupposes regulation by a geographically based sovereign. The degree to which the Internet challenges notions of territorial sovereignty has been the subject of an extensive theoretical debate,[368] and the issues play out in a variety of doctrinal categories.[369]

We might assume that this debate has little to tell us about a federal surveillance regime, particularly those portions of it that are designed to acknowledge and protect a "reasonable expectation of privacy"—or, more precisely, a subjective expectation of privacy that "society" is prepared to accept as reasonable. Put another way, because the Fourth Amendment, as interpreted by the Supreme Court, calls upon courts to weigh a concept of privacy that is U.S.-specific but that seems, within the United States, to be independent of geography, and because Congress can set a floor for privacy standards nationwide,[370] we might not see the fact that Internet communications

368 A series of pieces by David Post and Jack Goldsmith mark the poles of the debate. *Compare* David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155 (1996), *and* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996), *and* David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent": Towards A New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055 (1998), *with* Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119 (1998), *and* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998) [hereinafter Goldsmith, *Territorial Sovereignty*], *and* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998), *and* Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135 (2000). For Post's response to Goldsmith and others, see David G. Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365 (2002).

369 *See* Paul Schiff Berman, *The Globalization of Jurisdiction*, 157 U. PA. L. REV. 311 (2002).

370 Such legislation would of course have to fit within one of Congress's enumerated powers. The Commerce Clause provides an appropriate basis for Congress's enactment of laws regulating the privacy of wire and electronic communications. For oral communications, which are far less likely to affect interstate commerce, Congress attempted to shore up the constitutionality

cut across geographic boundaries as posing any significant challenges to the surveillance framework. As I will show, however, it is a mistake to approach any surveillance law reform without taking account of the problems of territorial sovereignty that communications cutting across geographic boundaries present. The challenges that the Internet creates for territorial sovereignty have already led to significant changes in our surveillance regime, and we are likely to see additional pressures in the future. Although the debates in the Internet law literature over state regulation do not take these surveillance-related dilemmas into account, bringing those debates to bear on surveillance issues highlights the importance of procedural aspects of the surveillance framework in supplementing the substantive standards. I do not claim that the Fourth Amendment itself dictates a particular congressional response to the challenges the Internet creates for territorial sovereignty as it bears upon surveillance issues, but I do argue that these pressures heighten the nonconstitutional privacy concerns the surveillance framework already raises.

Even before widespread use of electronic communications, transactions cutting across state (not to mention international) borders raised difficult interpretive questions for courts applying Title III. Section 2518(3) of the statute authorizes a district court judge to issue an order "authorizing or approving interception of . . . communications *within the territorial jurisdiction* of the court in which the judge is sitting."[371] Beginning in the early 1990s, courts wrestled with a series of cases in which law enforcement officials located in one jurisdiction would engage in surveillance of facilities located in another jurisdiction. Early cases involved use of a dedicated telephone line to carry communications from the targeted facility in one jurisdiction to a listening post in another jurisdiction.[372] Similar questions arise when law enforcement officials place electronic listening devices that transmit communications to a nearby location, from which they are further transmitted through a telephone line to investigators in another jurisdiction.[373] The advent of digital telephony makes the use of these techniques even more likely, as a telephone company can—and, indeed, is required by law to have the capability to—isolate the communications of a subject at its facilities and provide the communications to law enforcement officials.[374] To carry out surveillance activities in such cases, law enforcement officials do not need to attach any device to the facilities the investigation targets.

---

of Title III by defining an "oral communication" as a communication uttered by a person exhibiting a justifiable expectation that such communication is not subject to interception. 18 U.S.C. § 2510(2) (2000). For provisions regulating state governmental surveillance, the statute can be viewed as "enforcement" of the Fourth Amendment, as incorporated by the Fourteenth Amendment. The report of the Senate Committee on the Judiciary accompanying the bill contains a candid discussion of the potential constitutional problems with application of the statute to private conduct with respect to oral communications. *See* S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2180.

371 18 U.S.C. § 2518(3) (emphasis added).

372 *See, e.g.*, United States v. Rodriguez, 968 F.2d 130, 134 (2d Cir. 1992).

373 *See, e.g.*, United States v. Jackson, 207 F.3d 910, 914–15 (7th Cir. 2000).

374 *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 103, 108 Stat. 4279, 4280 (1994) (codified at 47 U.S.C. § 1002).

The statutory question for courts confronted with such cases was whether an "interception" occurred where the targeted facilities (from which the communications were redirected) were located, or where law enforcement officials first overheard the communications. If the interception occurred solely where the targeted facilities were located, then a judge in the territorial jurisdiction where the investigators were located would lack the authority to issue the order.[375] In *United States v. Rodriguez*,[376] the first appellate case to confront this issue directly,[377] the Second Circuit considered whether a judge in the Southern District of New York had authority to approve an interception of communications between co-conspirators in New Jersey, when the intercepted communications were carried from New Jersey by a dedicated telephone line to Drug Enforcement Agency agents in New York.[378] The court held that for purposes of Title III, an "interception" of a wire communication occurs both where a communication is redirected—in this case, at the targeted facilities in New Jersey—and where officials first hear the communications—in this case, at the DEA listening post in New York.[379] Other courts have followed this approach with respect to wire and oral communications.[380]

As the cases indicate, with respect to wire and oral communications, courts have rather smoothly accommodated the problems with cross-jurisdictional surveillance activities. Part of this accommodation, however, relies on the language of Title III's definition of "intercept," which refers to the "aural or other acquisition" of the contents of a communication. When a communication is redirected by a device in one jurisdiction, and first overheard in another, courts have deemed the redirection to constitute an initial "other acquisition," and the overhearing to constitute the "aural" acquisition.[381]

---

375 18 U.S.C § 2518(3).

376 *Rodriguez*, 968 F.2d 130.

377 Earlier cases included the district court decision in *United States v. Burford*, 755 F. Supp. 607, 609–11 (S.D.N.Y. 1991) (upholding a wiretap order issued in New York when device was attached to telephone in Maryland and communications were transmitted to New York), and a Court of Appeals decision presenting the converse factual scenario with respect to a state wiretap order, United States v. Nelson, 837 F.2d 1519, 1526–27 (11th Cir. 1988) (declining to suppress evidence when wiretap order was issued by state court judge for circuit in which targeted facilities were located, but communications were transmitted to listening post outside of judge's circuit).

378 *Rodriguez*, 968 F.2d at 135.

379 *Id.* at 136.

380 *See* United States v. Jackson, 207 F.3d 910, 914–15 (7th Cir. 2000) (denying motion to suppress evidence where judge in the Northern District of Illinois authorized use of electronic listening devices in prison in Southern District of Illinois, but conversations were relayed to officials in the Northern District); United States v. Denman, 100 F.3d 399, 402–04 (5th Cir. 1996) (denying motion to suppress wiretap evidence where judge in Eastern District of Texas issued order, where calls were monitored and recorded, but where tapped telephones were located in Southern District of Texas); United States v. Giampa, 904 F. Supp. 235, 278 (D.N.J. 1995) (denying motion to suppress wiretap evidence where order was issued in New Jersey and communications were relayed from New York to New Jersey); *see also* United States v. Tavarez, 40 F.3d 1136, 1138 (10th Cir. 1994) (following *Rodriguez* in a case involving the Oklahoma wiretap statute, when law enforcement officials targeted facilities in one county but listened to the conversations in another).

381 *Jackson*, 207 F.3d at 914; *Rodriguez*, 968 F.2d at 136; *Giampa*, 904 F. Supp. at 278.

Under this approach, law enforcement officials can seek a Title III order from a district court with jurisdiction over the area in which the law enforcement officials listen to the communications, or from a court with jurisdiction over the area in which the device that redirects the communications is installed. For electronic communications, law enforcement officials need only identify a point on the network through which a target's communications pass; the target's communications can be duplicated at that point and transmitted to law enforcement officials in a different jurisdiction. Although this issue has not yet arisen in a reported case—most likely because of the absence of a nonconstitutional suppression remedy for electronic communications seized in violation of Title III—a court following the *Rodriguez* line would likely conclude that an interception occurs at the point of duplication or extraction, as well as where law enforcement officials view or process the communications, notwithstanding the fact that such communications are not "aural[ly]" acquired like wire or oral communications. In other words, a court would likely treat the scenario as involving at least two "acquisitions," with an order authorizing an acquisition in either jurisdiction sufficient.

Even though courts have used room within the definition of "intercept" to account for the pressures cross-jurisdictional investigations place on Title III's application to wire and oral communications, and would likely do so with electronic communications, there are significant unexplored policy dimensions to this problem—dimensions that take on even greater significance with electronic communications. Consider first the factors that support the inclusion in Title III of a requirement that a judge authorize interception only within the territorial jurisdiction of the court. The same requirement applies with the issuance of ordinary search warrants under the Federal Rules of Criminal Procedure: a magistrate judge can order a search or seizure of property "located within the district" in which the judge sits[382] (although the USA Patriot Act relaxed that requirement in connection with certain kinds of terrorism investigations).[383] Apart from theories that constitutional provisions limiting the jurisdiction of federal courts dictate such restrictions,[384] such limitations play an important role in protecting privacy: requiring that a warrant be issued by a judge within the jurisdiction where it will be executed allows the judge greater supervisory power over the execution of the warrant. More important, it prevents any kind of forum shopping, under which law enforcement officials could seek a warrant in the jurisdiction where they believe a judge would be most inclined to grant one.[385]

The § 2518(3) requirement that a judge issue an order for interception of communications within the territorial jurisdiction in which the judge sits[386] also facilitates supervisory control over the surveillance; the statute, indeed,

382 FED. R. CRIM. P. 41(b)(1).

383 *Id.* R. 41(b)(3) (authorizing magistrate judges to issue warrants "within or outside" their districts for terrorism-related investigations).

384 *See, e.g.*, United States v. Burford, 755 F. Supp. 607, 611 (S.D.N.Y. 1991) (considering whether Article III, Section 2 of the Constitution prohibits a court from issuing search warrants or wiretap orders that reach beyond the territorial limits of its district).

385 *See Jackson*, 207 F.3d at 914.

386 18 U.S.C § 2518(3) (2000).

is premised on the notion that extensive supervisory power is appropriate, insofar as it empowers a judge to order whatever periodic reports he or she sees fit. The rationale for allowing both the situs of the surveilled facilities and the situs at which law enforcement officials hear the communication to serve as the location where the interception occurs has been that it allows a single judge to monitor the multiple interceptions involved in an investigation with an eye toward protecting privacy: "If all of the authorizations are sought from the same court, there is a better chance that unnecessary or unnecessarily long interceptions will be avoided."[387] Of course, this approach does not account for the potential for the opposite problem: giving law enforcement officials the choice between two or more jurisdictions in which to seek an order—one of which is dictated not by where the offense is occurring, but by where law enforcement officials choose to base their operations—allows the choice of a more favorable forum.[388]

The point here is not that courts have weighed in on the wrong side of this policy question. The point, rather, is that it is much more a question of policy than of statutory interpretation, and it is going to arise more frequently with electronic communications. Because of the absence of a nonconstitutional suppression remedy in Title III, it may never be litigated in an adversarial context in a criminal case. That possibility makes it all the more important for Congress to consider the policy question going forward.

As Congress considers the policy question, the debate within the Internet law literature concerning the challenges the Internet poses for government regulation is instructive. The response to scholars who argue that regulation of Internet conduct is neither feasible nor legitimate has been that states have successfully regulated cross-border transactions in a number of other contexts; the Internet, the argument goes, is nothing more than a mode of communication, like the telephone.[389] In outlining what I anticipated would be courts' response to a challenge to an order authorizing an interception of electronic communications in another jurisdiction, I suggested that courts would likely permit the conduct in question, just as they permit the conduct with respect to wire communications. The response to the argument that Internet transactions are functionally equivalent to other transactions that cut across international borders has been that we must take account of questions of scale:[390] if a vastly higher percentage of Internet transactions will cut across international borders, then the measures that states usually use to cope with the problems of enforcement and legitimacy may themselves be ineffective or illegitimate. The question of scale is necessarily relevant to the policy issues raised by cross-jurisdictional surveillance. Congress has, how-

---

387 United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992).

388 *See Jackson*, 207 F.3d at 914 (noting potential for abuse).

389 *See, e.g.*, Goldsmith, *Against Cyberanarchy*, *supra* note 368, at 1240 (arguing that "activity in cyberspace is functionally identical to transnational activity mediated by other means, such as mail or telephone or smoke signal"); Goldsmith, *Territorial Sovereignty*, *supra* note 368, at 476 ("Like the telephone, the telegraph, and the smoke signal, the Internet is a medium through which people in real space in one jurisdiction communicate with people in real space in another jurisdiction.").

390 *See* Post, *Against "Against Cyberanarchy,"* *supra* note 368, at 1376–81.

ever, gone forward with statutory changes to facilitate cross-jurisdictional surveillance with respect to electronic communications without thorough consideration of these issues.

Consider two important changes the USA Patriot Act made to the surveillance regime. First, the USA Patriot Act established a mechanism for federal agents to seek an order for use of a pen register or trap and trace device anywhere in the United States. Prior to passage of the USA Patriot Act, a "court of competent jurisdiction" could authorize installation of a pen register or trap and trace device "within the jurisdiction of the court."[391] The statute defined a "court of competent jurisdiction" as a federal district court or court of appeals, or a state court of general criminal jurisdiction authorized by the law of the state to enter pen/trap orders.[392] The restriction of the geographic area in which the court could authorize installation of the device had the effect of requiring law enforcement officials to seek an order from the court where the device was to be installed, not necessarily the court where the offense was being investigated.[393]

The USA Patriot Act's amendments to the pen/trap statute, which are not scheduled to expire, made two changes related to the geographic limitations on pen/trap orders.[394] First, when a federal official seeks a pen/trap order from a court of competent jurisdiction, the court can authorize use of the device "anywhere in the United States."[395] The statute also amended the definition of a court of competent jurisdiction to describe a court with jurisdiction over the offense being investigated.[396] In other words, it is the court having jurisdiction over the offense, not the court located where the device is to be installed, that issues the order. Second, the statute clarified where, and from whom, the court could compel assistance in installing the device. The pen/trap statute had authorized a court to direct other parties to furnish "information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device,"[397] but it was unclear whether a court could order such assistance of a provider outside of its territorial jurisdiction. Moreover, communications—particularly electronic communications—are often passed from provider to provider, and an order specifying assistance of one provider would be ineffective against another.

---

391 18 U.S.C. §§ 3122(a), 3123(a) (2000).

392 *Id.* § 3127(2).

393 With respect to wire communications, installation of pen registers raised issues similar to those arising when law enforcement officials redirect communications and listen to them in a different jurisdiction. Here, however, the statutory language had less flexibility, because the statute required the installation of the pen register within the court's jurisdiction. 18 U.S.C. § 3123(a). When law enforcement officials leased a line so as to transmit communications into the jurisdiction where the investigators were located, courts upheld the use of a pen register where the device was installed in that jurisdiction, on the leased line. *See* United States v. Rodriguez, 968 F.2d 130, 135 (2d Cir. 1992); United States v. Burford, 755 F. Supp. 607, 611–12 (S.D.N.Y. 1991).

394 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288–90.

395 18 U.S.C.A. § 3123(a)(1) (West Supp. 2003).

396 *Id.* § 3127(2)(A).

397 18 U.S.C. § 3123(b)(2) (2000).

As amended by the USA Patriot Act, the pen/trap statute addresses both of these problems by providing that a pen/trap order "shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order," whether or not the order specifically names the provider.[398]

The USA Patriot Act also altered the geographic scope of search warrants and orders to acquire wire and electronic communications from electronic storage, by virtue of two subtle changes in section 220 of the Act.[399] For search warrants to acquire communications in electronic storage, the SCA previously required a warrant issued "under the Federal Rules of Criminal Procedure."[400] As noted above, Rule 41(b)(1) authorizes a warrant for a seizure within the district in which the magistrate sits. The USA Patriot Act amended the language of § 2703(a) of the SCA to require only that a court "with jurisdiction over the offense under investigation" issue such a warrant "*using the procedures described* in the Federal Rules of Criminal Procedure."[401] The effect of the change was to shift the responsibility for issuance of the order from the court where the service provider is located to the court with jurisdiction over the offense being investigated; prior to passage of the USA Patriot Act, a disproportionate number of such orders were issued in the Eastern District of Virginia, where AOL is located.[402] Similarly, for orders issued under § 2703(d), Congress removed any geographic limitation on where a service provider might be compelled to produce communications or records. Prior to the Patriot Act, § 2703(d) simply provided that such orders could be issued by a court of competent jurisdiction—a term defined with respect to former § 3127(2)(A) of the pen/trap statute as a federal district court or court of appeals.[403] The amendments to the pen/trap statute discussed above, of course, defined a court of competent jurisdiction as a court with jurisdiction over the offense being investigated.[404] Although the SCA still cross-references that definition, the Patriot Act added a new provision to the SCA stating that the definition "includes any Federal court within that definition, without geographic limitation."[405] At a minimum, this change suggests that a court can order production of records outside of its geographic jurisdiction. It is also possible to conclude that the government can seek a § 2703(d) order from *any* federal court—that the "without geographic limitation" qualification in § 2703(d) removes even the requirement that the issuing court have jurisdiction over the offense in question.

---

398 18 U.S.C.A. § 3123(a)(1).

399 USA PATRIOT Act § 220, 115 Stat. at 291–92.

400 18 U.S.C. § 2703(a) (2000).

401 18 U.S.C.A. § 2703(a) (West Supp. 2003) (emphasis added).

402 *See* U.S. DEP'T OF JUSTICE, DISPELLING SOME OF THE MAJOR MYTHS ABOUT THE USA PATRIOT ACT, *available at* http://www.lifeandliberty.gov/subs/add_myths.htm#_Toc65482106 (last visited July 18, 2004) (noting the administrative burden that prior law placed on jurisdictions in which major Internet service providers are located, including the Eastern District of Virginia).

403 18 U.S.C. § 2703(d); *see id.* § 3127(2)(A).

404 18 U.S.C.A. § 3127(2)(A) (West Supp. 2003).

405 *Id.* § 2711(3).

As I argued above, a territorial limitation on a surveillance order can serve important privacy-protective functions. That is true for Title III, which, because of the ongoing nature of the surveillance, specifically contemplates more intensive judicial supervision than other kinds of warrants. For the SCA, we can identify similar competing policy interests. On the one hand, confining a court's ability to issue an order to its territorial jurisdiction requires law enforcement officials to seek an order in a jurisdiction distant from that in which the offense is being investigated. On the other hand, allowing a court to compel production of evidence in a different jurisdiction has two negative consequences: it allows law enforcement officials to forum shop, and it makes a challenge by a distant service provider to the legality of the order or the burdens it imposes far less likely. In the context of the pen/trap statute, where "judicial review" is purely ministerial, the privacy-protective function of the territorial limitation can be seen from the effect of its absence. Once law enforcement officials have a nationwide order, capable of being served on any provider in the country, without any temporal limitation, the initial articulation of the "relevance" of the information the device will yield must bear the weight of a potentially broad investigation. The relevance of the use of a pen register or trap and trace device having already been articulated, the statute imposes no limitations on use of the order in circumstances where investigators could not meet the standard. We need not assume that law enforcement officials will abuse the nationwide, all-provider features of the order to be troubled by the fact that the statute gives the appearance that courts restrain investigators, when in fact investigators must restrain themselves.

I do not intend to suggest that the concerns raised by cross-jurisdictional electronic surveillance are constitutional concerns, as they are sometimes claimed to be.[406] An appropriate policy analysis, however, would take three factors into account. First, the move away from the trespass model of the Fourth Amendment to the "reasonable expectation of privacy" formulation in part reflected recognition of the inability of the trespass concept to protect intangible communications. Just as our constitutional conception of privacy evolved, our statutory conception of privacy should evolve to take account of the fact that geographically based protections, such as the territorial limitation in § 2518(3), do not necessarily provide adequate checks on surveillance activities; the checks need to be built into the statute in a different form. Second, in areas where no expectation of privacy is involved, and the statutory framework thus does not require a warrant, the geographic limitations may be all the more important, because of the lower level of scrutiny that government actions receive; there is a strong case for additional checks to do the work that the geographic limitation otherwise might do.[407] Finally, if in-

406 *See, e.g.*, CTR. FOR DEMOCRACY AND TECH., ANTI-TERRORISM ACT EXPANDS GOVERNMENT SURVEILLANCE AUTHORITIES, WEAKENS PRIVACY PROTECTION WITH NO CLEAR BENEFIT TO SECURITY (2001) (on file with author) (discussing provision that would allow nationwide service of search warrants for electronic evidence).

407 The pen/trap statute provides a useful example. When law enforcement officials intend to use a device to acquire communications from facilities outside the jurisdiction of the court, they could be required to articulate reasonable grounds to believe that the communications as to

deed investigations involving electronic communications call for cross-jurisdictional surveillance far more often than investigations involving wire communications, then perhaps the substantive standard, or other procedural protections, should be adjusted to account for this issue of scale.[408]

3. Service Providers as Points of Control

The third theme within the Internet law literature that can fruitfully be brought to bear on Internet surveillance issues relates to the extent to which service providers and other intermediaries can become points of "control," where the government seeks to achieve its regulatory objectives.[409] Indeed, service providers play a prominent role in the debate over the power of geographically based sovereigns to apply their law to Internet-related transactions. Scholars argue that states wishing to regulate Internet-related transactions can in fact do so by targeting service providers with a presence within their geographic boundaries.[410] For example, to the extent that the government wishes to curb online copyright infringement—much of which occurs outside of the territorial United States—it can impose an obligation on service providers or other intermediaries that host or index that content to disable access to it upon receiving a claim that the material is infringing, as it has done with provisions of the Digital Millennium Copyright Act.[411] Similarly, when efforts to regulate objectionable content directly fail, states can attempt to impose the obligation to disable access to such content on service providers, as the Commonwealth of Pennsylvania has done with its child pornography statute.[412] Even where a statute does not directly target service providers or other intermediaries, such entities can greatly affect the shape of the Internet—the degree of anonymity (or pseudonymity) that users experience, what data concerning a user's activities is retained (and for how long), and so on.[413]

Although this issue has been extensively explored within the Internet law literature, the scholarship has not considered the relevant Internet surveillance activities. Our surveillance laws still conceive of the most important form of electronic surveillance as that occurring through unilateral installa-

---

which the pen register or trap and trace device is to be applied will pass through multiple jurisdictions, and that identification of the source and destination of such communications will require the involvement of multiple service providers. Moreover, a nationwide order that applies to unnamed providers should be limited in duration.

408 *See* Post, *Against "Against Cyberanarchy," supra* note 368, at 1376–81.

409 *See, e.g.*, Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

410 *See* Goldsmith, *Against Cyberanarchy*, *supra* note 368, at 1217; Goldsmith, *Territorial Sovereignty*, *supra* note 368, at 481 (noting that nations can "regulate the local means through which foreign content is transmitted").

411 *See* 17 U.S.C. § 512(c)–(d) (2000).

412 *See* 18 PA. CONS. STAT. ANN. § 7622 (West 2004) ("An Internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet service provider is notified by the Attorney General . . . that child pornography items reside on or are accessible through its service."); Zittrain, *supra* note 409, at 674–82.

413 *See* LESSIG, *supra* note 350, at 66–71; Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1675–76 (1995).

tion of devices by law enforcement officials or installation of such devices with the assistance of third parties, and it is this kind of surveillance that generates the most public concern and scholarly attention.[414] Although we obviously must consider the appropriate boundaries of device-based surveillance, the fact that service providers and other intermediaries hold so much data means that we must focus on them not only as points of "control"—where the government can seek to achieve its regulatory objectives—but also as points of "extraction"—where government can achieve its investigatory objectives. I have already tried to make the case that extraction of communications from service providers, under government compulsion, has a constitutional dimension. But we need to be equally concerned about disclosures of information that involve no state compulsion. The challenge for Congress going forward, then, is to acknowledge that what we traditionally think of as government "surveillance" is not necessarily the sole or primary means by which the government can acquire intangible communications. Apart from the fact that copies of electronic communications are stored far more frequently than copies of wire communications, it may be necessary for law enforcement officials to gather electronic communications from service providers whenever possible, because Title III requires the exhaustion of other investigative methods.

The issues have both substantive and institutional dimensions. As discussed in Part I, the statutory framework for compelled production of communications involves varying substantive standards and necessarily rests on the premise that at least some electronic communications held by service providers are not subject to an expectation of privacy. If compelled production of communications from a third party is an attractive alternative to device-based surveillance for technical and statutory reasons, then it may be appropriate to ratchet up the standard. As for voluntary disclosure, the Fourth Amendment line including the *Lopez*, *Hoffa*, *Osborn*, and *White* cases, discussed earlier,[415] suggests that no expectation of privacy exists. The SCA provides a layer of statutory protection against disclosure to government officials, but that protection applies only to providers that offer services to the general public. Because service providers hold copies of electronic communications in so many instances, they may serve as an attractive point for law enforcement officials to extract communications. Because the line between a "voluntary" disclosure and compelled production is blurry, Congress must consider additional disclosure limitations.

As for the institutional competence issue, I argued in Part I that courts should test the SCA against the Fourth Amendment, because it is based on a

414 Public reaction to revelations about the use of Carnivore provides a useful example. *See, e.g.*, John Schwartz, *FBI Internet Wiretaps Raise Issues of Privacy: New System Tracks Suspects Online*, WASH. POST., July 12, 2000, at E1. For discussion of the concerns raised by Carnivore's use, see Frank J. Eichenlaub, Comment, *Carnivore: Taking a Bite out of the Fourth Amendment?*, 80 N.C. L. REV. 315 (2001); Johnny Gilman, Comment, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS 111 (2001); Trenton C. Haas, Note, *Carnivore and the Fourth Amendment*, 34 CONN. L. REV. 261 (2001); Maricela Segura, Note, *Is Carnivore Devouring Your Privacy?*, 65 S. CAL. L. REV. 231 (2001).

415 *See supra* notes 142–57 and accompanying text.

faulty constitutional premise. Congress nevertheless is the primary guarantor of privacy in this area. In light of the current state of Fourth Amendment law, it is clear that Congress, not the courts, must have the primary responsibility in crafting voluntary disclosure limitations.

Conclusion

The approach of the USA Patriot Act's sunset date provides Congress with the opportunity to rethink Internet surveillance law. The constitutional and statutory categories governing electronic surveillance law developed at a time when electronic communications either did not exist or were not widely used, and subsequent technological developments have placed tremendous strain on those categories. Most important, in 1986, when Congress sought largely to align treatment of electronic communications with treatment of wire communications, it could not have anticipated that technological developments would place so many electronic communications in the hands of third parties. As I have argued, the relatively weak protection the law provides to several categories of electronic communications held by third parties stems from an overly broad reading of case law that developed in a far different context. Although a number of basic changes would improve the state of surveillance law, the pressures that electronic communications place on the surveillance law framework will only continue to mount. Bringing Internet surveillance law within the mainstream of Internet law scholarship can provide much-needed normative guidance to Congress as it reconsiders the surveillance law framework.