Minnesota Journal of Law, Science & Technology

Volume 9 | Issue 1 Article 12

2007

Constitutionalizing Email Privacy by Informational Access

Manish Kumar

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

Note

Constitutionalizing E-mail Privacy by Informational Access

Manish Kumar[*]

The popular embrace of electronic mail (e-mail)[1] has not led to its recognition by the Supreme Court as a constitutionally protected realm of privacy. Perhaps this is for good reason. No prevailing legal theory for such a result presents itself in the Fourth Amendment jurisprudence. By analogizing the function of the Internet to the postal system, some courts have found an absence of a constitutional privacy interest because electronic data is exposed in transit like the writing on a postcard.[2] The Supreme Court, however, has emphasized the social expectations regarding the use of a communication system as relevant to the constitutional analysis in other contexts, which leads to the opposite conclusion.[3] It has not, however, gone so far as to recognize a general right to privacy or an interest in mere content.[4] Still other courts have adopted modern translations of the Fourth Amendment, concluding that e-mails are the contemporary equivalent of "papers" referenced in the Fourth Amendment.[5]

---

* J.D. Candidate 2008, University of Minnesota Law School; A.B. 2004, Stanford University. I thank Professor Stephen Cribari for his invaluable guidance, the Journal's editors and staff for their dedication in seeing this article to production, and my parents for everything else.

1. For example, electronic mail (e-mail) volume increased from 5.1 million messages in 2000 to 135.6 million in 2005. Lizzette Alvarez, *Got 2 Extra Hours for Your E-mail?*, N.Y. TIMES, Nov. 10, 2005, at G1. This Note focuses on electronic mail, though its conclusions are generalizable to other types of electronic files.

2. Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001) (rejecting an expectation of privacy in (non-content) information disclosed to an Internet Service Provider (ISP)).

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

4. *Id.* at 350 ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'").

5. ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996).

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

An alternative approach to constitutionalizing e-mail privacy is to deemphasize the technological aspects and social expectations relating to its use. In a line of technological surveillance cases culminating most recently in *Kyllo v. United States*,[6] the Supreme Court has suggested the constitutional inquiry into what constitutes a reasonable expectation of privacy can be reduced to a simple question: Does the government have to employ special means not available to the public to access to the allegedly private information? If so, there is a government search cognizable by the Fourth Amendment.[7] This approach can provide a useful framework for analyzing e-mail privacy.

This Note presents an informational access interpretation of the Fourth Amendment. Part I describes the technological trends underlying the need for electronic privacy. Part II describes the existing statutes regulating electronic privacy. Part III develops the information access theory to privacy by examining the prior case law. Part IV applies the theory to e-mail. Part V considers some of the objections to constitutionalizing e-mail privacy.

I. A SUPERHIGHWAY LIKE NO OTHER

Because it is so different from previous forms of communication, e-mail challenges traditional notions of Fourth Amendment privacy. Case law discussing privacy expectations for other forms of communication provides imperfect analogies for analyzing e-mail privacy issues. Like the postal and telephone systems, the Internet is a communications network for human-to-human contact. Unlike the postal mail and telephone calls, however, a large portion of Internet traffic involves a single person. For example, a user may use a computer to access webpages from a remote server.[8] Other communications are fully autonomous, as when computer

6. 533 U.S. 27, 34–36 (2001).

7. Government conduct violating an individual's reasonable or legitimate expectation of privacy is a Fourth Amendment search. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

8. Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 613 (2003) [hereinafter Kerr, *Big Brother*].

servers coordinate to route network traffic.[9] It is therefore not clear to what extent one category of electronic communications should receive differing constitutional treatment from another.

The Internet's method of routing data presents other analytical difficulties. The Internet is a packet-switched network, meaning that computers transmit information by reducing it into smaller groups of data, called packets.[10] Intermediate routers advance the packets from one point on the network to another.[11] Alternatively, the routers may store, reassemble, and repacketize the data.[12] Each packet contains a header identifying the origin, destination, type, and size of the conveyed information.[13] Computers use this information to reassemble packets into the original communication.[14] This process differs from the operation of the phone and postal systems, which do not break information down into packets. A postal communication consists of a single document with "header" information located on the front of the envelope,[15] while the typical telephone call consists of a bidirectional stream of voice data preceded by a series of tones (by dialing a phone number) serving as the addressing information "read" by switching equipment.[16]

A third distinguishing feature of Internet communications is that information often ends up with third parties. Unlike the postal system, where the mail carrier relinquishes possession of the letter after delivering it to the addressee, Internet usage often involves storing information with a third party service provider.[17] A user has no physical possession over content, unlike the interior contents of a letter in an envelope. Instead,

9. *Id.*

10. *Id.*

11. *Id.*

12. Samantha L. Martin, Note, *Interpreting the Wiretap Act: Applying Ordinary Rules of "Transit" to the Internet Context*, 28 CARDOZO L. REV. 441, 449 (2006).

13. Kerr, *Big Brother*, *supra* note 8, at 614.

14. *Id.*

15. The term "envelope information" describes the addressing and routing information that communications networks use to deliver the contents of communications. *Id.* at 611.

16. Modern digital switches may also packetize information, but this does not appear to have affected the case law.

17. 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, 1209 (2004) [hereinafter Kerr, *User's Guide*].

the user often relies on a network service provider to provide a block of storage on a computer server, such as for an e-mail account. Furthermore, third parties responsible for only conveying the information may nevertheless retain copies, as when communicating servers retain a copy of a transmitted packet.[18] Since private data is so routinely entrusted to others, interested parties can discreetly obtain recorded data without ever entering the home.

Technological trends reinforce the migration of private data into the hands of third parties. "Always on" high-speed Internet connectivity encourages users to use web-enabled communications services.[19] For example, users may rely on document sharing software such as Google Desktop.[20] The program sends a copy of a user's documents to Google's servers, allowing this information to be searched and retrieved from a computer anywhere in the world. It requires, however, that a copy of all the user's documents reside with Google.[21] Alternatively, users may use online applications accessed via the Internet. For example, instead of loading a word processor program installed on the computer's hard drive, an author can access a server that runs the word processor program and maintains a copy of the author's work via the Internet. The benefits of this type of distributed computing have caused the Federal Aviation Administration to review its software procurement policies.[22] The consequence of the trend toward remotely stored and manipulated data is that a user's documents are less often within the home, which may impact individual and social expectations of privacy.

18. Martin, *supra* note 12, at 449.

19. Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 83 (2006).

20. Google Desktop Homepage, http://www.googledesktop.com (last visited Oct. 5, 2007).

21. Press Release, Electronic Frontier Foundation, Google Copies Your Hard Drive — Government Smiles in Anticipation (Feb. 9th, 2006), http://www.eff.org/press/archives/2006/02/09.

22. Paul McDougall, *FAA May Ditch Microsoft's Windows Vista And Office For Google And Linux Combo*, INFORMATION WEEK, Mar. 6, 2007, http://www.informationweek.com/shared/printableArticle.jhtml?articleID=197800480.

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

II. EXISTING STATUTORY LAW

Congress has attempted to regulate Internet privacy through two pieces of legislation: the Electronic Communications Privacy Act of 1986 (ECPA)[23] and the Stored Communications Act (SCA).[24]

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The ECPA applies to prospective surveillance of information in transmission, prohibiting the interception of oral, wire, or electronic communications. The Statute punishes anyone who "intentionally intercepts . . . any wire, oral or electronic communication."[25] In order to overcome this prohibition, the Wiretap Statute provides for a special type of warrant with enhanced requirements.[26]

The Wiretap Act suffers from ambiguity surrounding the word "transmission" as used in § 2511 of the statute. A provision defined "wire communication" as including communications in electronic storage, but the USA PATRIOT Act deleted this.[27] Therefore, it is not clear whether communications in *temporary* electronic storage are within its scope, as when intermediate routing computers retain copies of packetized information. Uncertainty also arises over whether the information, because it is simultaneously in storage and in transit, is subject to the heightened protections of the Wiretap Act or the lesser protections of the SCA.[28] The First Circuit grappled with these issues in *United States v. Councilman*,[29] reversing itself *en banc* and finding that "an e-mail message does not cease to be an 'electronic communication' during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage."[30] Once the electronic communication reaches its destination, the

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

24. *See* 18 U.S.C. §§ 2701–2711 (2000 & Supp. I 2001).

25. 18 U.S.C § 2511(1)(a) (2000).

26. The warrant requires a finding, beyond probable cause, that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.* § 2518(3)(c). Only certain government officials can apply for this type of warrant. *Id.* § 2516.

27. Martin, *supra* note 12, at 451.

28. *Id.* at 455–56.

29. 418 F.3d 67 (1st Cir. 2005).

30. *Id.* at 79.

protections of the ECPA do not apply.[31] Neither does the ECPA prohibit Internet service providers from intercepting, disclosing, or using data that they transmit or receive.[32]

THE STORED COMMUNICATIONS ACT

If electronic information is not eligible for protection under the ECPA, it may still be subject to the SCA. The SCA distinguishes between providers of communication services, who send or receive wire or electronic communications,[33] and providers of remote computing services, who trade in "computer storage or processing services by means of an electronic communications system."[34] The former specifies that for unopened e-mail communications in storage for less than 180 days, the government must obtain a search warrant for acquiring content information. After 180 days, the minimum proof requirement drops to (1) a mere subpoena or (2) prior notice plus a "specific and articulable facts" court order.[35] The same level of protection applies for opened e-mails and files in storage or processing.[36] Both requirements are less stringent than the enhanced search warrant outlined in the Wiretap Act.

The SCA is not without its loopholes. First, it distinguishes between compelled and voluntary disclosures. Like the ECPA, the protections outlined above do not apply to nonpublic providers of remote computing services who voluntarily disclose information to the government, such as employers.[37] Second, the SCA refers to remote computing services that offer processing or storage services to the public.[38]

---

31. *See* United States v. Steiger, 318 F.3d 1039, 1040 (11th Cir. 2003); Wesley Coll v. Pitts, 974 F.Supp. 375, 389 (Del. 1997), *aff'd*, 172 F.3d 861 (3d Cir. 1998).

32. 18 U.S.C. § 2511(2)(a)(i) (2000); *see also* Joshua L. Colburn, Note, *"Don't Read This If It's Not for You": The Legal Inadequacies of Modern Approaches to E-mail Privacy*, 91 MINN. L. REV. 241, 249 (2006) (summarizing commentary on this exception).

33. 18 U.S.C. § 2510(15) (2000 & Supp. I 2001).

34. *Id.* § 2711(2).

35. *Id.* § 2703(d) (requiring "specific and articulable facts showing that there are reasonable grounds to believe that the [information to be compelled] is 'relevant and material to an ongoing criminal investigation'").

36. *Id.*

37. *See id.* § 2702(a) (imposing restrictions on providers of services "to the public").

38. *Id.* § 2711(2).

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

Some legislative history suggests this only applies to "outsourcing" functions.[39] But "outsourcing" is an anachronistic term. In the early days of computing, businesses sent raw data to remote computing services to perform the necessary calculations because powerful desktop spreadsheet applications did not yet exist.[40] Today, however, websites are often computing destinations in themselves, allowing users to manipulate the relevant data.[41] It is not clear whether using a website is "outsourcing" data, especially if one's local computer must process data (such as to packetize it) to send it over the Internet to a remote server. If processing is narrowly defined to exclusively consist of remote processing services, and the Internet service provider (ISP) is not specifically providing storage services to the user, then the SCA does not apply.

The ECPA and SCA suggest that congressional rules are imperfect methods for protecting privacy. The complexities of Internet infrastructure can lead to judicial confusion regarding statutory interpretation.[42] If legislators try to alleviate this problem by writing statutes that track technologies too closely, they risk creating laws that soon become anachronistic.[43] Frequents revisions to such statutes are not possible given the administrative and opportunity costs. Indeed, despite the tremendous growth of microprocessing technology, Congress has significantly revised the electronic surveillance law only five times.[44] Furthermore, commentators have argued that congressional rulemaking has resulted in a piecemeal approach to electronic privacy.[45] Many other forms of electronic surveillance are unregulated, such as global positioning satellite (GPS) tracking, video surveillance, facial recognition systems, satellite technologies, radio frequency identification

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

40. Kerr, *User's Guide*, *supra* note 17, at 1213–14.

41. *Id.* at 1230.

42. *See supra* notes 27–30 and accompanying text. At least one commentator has pointed out that the fact Orin Kerr had to write an article describing the basic operation of the SCA demonstrates its Byzantine nature. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 766 (2005) ("If electronic surveillance law was clear, Kerr would have a lot less to write about.").

43. *Id.* at 767–69.

44. *Id.* at 769.

45. *Id.* at 763–64.

(RFID) systems, and sensory enhancement technologies.[46]

In light of these shortcomings, judge-made law could make a useful contribution by articulating broad standards to regulate electronic privacy. As technology changes, courts can gradually revise precedent, a more practical possibility than getting a law passed in Washington. Alternatively, Congress can provide supplementary legislation to clarify judicial standards. This happened when the Supreme Court established general standards for protecting the content of telephone conversations in *Berger v. New York*[47] and Congress subsequently assumed those specific provisions when writing the Wiretap Act.[48]

So far, however, courts have played a minimal role in the creation of privacy rules in the electronic context. Most of the statutes regulating electronic information lack an exclusionary rule, discouraging litigants from redressing such matters with the courts.[49] Courts have also deferred to Congress to determine what deserves a reasonable expectation of privacy, characterizing such line-drawing as the province of the legislative branch.[50] Judicial law, however, could provide a flexible standard in an area that is rapidly changing and guide policymakers toward framing the appropriate regulations. The following presents a possible legal basis for such a standard.

46. *Id.*

47. 388 U.S. 41 (1967).

48. S. REP. NO. 90-1097, at 214-18 (1969), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2113.

49. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 806-07 (2003) [hereinafter Kerr, *Lifting the "Fog"*].

50. *E.g.*, Askin v. McNulty, 47 F.3d 100, 106 (4th Cir. 1995) ("As new technologies continue to appear in the marketplace and outpace existing surveillance law, the primary job of evaluating their impact on privacy rights and of updating the law must remain with the branch of government designed to make such policy choices, the legislature."); *see also* Adams v. City of Battle Creek, 250 F.3d 980, 986 (6th Cir. 2001) ("Congress made the [Electronic Communications Privacy Act] the primary vehicle by which to address violations of privacy interests in the communication field.").

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

III. PRIOR CASE LAW AND THE INFORMATIONAL APPROACH TO THE FOURTH AMENDMENT

PREVIOUS APPROACHES TO THE FOURTH AMENDMENT

Several policy justifications exist for protecting electronic communications under the Fourth Amendment, such as that it prevents untrammeled government surveillance,[51] protects legitimate conduct,[52] and so on. Some commentators argue in normative terms for greater privacy protections, arguing that persons routinely entrust private information to the Internet.[53] Others make constitutional arguments, noting that the Supreme Court's current stance toward electronic communications departs from popular expectations of privacy.[54]

The Fourth Amendment question turns not on any general notions of unreasonable governmental conduct, but instead whether there was an unreasonable search or seizure.[55] This depends on whether government conduct violated an individual's "reasonable expectation of privacy" as described in Justice Harlan's oft-cited concurrence in *Katz*.[56] To determine what is a search or seizure, the analysis proceeds in two steps.[57] The first is to ask whether the challenged governmental conduct violated the individual's subjective

51. Zittrain, *supra* note 19, at 83–84.

52. *Id.*

53. *Id.* at 83 (arguing that the increasing use of data networks means that Fourth Amendment protections for home life ought to be extended to "digital life"); *see also* Deirdre Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1586–88 (2004) (arguing electronic information is analogous to Fourth Amendment papers).

54. *See* Kerr, *Big Brother*, *supra* note 8, at 629 n.98 ("This approach surely reflects honorable aspirations, but it strangely ignores the fact that in the thirty-five years since *Katz*, the courts have mostly rejected such an expansive view of its holding.").

55. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable *searches and seizures*, shall not be violated . . . ." U.S. CONST. amend. IV (emphasis added).

56. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

57. *See* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create A Reasonable Expectation of Privacy?*, 33 CONN. L. REV. 503, 507 (2001) [hereinafter Kerr, *Encryption*] (providing this formulation of the *Katz* test).

expectation of privacy, which almost always is the case.[58] At that point, the analysis turns to the more essential question of whether the expectation is "one that society is prepared to recognize as 'reasonable.'"[59] Courts have encountered difficulty in performing this inquiry.[60]

There are at least two theories underlying the reasonable expectations inquiry for the Fourth Amendment. The first is rights-based: an expectation is reasonable when it is backed by an enforceable right to enjoin the government's invasion of privacy, such as through property law.[61] For example, the Supreme Court in *Rakas v. Illinois*[62] noted that "concepts of real or personal property law" could be instructive.[63] The Supreme Court exemplified this theory by noting that a

> burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as "legitimate." His presence . . . is "wrongful"; his expectation is not "one that society is prepared to recognize as 'reasonable.'"[64]

Because the criminal's presence in the cabin has no enforceable basis, he can have no reasonable expectation of privacy. Third party disclosure cases such as *United States v. White*[65] implicitly endorse this approach. They suggest that because a defendant has no right to limit the divulgences of an unreliable informant, no constitutional protection is available even for confidential conversations.[66]

The second theory underlying the Fourth Amendment is based on the reasonable person in tort. A legitimate expectation of privacy turns on whether a reasonable person placed in the individual's shoes would expect something to remain confidential.[67] The reasonable person in turn has an

58. *Id.* at 507.
59. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
60. *See infra* notes 72–77 and accompanying text.
61. Kerr, *Encryption*, *supra* note 57, at 507.
62. 439 U.S. 128 (1978).
63. *Id.* at 143–44 n.12.
64. *Id.* (internal citations omitted).
65. 401 U.S. 745 (1971).
66. *See infra* Part V.
67. Kerr, *Encryption*, *supra* note 57, at 507.

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

objective basis, determined by the widely held beliefs of society. This standard originated in *Katz v. United States*, where the Supreme Court emphasized strong privacy protections for new technologies.[68] The *Katz* decision presented a paradigm shift in Fourth Amendment jurisprudence. It expanded the scope of applicability of the Fourth Amendment by deemphasizing the property law concepts that had immunized many forms of government surveillance from constitutional scrutiny.[69] Subsequent cases have continued to stress the predominance of social views.[70]

This social expectations view of the Fourth Amendment holds the most potential for e-mail privacy advocates. The rights-based model, on the other hand, has limited applicability because few demonstrable rights can enjoin an invasion of privacy in cyberspace. As technology advances, situations implicating an individual's expectations of privacy increasingly involve electronic information. Since people routinely entrust private material to the Internet, this supports a finding that government access to the data is a search. The problem, however, is that while commentators support the social expectations theory, the case law does not seem to be in agreement.[71] The *Katz* decision has had its share of criticism.[72] It provides little guidance for its application, and

68. 389 U.S. 347 (1967).

69. The paradigmatic case of the pre-*Katz* era is *Olmstead v. United States*, 277 U.S. 438 (1928), in which the Court found that wiretapping in a suspected bootlegger's basement and office building did not trigger Fourth Amendment protections because no trespass had occurred on the defendant's property.

70. Justice Rehnquist observed that "legitimation of expectations of privacy by law must have a source outside the Fourth Amendment . . . [such as] understandings that are recognized and permitted by society." Rakas v. Illinois, 439 U.S. 128, 143–44, n.12 (1978). The Court has restated this factor as "our societal understanding that certain areas deserve the most scrupulous protection from government." O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)).

71. Kerr, *Encryption*, *supra* note 57, at 508.

72. *See* Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 204 n.10 (1993) (citing Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468 (1985) ("The Fourth Amendment is the Supreme Court's tarbaby: a mass of contradictions and obscurities that has ensnared the 'Brethren'. . . ."); Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 616 (1996) ("The *Katz* approach has degenerated into a standardless 'expectations' analysis that has failed to protect either privacy or property interests."); Morgan Cloud,

the Court's subsequent pronouncements have been less than conclusive.[73] Scholars[74] and Justices[75] have questioned the consistency of the resulting case law. The Court has failed to adopt an expansive reading of *Katz* in the intervening years, saying little on the subject of electronic communications privacy.[76] Instead, many decisions continue to be rights-based, focusing on property concepts in analyzing the legitimacy of privacy expectations.[77] More recently, however, the Supreme Court again endorsed the social expectations theory.[78] The

Search and Seizure by the Numbers: The Drug Courier Profile and Judicial Review of Investigative Formulas, 65 B.U. L. REV. 843, 845 (1985) (criticizing observing "contradictory results in spite of remarkably similar facts"); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 587 (1989) ("[T]he entire course of recent Supreme Court fourth amendment precedent . . . is misguided and inconsistent with the spirit of the fourth amendment."); Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173 (1988) (criticizing Fourth Amendment balancing as a methodology because it dilutes liberty); Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 383 (1988) (arguing that the Court has failed "to develop a coherent analytical framework" for the Fourth Amendment); Silas J. Wasserstrom & Louis M. Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 20, 20 (1988) ("[T]here is virtual unanimity . . . that the Court simply has made a mess of search and seizure law."); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1080 (1987).

73. For example, the Supreme Court has phrased the determinative factors for a socially acceptable expectation of privacy as "the intention of the Framers of the Fourth Amendment, . . . the uses to which the individual has put a location, . . . and our societal understanding that certain areas deserve the most scrupulous protection from government invasion." California v. Ciraolo, 476 U.S. 207, 220 (1986) (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)). This suggests a totality of the circumstances inquiry rather than a strict standard, and the Supreme Court has since revisited privacy expectations on a case-by-case basis.

74. *See supra* note 72.

75. Justice Scalia's assessment of the *Katz* doctrine conceded that it has been criticized as "circular, and hence subjective and unpredictable . . . it may be difficult to refine . . . ." Kyllo v. United States, 533 U.S. 27, 34 (2001).

76. *Id.*

77. *Id.*

78. Georgia v. Randolph, 547 U.S. 103 (2006). Justice Souter, writing for the majority, observed

> The constant element in assessing Fourth Amendment reasonableness . . . is the great significance given to widely shared social expectations, which are naturally enough

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

Court's embrace of social expectations in the consent context suggests it may play a role in other types of Fourth Amendment claims.

> influenced by the law of property, but not controlled by its rules . . . the reasonableness of such a search is in significant part a function of commonly held understandings about the authority that co-inhabitants may exercise in ways that affect each other's interests.

Id. at 111. Notably, the Court chose not to apply a more formal rights-based approach grounded in property law. *Id.* at 110 ("The common authority that counts under the Fourth Amendment may thus be broader than the rights accorded by property law."). The Chief Justice questioned the scope of applicability of the social expectations concept but agreed that it could be used to determine whether there was a government search. *Id.* at 130 (Roberts, C.J., dissenting).

THE GENERAL PUBLIC USE DOCTRINE AND PUBLICLY EXPOSED INFORMATION

Fourth Amendment cases involving surveillance technology provide a possible basis for constitutionalizing e-mail privacy. *Kyllo v. United States*[79] is the most recent in this line of cases. It involved the government's use of a thermal imager to detect infrared radiation emitting from inside a home.[80] Special lamps for growing marijuana plants may give off this type of radiation. Without ever setting foot on the petitioner's property, the government agent scanned the home and used this information to obtain a warrant to search the premises.[81] The Court held, "[w]here, as here, the Government uses a device not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[82] Justice Scalia, writing for the majority, suggested a rights-based approach to privacy expectations, noting that the search involved the interior of the home, which is "the prototypical and hence most commonly litigated area of protected privacy."[83] As a result, there is a "ready criterion, with roots deep in the common law, of the minimal expectation of privacy . . . that is acknowledged to be reasonable."[84]

In order to reach this conclusion, it was necessary for the Court to analyze the technology used to conduct the government surveillance. It twice rested its holding on thermal imagers not being in the general public use.[85] This forms the basis for the informational access interpretation of the Fourth Amendment. A significant factor for defining a Fourth Amendment "search" is the extent of public access to the information sought to be suppressed. Had the telltale heat signature produced by the defendant's growing lamps been

79. *Kyllo*, 533 U.S. at 33–34 (2001).
80. *Id.* at 29.
81. *Id.* at 30.
82. *Id.* at 40.
83. *Id.* at 34.
84. *Id.*
85. *Id.* ("[A]t least where (as here) the technology in question is not in general public use."); *id.* at 40 ("Where, as here, the Government uses a device that is not in general public use.").

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

readily accessible because the public regularly used thermal imagers, the Court would have arrived at the opposite result.[86] According to this approach, the use of technology is not the dispositive factor; rather, it is the extent of accessibility to the relevant information through either aided or unaided means. For example, if it had been snowing on the night of the surveillance, and one could readily observe an unusual pattern of snowmelt on the roof of the defendant's home, there would be no search because that information was available to passersby who were members of the public.[87]

Justice Scalia's response to an objection that the information was already in the public domain supports the view of reasonable privacy expectations turning on information access.[88] There was a colorable argument that the heat signature was merely information being radiated from the external surface of the house.[89] The Court responded that this was a "mechanical" interpretation of the Fourth Amendment.[90] Justice Scalia referenced other examples where it would have found a denial of Fourth Amendment protections problematic.[91] The Court seemed to reason that the mere fact that the information existed in the public domain was irrelevant. Instead, it was the inability to meaningfully access and interpret it through readily available means that created the privacy invasion.

This is not the first time the Supreme Court has relied on the public accessibility of information to determine the scope of a constitutional privacy interest. In *Katz*, government agents placed a microphone outside a telephone booth to overhear a

86. The 2007 Mercedes Benz S-Class sedan comes equipped with an infrared camera for nighttime driving. *2007 Mercedes-Benz S-Class*, POPSCI.COM, http://www.popsci.com/cars/article/2005-11/2007-mercedes-benz-s-class. This camera is functionally similar to the thermal imager in *Kyllo*, and suggests that had *Kyllo* been decided more recently, the government's evidence might not have been excluded.

87. The dissent raised this possibility as a means for arguing the information collected from the imager was public in nature, but the majority characterized this argument as "irrelevant" because "on the night of January 16, 1992, no outside observer could have discerned the relative heat of Kyllo's home without thermal imaging." *Kyllo*, 533 U.S. at 35 n.2.

88. *Id.*

89. *Id.* at 35.

90. *Id.*

91. The Court referenced a satellite picking up light from a house or a microphone picking up sound from a house. *Id.* at 35.

conversation.[92] The phone call theoretically could have been overheard by a member of the public, but the Court found the placement of the microphone to have no constitutional significance.[93] Instead, it was the fact that the microphone created an uninvited ear undetectable to the defendant that implicated the constitutional interest.[94] Because the public could not have been similarly situated, either because such recording devices were not generally used by the public, or because a member of the public standing near the booth would have provoked the suspicion of the caller, the Court found that a Fourth Amendment search occurred.

California v. Ciraolo[95] continued the line of cases where reasonable expectations of privacy turn on public accessibility to information. Responding to an anonymous tip about the cultivation of marijuana, a police officer flew a private plane over the respondent's house within navigable airspace and photographed the backyard using a standard thirty-five millimeter camera.[96] Justice Burger, writing for the majority, found no constitutionally cognizable search, and wrote famously that the Fourth Amendment did not require law enforcement officers to shield their eyes when passing by a home.[97] He cited *Katz* for the proposition that one could waive a privacy expectation by exposing information to the public.[98] The fact that the cultivation area was within the curtilage was not dispositive.[99]

Ciraolo presents a tension when compared to the facts of *Kyllo*. In both cases, the petitioner released incriminating information into the public domain (the heat signatures and the appearance of the marijuana plants), the information had a private character (in neither case did the homeowners want

92. Katz v. United States, 389 U.S. 347, 348 (1967).

93. *Id.* at 353.

94. *See id.*

95. 476 U.S. 207 (1986).

96. *Id.* at 209–10.

97. *Id.* at 213.

98. "'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'" *Id.* (citing *Katz*, 389 U.S. at 351 (1967)).

99. *Ciraolo*, 476 U.S. at 213 ("That the area is within the curtilage does not itself bar all police observation."). Part V discusses this waiver doctrine in more detail.

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

their activities to be detected), and both cases involved a personal residence. The reason the outcome in these two cases diverged is explained by availability of access to the information sought to be suppressed. In *Ciraolo*, the Court noted the routine nature of private and commercial flights.[100] The consequence of this was that "[a]ny member of public flying in this airspace who glanced down could have seen everything that these officers observed."[101] The information was readily accessible, and hence no constitutional protections applied. Conversely, in *Kyllo*, the thermal imager was not in the general public use,[102] and the information it uncovered was not generally accessible. The result in *Ciraolo* would have been different if access to the flight path was restricted to law enforcement personnel.

Florida v. Riley[103] confirmed public access to protected information as a cornerstone of the Fourth Amendment inquiry. On facts similar to *Ciraolo*, a law enforcement agent flew a helicopter within public navigable airspace at a height of 400 feet above the defendant's residence to view the marijuana plants growing inside.[104] Writing separately, Justice O'Connor clarified the standard following from *Ciraolo* in her concurrence:

> [C]onsistent with *Katz*, we must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not "one that society is prepared to recognize as 'reasonable.'" Thus . . . . [i]f the public rarely, if ever, travels overhead at such altitudes, the observation cannot be said to be from a vantage point generally used by the public and Riley cannot be said to have "knowingly expose[d]" his greenhouse to public view. However, if the public can generally be expected to travel over residential backyards at an altitude of 400 feet, Riley cannot reasonably expect his

100. "In an age where private and commercial flight in the public airways is routine, it is unreasonable . . . to expect that [defendant's] marijuana plants were constitutionally protected from being observed . . . ." *Id.* at 215.

101. *Id.* at 213–14.

102. *See supra* note 85 and accompanying text.

103. 488 U.S. 445, 445 (1989).

104. *Id.*

curtilage to be free from such aerial observation.[105]
Finding the inspection conducted with the helicopter to be routine, the Court held that it did not constitute a search.[106]

The Court has considered the constitutional relevance of public access to information in contexts outside the home as well. *Dow Chemical Company v. United States*,[107] another flyover case, involved a business entity. The Court found a constitutional difference between the privacy interest of the home and the "outdoor areas or spaces between structures and buildings of a manufacturing plant."[108] Nevertheless, the decision suggested that the same calculus based on public access to information was applicable: "It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment *not generally available to the public*, such as satellite technology, might be constitutionally proscribed absent a warrant."[109] A future Supreme Court could therefore rely on this language to apply the information access approach to privacy expectations outside the home.

Public access to information sought to be protected under the Fourth Amendment has been a dispositive factor in lower court decisions as well. For example, in *Askin v. McNulty*,[110] the Fourth Circuit addressed whether the government could monitor telephone conversations between the appellant and a third party as part of a pre-indictment investigation of a drug conspiracy.[111] Law enforcement agents used a commercially available radio scanner to overhear the defendant's conversation. The court observed that "[t]hese signals can be intercepted with relative ease by standard AM radios."[112] The court likened the situation to cases involving conversations with government informants, finding that the defendant had assumed the risk of negating a legitimate expectation of privacy by "broadcast[ing] the conversation over radio waves to

105. *Id.* at 454–55 (O'Connor, J., concurring) (citations omitted).
106. *Id.* at 451–52.
107. 476 U.S. 227 (1985).
108. *Id.* at 236.
109. *Id.* at 238.
110. 47 F.3d 100 (4th Cir. 1995).
111. *Id.* at 101.
112. *Id.*

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

all within range who wish to overhear."[113] Similarly, in *McKamey v. Roach*,[114] the Seventh Circuit held that there was no reasonable expectation of privacy in a cordless phone conversation because "[the] communications are broadcast over the radio waves to all those who wish to overhear . . . [and] are easily intercepted."[115] These decisions rested on the fact that the information being exposed was accessible through standard household appliances in the general public use. Moreover, once captured with an AM radio, the radio signals required no specialized interpretation or analysis, since they were readily converted into an intelligible format.

Kyllo, the airplane flyover cases, and the cordless phone cases demonstrate that the crucial factor in assessing the legitimacy of a privacy expectation turns not on the fact that the information was disclosed to public, but that once disclosed, the public had a ready, generally available means to understand the information.

EXPECTATIONS, ACCESS, AND E-MAIL

The precedent discussed above suggests that a user's e-mail privacy turns on whether the public has general access to the electronic information obtained by the government. If so, then the user cannot have a legitimate expectation that the information will remain private. If the information is not readily accessible, it falls within a similar set of facts to *Kyllo*, where the information, though technically released into the public domain, was not intelligible by the public and hence implicated a reasonable expectation of privacy.

E-mail information stored on third party servers is difficult to access. The first possible way to obtain such information is through retrospective surveillance, defined as the retrieval of information from a third party server. There is a minimal possibility of regular human observation through such a method. Recall that in *Ciraolo* and *Riley*, members of the public could view the contraband from within public navigable airspace because civilian travel was common.[116] No analogous means exist for the public to view the streams of data sent over

113. *Id.* at 105.

114. 55 F.3d 1236 (6th Cir. 1995).

115. *Id.* at 1239–40.

116. Florida v. Riley, 488 U.S. 445 (1989); California v. Ciraolo, 476 U.S. 207 (1986).

the Internet because it cannot regularly access the servers hosted by third parties. Moreover, service providers usually attempt to safeguard such information from the public.[117] While computer hackers and other cybersecurity threats abound, the informational access theory does not seem to require a server be an impenetrable fortress, but merely that the reasonable person cannot, without violating applicable law, gain access to one. The thermal imager in *Kyllo*, after all, was commercially available at the time it was used.[118]

Even if third party servers were easily accessed, the layperson must be able to intelligibly interpret the information to overcome constitutional objections. The officers in the flyover cases were trained in marijuana detection, but the Court rejected this as a salient consideration, presumably because anyone could have seen the plants and figured out its species with a reference book.[119] A more difficult problem occurs when taking information off a server. Computer data in stored form does not appear as coherent letters, numbers, and images, but instead as an unintelligible stream of 1s and 0s. Even if a member of the public knew they were looking at an e-mail address, they would probably not immediately know that 01100010011011110110001001000000001100001 translated to "bob@aol.com" according to the American Standard Code for Information Exchange (ASCII).[120] In fact, in many cases this type of interpretation presents so much of a challenge that the government obtains the information directly from the service provider by court order.[121] A member of the public would therefore need analogous access to these tools in a generally available means, which does not seem possible given the current state of technology. To this extent, the information is as inaccessible as the heat signatures that required exotic equipment to detect in *Kyllo*, or the hypothetical satellite discussed in *Dow* that could yield a special, high-resolution

117. *See, e.g.*, Google Privacy Center: Privacy Policy, http://www.google.com/privacypolicy.html (last visited Oct. 18, 2007).

118. United States v. Kyllo, 190 F.3d 1041, 1044 n.4 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).

119. *Ciraolo*, 476 U.S. at 213 (1986) ("That the observation from aircraft was directed at identifying the plants and the officers were trained to recognize marijuana is irrelevant.").

120. Kerr, *Big Brother*, *supra* note 8, at 650.

121. *Id.* at 652.

image of the industrial curtilage. Because the layperson cannot access such information, it seems reasonable to conclude that an expectation of privacy could be found.

Unlike retrospective surveillance, prospective surveillance involves the capture of information while it is in transit over a network. However, the same confounds to general accessibility apply. To pass muster under the public access doctrine, a layperson would need to be able to view a section of a network in the same way that Ciraolo's backyard was exposed to passersby. This presents multiple problems because not only must the user find a way to physically connect to a particular network, but she must also overcome the various protocols designed to discourage hackers, such as anti-virus software, encryption codes, and system firewalls.

Even if there was regular access to the transmitted information, the resulting data would be meaningless unless one could interpret the information. Depending on the point of access, surveillance activity could yield a "full pipe" of information, similar to trying to listen to all the phone conversations going through a telephone switchboard at once.[122] A layperson would then need a filtering device to convert this data into intelligible information. One possibility is a special piece of software called a packet sniffer, which is programmed to look for a certain combination of 1s and 0s corresponding, for example, to a particular e-mail address.[123] The FBI has a special piece of software called "Carnivore" that it used for this purpose, and has installed black boxes containing computers running this software at the offices of various service providers.[124] This type of government activity is precisely the sort that *Kyllo* characterized as nonpublic conduct. Therefore, unless this type of software is made generally available, and the public regularly uses it, it seems

122. The FBI has abandoned its earlier packet sniffing device called Carnivore (later renamed DCS-1000) in favor of this full-pipe surveillance. Note this requires extensive computing capabilities, both to store all the information traveling through the network and later to apply a filter to recover the information that is necessary.

123. A commercial application is available for system administrators called "EtherPeek." It is, however, rather expensive, and has a specialized user interface. The only point in purchasing this software would be to administer a network. Wildpackets—Etherpeek—Family Overview, http://www.wildpackets.com/products/etherpeek/overview (last visited Oct. 18, 2007).

124. Kerr, *Big Brother*, *supra* note 8, at 654.

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

unlikely that the release of this information into a networked environment could defeat a Fourth Amendment constitutional claim.

OBJECTIONS

Three issues arise when talking about privacy expectations for e-mail. The first arises from the fact that the general public use cases discussed above seem to involve privacy around the home. This is a problem in the Internet context, since computer usage does not necessarily have a domestic boundary. The second problem relates to the Supreme Court's reluctance to recognize constitutional protections with respect to existing communications networks, in particular the postal mail and telephone systems. Finally, the privacy argument must contend with prior jurisprudence finding a waiver of constitutional protections when a matter is disclosed to third parties, such as through a business record. Each objection is considered in turn.

WHERE IS THE HOME?

Much of the case law cited in the previous section involves the veil of privacy surrounding the home, characterized in *Kyllo* as the "prototypical" area of privacy.[125] Arguably, the Internet surveillance context is different, because it involves information being sent *outside* the home. Support for this approach also comes from *Dow*, where the Court observed that industrial curtilage could not enjoy the same protections as domestic curtilage.[126]

There is reason, however, to limit the language in *Dow* and *Kyllo* discussed above. In the case of *Dow*, the petitioner argued that its exposed manufacturing facilities were analogous to the curtilage surrounding a home because every possible step had been taken to bar access.[127] The Court was simply addressing the petitioner's argument rather than articulating a requirement for the operation of the Fourth Amendment. This would be a significant repudiation of *Katz*, which suggested that the Framers did not intend the

125. Kyllo v. United States, 533 U.S. 27, 34 (2006).
126. Dow Chem. Co. v. United States, 476 U.S. 227, 233 (1985).
127. *Dow*, 476 U.S. at 236.

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

reasonableness analysis to be tied to specific places like the home or a telephone booth: "[T]he correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.'"[128] *Katz* also observed that "the Fourth Amendment protects people—and not simply 'areas.'"[129] Finally, the Court was willing to consider an informational access Fourth Amendment argument in *Riley*, which involved not a home, but an industrial chemicals plant.[130] The Supreme Court has also recognized reasonable expectations of privacy of private employees in the workplace.[131] The case law therefore does not suggest that a legitimate expectation of privacy can only be invaded in the home.

Additionally, it is not clear that Internet usage does not implicate the home in the first place to the extent that access occurs from within its confines. Arguably, the government would reach into the home if it were to search data over a network sent to or from a computer located in a home. In *Berger v. New York*, the Court suggested this type of "virtual presence" theory when it suggested that electronically bugging the defendant's telephone effectively placed a government agent inside the home.[132] However, there may be significant exceptions, such as the workplace,[133] and the fact that users often "surf" the Internet outside their homes via wireless networks. It is unlikely that the Supreme Court would find a Fourth Amendment interest in all forms of Internet communications in all instances.

POSTCARDS AND TELEPHONES

Another objection to protecting e-mail and remotely stored files relies on prior jurisprudence relating to postcards and telephone calls.[134] Conveying information over the Internet is

128. Katz v. United States, 389 U.S. 347, 350 (1967).

129. *Id.* at 353.

130. *See supra* notes 103–106 and accompanying text.

131. Mancusi v. DeForte, 392 U.S. 364, 369 (1968).

132. Berger v. New York, 388 U.S. 41, 64–65 (Douglas, J., concurring).

133. *But see* United States v. Ziegler, 474 F.3d 1184, 1190 (9th Cir. 2007), *cert. denied*, No. 07-6712, 2008 WL 59457 (U.S. Jan. 7, 2008) (finding defendant had a reasonable expectation of privacy in the hard drive contents of his workplace computer).

134. *See, e.g.*, Brief for Orin S. Kerr as Amicus Curiae Supporting Appellant, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238),

like the writing on a postcard or dialing a phone number, the argument goes, because it shares information with the operator of the network who processes, stores, and transmits this data. In the context of communications networks, the Supreme Court has found no privacy in the information on the exterior of an envelope[135] or in the numbers dialed over a telephone[136] precisely because this type of information is disclosed to the network provider. However, because the envelope is sealed, and a closed connection established after dialing and receiving an answer on the other end of the line, the courts have recognized a constitutional interest in the content of these communications.[137] Conversely, an e-mail is as constitutionally "open" as a conversation overheard on a public bus, because it lacks this last step isolating the communication from the outside world.

To counter this argument, it is necessary to consider several limitations of the analogy. The envelope information on a postcard is distinguishable from electronic communications because the exposure of this content information is a necessary byproduct of the instrumentality of communication. In other words, it would be impossible to protect the information on this type of mail from exposure to a postal worker who must read the address information to deliver the letter. Given that this type of reliance on human exposure is not present in the telephone or Internet cases, which rely on automated systems, it is not clear why a postcard provides a good analogy for packetized streams of data.

Is there a constitutionally relevant "exposure" when a machine reads electronic data? The problem with a machine-based exposure theory is that it would force courts to engage in difficult line-drawing to define when a mechanical "exposure" implicates a privacy interest. The challenge arises from the fact that the Internet is essentially a series of interconnected

---

2002 WL 32139374, at 6 [hereinafter Kerr, *Amicus*].

135. United States v. Huie, 593 F.2d 14, 15 (5th Cir. 1979) (no Fourth Amendment protection for the non-content envelope information on the exterior of postal letters).

136. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (no legitimate expectation of privacy in telephone numbers, e.g. pen register information).

137. *Berger*, 388 U.S. at 51 (recognizing a privacy interest in telephone conversations).

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

machines that all "read" the data they send and receive.[138] There can also be subsidiary processing steps that further complicate this question. For example, some web-based e-mail programs automatically "expose" an e-mail when they scan it for viruses.[139] A definition of exposure turning on human access provides the more workable standard while keeping prior jurisprudence relating to telephones intact, since the phone system also uses machines that "read" data in the form of dialing information.

Additionally, it is not clear that the phone and e-mail systems provide a persuasive analogy to communications over the Internet. Unlike these other forms of communication, the Internet does not separate information between envelope and content. In recognizing an absence of a Fourth Amendment interest in the case of pen registers, the Supreme Court specifically limited its holding to noncontent information based upon this distinction:

> [A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications. This Court recently noted: "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purpose of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[140]

A narrower analogy to the telephone system makes more sense. The telephone system and the Internet both rely on streams of data sent over networks. In the case of Internet access via DSL, the same network carries both voice and data and depends upon digital switching. Human exposure to content information is not necessary for the functioning of

138. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551–54 (2005).

139. *See id.* at 554 (suggesting a search should occur when digital information is exposed to human observation).

140. Smith v. Maryland, 442 U.S. 735, 741 (1979) (citing United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

either communications medium. It is therefore not clear why there should be a constitutional difference between streams of data flowing through the servers of an ISP and the streams of data flowing through a telephone switch. The best reading of *Berger* is not that Fourth Amendment legitimacy flows from the fact that the information cannot be detected by third parties, since this decision did not even discuss the fact that a phone call consists of a closed circuit between two callers.[141] Instead, the decision focused on the invasive nature of the government conduct at issue, suggesting a constitutional interest in private conversation.

E-mail, because it is not susceptible to this clear distinction, encourages a different approach. By focusing the constitutional inquiry on access to an undifferentiated body of information, courts can better analyze privacy expectations for electronic information transmitted over the Internet.

THIRD PARTY WAIVER

Expectations of privacy are not indestructible. *Katz*, for all its expansiveness in announcing a constitutional privacy interest, limited its holding to when "a person knowingly expose[d information] to the public."[142] The Court has been unwilling to find that a defendant retains a constitutionally cognizable expectation of privacy when exposing information in a manner potentially discoverable by the government. This waiver applies whether the defendant exposes the information herself or by entrusting the information to an unreliable third party.

Related to this general waiver theory is the business records exception to the Fourth Amendment. This theory holds

141. Kerr, *Amicus*, *supra* note 134, at 7.

142. Katz v. United States, 389 U.S. 347, 351 (1967). *Katz* cited two cases: *Lewis v. United States* involved a defendant inviting an undercover agent to his home to buy drugs. 385 U.S. 206, 211 (1967). In *United States v. Lee*, the defendant exposed containers of alcohol to government agents from the deck of his boat. 274 U.S. 559, 563 (1927). In both cases, because the defendant voluntarily shared the incriminating information, the Court found no reasonable expectation of privacy. *Lewis*, 385 U.S. at 212; *Lee*, 274 U.S. at 650. Relying upon similar reasoning, *United States v. White* rejected a motion to suppress testimony obtained from a government informant who relayed the contents of a conversation by wearing an electronic transmitter on his body. 401 U.S. 745, 748–54 (1971).

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

that information given over to a third party quashes an individual's reasonable expectation of privacy in that material. The paradigmatic case is *United States v. Miller*,[143] where the government subpoenaed the defendant's financial records from his bank.[144] The Court rejected the defendant's motion to suppress, holding that there was no intrusion into a zone of constitutional privacy.[145] The Court rejected the argument that the records were constitutionally protected "private papers" because the documents contained information voluntarily conveyed to the banks and were exposed to employees in the ordinary course of business.[146] The petitioner could not argue that he possessed or owned the information because they were the business records of the bank, which had a substantial stake in the "availability" and "acceptance" of those records.[147] The Court cited *White* for the proposition that the depositor took the risk that the information could be conveyed by the bank to the Government.[148] It reasoned along similar lines in *Couch v. United States*,[149] finding no expectation of privacy in records provided to an accountant for preparing a tax return.[150]

The Court extended this doctrine to the electronic context in *Smith v. Maryland*,[151] where the Supreme Court did not find a Fourth Amendment interest in information acquired by a pen register, a device that records dialed numbers.[152] The Court reasoned that because the devices were located at the phone company rather than the home, people must "know that they must convey numerical information to the phone company [and cannot] harbor any general expectation that the numbers they dial will remain secret."[153]

The system of electronic privacy protections established by Congress focuses on the mode through which communications

143. 425 U.S. 435 (1976).
144. *Id.*
145. *Id.* at 440.
146. *Id.* at 442.
147. *Id.* at 440.
148. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).
149. Couch v. United States, 409 U.S. 322 (1972).
150. *Id.*
151. 442 U.S. 735 (1979).
152. *Id.*
153. *Id.* at 743.

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

are transmitted.[154] Congress assumed that electronic communications and information stored with third parties was analogous to the business records cases outlined above.[155] Given that Congress has found the business records cases apposite authority, a legitimate privacy expectation would have to overcome the Supreme Court's reluctance to recognize one on similar facts.

But are the facts truly so analogous to the Internet context? There is at least a colorable argument that the answer to this question is no.[156] The first important difference has been termed the "independent interest" factor. The parties in the business records cases needed them for carrying out a specific task. The accountant in *Couch* needed the records for preparing a tax return. The bank in *Miller* needed to maintain the record for accounting purposes and tax audits. The Court noted that the banks rely on the acceptance and availability of these records.[157] Similarly, the dialed phone numbers in *Smith* were essential records to the phone company for connecting and billing purposes. The general proposition suggested by these cases is that because the parties had an interest in the information being sought by the government, they were free to share this with the authorities without implicating the constitutional rights of the defendant.

Electronic communications are distinguishable from the business record cases. E-mail information or remotely stored data is not a business record at all, since the business of operating a website or ISP does not require access to informational content, with the exception of the packet header. No revelation of the substance of the communication is required for a functional purpose like the accounting records in *Couch* and *Miller*, or the phone numbers for billing purposes in *Smith*.[158] The service provider acts as a conduit or a passive

154. Mulligan, *supra* note 53, at 1576–78.

155. *See* H.R. REP. NO. 99-647 (1986), at 23, 72–73.

156. *See* Mulligan, *supra* note 53, at 1579–82 (discussing the three proceeding factors).

157. United States v. Miller, 425 U.S. 435, 440–41 (1974).

158. In some cases, some "revelation" of the information does occur. For example, a service provider might automatically scan the contents of the e-mail to post a relevant advertisement, as is the case with the Google's e-mail service. However, the relevant point is that Google does not make a record of the contents of the e-mail or expose it to human view.

receptacle for the information sought to be protected. It makes no difference to the ISP, in other words, whether the e-mail contains a string of gibberish or a love letter.

A second crucial difference focuses on the voluntary nature of the disclosure. In *Couch* and *Miller*, the petitioner chose to give the information in exchange for some sort of service, i.e. accounting and banking. In *Smith*, the Court noted that the numbers were shared with the phone company in part because customers requested the phone company to track nuisance callers and consented to be billed. In all three cases, the information was imparted to the third party as the end result of the individual's actions. With e-mail, however, the user does not intend to allow the service provider to access the content information of the communication, and service providers take elaborate measures to maintain the privacy of their customers.

The final difference arises from the nature of the record itself. Both *Miller* and *Smith* suggested that the information contained in the record was not confidential. In *Miller*, the Court noted that the checks and deposit slips were "not confidential communications but negotiable instruments to be used in commercial transactions."[159] In *Smith*, the Court noted that the information exposed was *de minimis*, since the pen register only recorded phone numbers and did not reveal whether the parties actually communicated and what the parties may have communicated about.[160] Moreover, phone numbers are assigned by the telephone company, and can usually be found in a phone book. Courts should therefore make the same distinction between envelope and content information for e-mails, however problematic that may be, as they do in the case of telephone conversations.

What happens when information is exposed, but not readily accessible? Two doctrines seem in conflict: The general waiver cases[161] suggest there can be no expectation of privacy. On the other hand, if the information is exposed but inaccessible, it seems strange to find the information was available according to the public access doctrine. *Kyllo* seems to be the only Supreme Court case juxtaposing these two factors, and there the Court suggested that the inaccessible nature of the information was the determinative factor for

159. *Miller*, 425 U.S. at 442.
160. *See* Smith v. Maryland, 442 U.S. 735 (1979).
161. *See supra* note 142.

MANISH KUMAR. CONSTITUTIONALIZING E-MAIL PRIVACY BY INFORMATIONAL ACCESS. MINN. J.L. SCI. & TECH. 2008;9(1):257-286.

characterizing the governmental conduct as a search.

An Internet communication bears little resemblance to the information shared with third parties in *Couch*, *Miller*, *and Smith*. The Court's attempts to grapple with the constitutional status of information in *Kyllo* and its predecessors provide the better resolution to the constitutional questions presented by e-mail privacy.

IV. CONCLUSION

The particular issues raised by e-mail privacy draw attention to society's reliance on the rapid and unfettered dissemination of a broad range of information. In *Kyllo*, Justice Scalia observed the interrelationship between technology and privacy, writing, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[162] It is unclear, however, whether the Court's wariness toward the revelatory power of technology will extend to e-mail, because it is society, not the government, that has chosen to use this technology. The *Kyllo* line of cases suggests one way our increasingly digital lifestyles can receive the same sort of constitutional protections we take for granted in other contexts. To the extent that the reasonableness of an expectation of privacy for the contents of e-mail is far from certain, it suggests that the oftentimes unconditional embrace of technology, and its implications on ways of living, deserves our careful reflection.

162. Kyllo v. United States, 533 U.S. 27, 33–34 (2001).