Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act

Deirdre K. Mulligan

Berkeley Law

Follow this and additional works at: https://scholarship.law.berkeley.edu/facpubs

Part of the Law Commons

Recommended Citation
Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act

Deirdre K. Mulligan*

Many hailed the passage of the Electronic Communications Privacy Act of 1986 ("ECPA") as a victory for privacy. It created the statutory framework of privacy protections and related standards for law enforcement access covering electronic communications and remotely stored electronic records. Significantly, the ECPA established the standards that currently control law enforcement access to personal e-mail and electronic records, such as pictures and date books, stored on remote servers.

In 1986, relatively few people had Internet access; commercial electronic mail services and commercial data processing centers were emerging, but both primarily served the business community. The World Wide Web was barely a gleam in its creator’s eye. Today, increasing numbers of individuals have adopted the Internet for business and interpersonal communication and as a data repository. Millions of individuals use e-mail, chat, and "blog" on a daily basis. Individuals store personal photo albums, journals, and other

---

* Acting Clinical Professor of Law and Director of the Samuelson Law, Technology & Public Policy Clinic, Boalt Hall, School of Law, University of California at Berkeley. Many thanks to Jerry Berman and James X. Dempsey for the knowledge, information, and background on electronic surveillance and privacy issues they shared with me during our years of work together. Thanks to John Podesta for sharing his insight on the process and substance of the ECPA and for contemporaneous background materials. Many thanks to Patricia Bellia, Paul Schwartz, Peter Swire, Jennifer Urban, and Charles Weisselberg for their comments and suggestions. Thanks to Raechel Groom, Amalie Weber, and Laura Quilter for expert research assistance and comments on this draft. Many thanks to Pamela Samuelson for her guidance and support. Thanks as well to participants in the Boalt faculty workshop for helpful comments and feedback.


3 See infra notes 7–19 and accompanying text.

4 See infra notes 115–45 and accompanying text.

5 According to one study, “[o]n an average day, about 72 million American adults go online.” Pew Internet & Am. Life Project, Daily Internet Activities, http://www.pewinternet.org/reports/chart.asp?img=Daily_Activities_4.23.04.htm (last modified Apr. 23, 2004) [hereinafter Daily Internet Activities]. “[O]n a typical day,” of those on-line: forty-eight percent “[s]end e-mail” (February 2004); ten percent “[s]end an instant message” (February 2004); four percent “[c]hat in a chat room or in an online discussion” (June–July 2002); and one percent “[c]reate a web log or ‘blog’” (February 2004). Id.; see Julie Flaherty, Many Started Web Logs for Fun, but Bloggers Need Money, Too, N.Y. TIMES, Apr. 19, 2004, at C4 (noting there are an “estimated 2.1 million Web logs”).
information on commercial servers. In the eighteen years since the ECPA’s passage, we have witnessed an enormous growth in personal use of the Internet.

The increased personal use of the Internet to communicate and store communications and other personal electronic records, such as photos, diaries, and date books, raise questions about the adequacy of the privacy standards developed in 1986.

Two forces, one technical and one legal, influenced the privacy protections and law enforcement access standards found in the ECPA. First, multiple transitory copies of an e-mail’s content are created as it moves across the network from sender to recipient. The existence of static copies of the e-mail communication’s content, which can be accessed after the fact from entities not party to the communication, is distinct from traditional voice communications over a wire, which, because of its ephemeral nature, can only be accessed by eavesdropping in real-time or through the cooperation of a party to the communication. This technical distinction was important because as a practical matter it meant that the contents of a communication could be accessed at multiple points in time, from multiple parties, and at multiple locations. Second, this practical difference had the potential to influence the privacy afforded the contents of e-mail communications under the Fourth Amendment. A series of 1970s Supreme Court decisions (the “business records cases”) raised the possibility that these multiple copies of e-mails, in addition to electronic files that were intentionally placed on remote commercial servers for safekeeping, were wholly without Fourth Amendment protection. Broadly stated, these decisions were asserted to support the proposition that individuals have no protected privacy interest in personal information and records voluntarily disclosed to businesses. This broad interpretation, strongly supported by the law enforcement community during the consideration of ECPA, and at a time when present personal uses of the Internet were largely unforeseen, played an important role in shaping the privacy protections ultimately afforded to the content of electronic communications and remotely stored electronic records.

In this Article, I question whether the privacy standards set out in the ECPA provide adequate protection as a matter of policy and Fourth Amendment law. Part I discusses the genesis of the ECPA. Part II describes the privacy and law enforcement access provisions relevant to electronic communications and electronic records maintained on remote servers. Part III documents the increasing use of the Internet by individuals for personal purposes. Part IV examines the “business records cases” and identifies three principles that should limit their reach. Part V documents the way in which

---

6 Bob Tedeschi, You Ought To Be in Pixels, N.Y. TIMES, May 9, 2004, § 5 (Late Edition), at 4; David F. Gallagher, Site To Pour Out Emotions, and Just About Anything Else, N.Y. TIMES, Sept. 5, 2002, at G6; see also Anne Eisenberg, What’s Next; Memories as Heirlooms Logged into a Database, N.Y. TIMES, Mar. 20, 2003, at G6 (discussing MyLifeBits project at Microsoft, “software for an electronic diary that can keep track of a multitude of everyday details in a person’s life—the e-mail sent, the family photographs taken, the phone calls made, the Web pages visited—in a single database”).

7 See infra notes 115-45 and accompanying text.
ECPA's reliance on the "business records cases" as a point of departure ignores these limiting principles and is in tension with other areas of Fourth Amendment law. The Article concludes that given the current personal use of the Internet, key provisions of ECPA no longer adequately protect privacy as a matter of public policy and constitutional law, recommends that ECPA be revised, and suggests several provisions that are ripe for constitutional challenge.

Today, millions of U.S. individuals are using electronic mail for personal communications and storing personal effects such as family photos, diaries, and date books on the Internet. The changed ways in which people use the Internet, enabled by new technical standards, laws, and business models, have exposed fundamental weaknesses in the structure of the ECPA. Many who supported the statute would agree that it has failed to keep pace with changes in and on the Internet and therefore no longer provides appropriate privacy protections. It is time to revisit and revise ECPA to establish appropriate privacy protections that respect individuals' expectations and constitutional requirements.

I. The Genesis of the Electronic Communications Privacy Act

By the mid 1980s, there was a growing consensus among members of Congress, the telecommunications and computing industry, and civil libertarians that advances in telecommunications, such as wireless telephones and e-mail, were outpacing existing privacy protections for communications and stored electronic records. By 1986, the business world had begun to use the Internet actively. While most small business owners remained unfamiliar with electronic mail, there were signs of change. The year 1985 saw new entrants, such as AT&T, poised to leverage their substantial telephone wire markets to enter the modest $300 million dollar electronic mail market, which was expected to nearly triple to $882 million during the following three years. This proliferation of electronic mail affected the security of com-

---

8 See Hearing Before the Subcomm. on Patents, Copyrights, and Trademarks, Electronic Communication Privacy of the Senate Comm. on the Judiciary, 99th Cong. 130-31 (1985) (prepared statement of Jerry J. Berman, on behalf of the American Civil Liberties Union ("ACLU"); Civil Liberties and the National Security State: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary, 98th Cong. (1984); Office of Tech. Assessment, U.S. Congress, Electronic Surveillance and Civil Liberties (1985) [hereinafter OTA REPORT]; Priscilla M. Regan, Legislating Privacy: Technology, Social Values and Public Policy 131 (1995) (discussing the formation of the Privacy and Technology Project of the ACLU and the consultations between privacy groups, technology experts, business groups, and congressional staff, and documenting the three conclusions of the consultations). In addition, Jerry Berman, the director of the ACLU's Privacy and Technology Project was the director of the Center for Democracy & Technology while the author worked there from 1994-2000, and the history of ECPA was a topic of frequent conversation.

9 Pacific Bell Survey: Small Business Slowly Adapting to Information Age, COMMUNICATIONS DAILY, July 24, 1985, at 3.

pany-held data.¹¹ Users increasingly downloaded files to microcomputers or spread them throughout the office via e-mail, rendering confidential information—which had been relatively well protected on mainframe computers—virtually unguarded.¹² Computers in 1986 were not nearly as powerful as their modern counterparts.¹³ Businesses frequently chose to outsource data processing and storage, creating concerns about the legal protections afforded outsourced data. By 1986, "businesses of all sizes—hospitals, banks and many others—used remote computing services."¹⁴ The primary means of transmitting data to these services was electronic communications.¹⁵

While businesses were beginning to use the Internet in 1986, the consumer market was nascent. In 1984, personal computers were in a mere five percent of households.¹⁶ Few individuals had Internet access at home.¹⁷ The first noncommercial, recreational bulletin board system (with chat, e-mail, and an announcements page), the WELL (Whole Earth 'Lectronic Link; www.well.com), came online in 1985.¹⁸ In 1986, it had fewer than 2000 sub-

---

¹¹ David Churbuck, *Potential Electronic-Mail Users Await Standard*, PC WEEK, April 22, 1986, at 147 ("About 140 million messages were sent through public electronic-mail systems last year, generating about $300 million in revenue for a crowded, competitive industry.").

¹² Mitch Betts, *Safeguarding Privacy MIS Confronts a Sensitive Challenge*, COMPUTERWORLD, July 7, 1986, at 53–54 (noting that "a trend toward end-user computing means that access to confidential information is spread to people who lack the data processing professional's instincts for data privacy and security, according to the OTA's final report, 'Automation of America's Offices'").

¹³ Ken Polsson, *Chronology of Workstation Computers*, at http://www.islandnet.com/~kpolsson/workstat/ (last modified September 11, 2003). Polsson writes that in January of 1986: IBM announces the IBM RT Personal Computer, using RISC-based technology from IBM's "801" project of the mid-70s. It is one of the first commercially-available 32-bit RISC-based computers. The base configuration has 1 MB RAM, a 1.2 MB floppy, and 40 MB hard drive, for US$11,700. With performance of only 2 MIPS, it is doomed from the beginning.


¹⁵ Id.


scribers.19 E-mail links to commercial mail carriers, such as MCI Mail and Compuserve, would not be available until 1989.20

Concern with the viability of this growing, primarily business market led business, civil liberties organizations, and policy-makers to focus on the need for appropriate privacy protections.21

Fueling the privacy concerns around electronic communications was a pending case in which the government sought backup copies of customer e-mail messages kept on computer tapes by an early e-mail service provider, Source Telecomputing Co. ("Source").22 The Assistant U.S. Attorney issuing the subpoena argued that such backup copies were akin to carbon copies of business letters kept in a corporation's file and deserved no privacy protection under the Fourth Amendment.23 Source fought the subpoena, arguing that if the U.S. Attorney's position was correct, it was "the complete destruction of the expectation of privacy."24 Because the defendant plead guilty, the court did not rule on the issue.25

Concerns about the lack of privacy protection for electronic communications and information in electronic storage stemmed from two sources. First, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),26 creating a statutory right of privacy in oral and wire communications, predated the advent of electronic communications. Written in 1968, the statute was directed at the "aural acquisition" of voice communications that passed, at least in part, over a wire.27 The wiretap provisions of Title III authorized law enforcement wiretapping of telephones within a framework designed to protect privacy and compensate for the uniquely intrusive aspects of electronic surveillance.28 Title III requires law enforcement to obtain what has been referred to as a "superwarrant" before intercepting phone conver-

20 Zakon, supra note 18.
21 REGAN, supra note 8, at 135–37.
22 See William C. Rempel, Computer Age Gaps; Privacy Law: Race to Pace Technology, L.A. TIMES, May 14, 1985, at A1; see also OTA REPORT, supra note 8, at 50.
23 See Rempel, supra note 22.
24 See id.
25 See id.
26 Wire and Electronic Communications Interception and Interception of Oral Communications, Pub. L. No. 90-351, 82 Stat. 197 (1968) (current version at 18 U.S.C. §§ 2510–2522 (2000)). Title III was passed in response to two Supreme Court decisions, one holding that wiretapping was a search and seizure subject to the strictures of the Fourth Amendment, and the other finding a New York state statute regulating the use of wiretaps by law enforcement to be deficient. Katz v. United States, 389 U.S. 347, 353 (1967) (finding that wiretapping a private conversation in a phone booth is a search governed by the Fourth Amendment); Berger v. New York, 388 U.S. 41, 63 (1967) (striking down state statute allowing eavesdropping based on ex parte order of the Court).
27 18 U.S.C. § 2518(1) (setting forth the definition of "intercept" as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device"); see United States v. Hall, 488 F.2d 193, 197 (9th Cir. 1973) (holding that a call must travel in part by wire to be covered by Title III).
While instinctually individuals using e-mail may have expected protections against interception to extend to this new means of communicating, courts had found that a literal reading of the statute did not provide protection. Electronic mail and data are not "oral" communications, nor are they subject to "aural" acquisition. Any prohibition on intercepting electronic communications would thus have to be based on the Fourth Amendment itself.

Unfortunately, the scope of Fourth Amendment protection that would be available for electronic mail and for remotely stored records was unclear due to a string of Supreme Court cases, the "business records cases," finding that records of individuals' transactions—including tax records, bank records, and telephone toll records—maintained by business entities were outside the scope of Fourth Amendment protection. The business records cases stand for the proposition that personal information voluntarily disclosed to a business is outside the scope of the Fourth Amendment. Businesses, it is argued, are therefore free to turn such information over to the government. The government may request or subpoena such information without informing the individual whose information is sought and without meeting the procedural and substantive requirements of the Fourth Amendment.

For technical reasons, the business records cases were potentially quite troubling for electronic mail. Unlike ephemeral telephone communications, electronic communications require the creation of contemporaneous records. As it flows from sender to recipient, the content of the communication is handled by a series of routers that are owned by many different

---


30 See United States v. N.Y. Tel., 434 U.S. 159, 166–68 (1977) (holding that conversation must be capable of being overheard to be covered by Title III); Hall, 488 F.2d at 196–98 (holding that conversation must travel in part by wire to be covered by Title III).

31 Data communications occur only in digital form that cannot be acquired aurally. See OTA REPORT, supra note 8, at 49.

32 See N.Y. Tel., 434 U.S. at 168–69 (finding that because pen registers are not governed by Title III, court has authority to authorize their installation pursuant to the Fourth Amendment); Hall, 488 F.2d at 198 (holding that interceptions of communications not governed by Title III must meet Fourth Amendment requirements). See generally OTA REPORT, supra note 8.


34 See Smith, 442 U.S. at 744; see also Miller, 425 U.S. at 442.

35 See Smith, 442 U.S. at 744; see also Miller, 425 U.S. at 443.

36 See Smith, 442 U.S. at 745–46; see also Miller, 425 U.S. at 444.

37 See generally OTA REPORT, supra note 8.

entities. As the communication traverses the network, it leaves replicas of itself, in whole or in pieces, in the hands of any number of third parties. Once a message arrives at the server associated with the recipient’s service provider, it remains in storage until it is retrieved. The messages generally travel in clear text, meaning that they can be read by those who handle them. Once retrieved by the recipient, it may be deleted from the service provider’s mail server, or it may remain there because the recipient keeps mail on the service provider’s server rather than on a local drive, or it may remain on the server in the form of a backup copy. While the Fourth Amendment clearly protected the contents of a private oral conversation occurring outside the confines of the home over a telephone network, it was unclear whether the copies of e-mail left behind on the network or the e-mail, or back-up copies, maintained on an e-mail service provider’s server would be considered devoid of Fourth Amendment protection under the business records case law.

Equally troubling was the likely lack of privacy protections for other electronic records intentionally stored on third-party servers used by banks, hospitals, and other businesses. The dominant thinking at the time of ECPA’s passage was that electronic records that were handed over to a third party for storage on remote servers would be controlled by the business records cases and found lacking Fourth Amendment protection.

Against this backdrop of uncertain legal status for electronic communications and other records processed and housed on servers owned by third parties, the desire to clarify the level of legal protection was high. Concerned that privacy protections and law enforcement access standards might not be clear in relation to burgeoning electronic communications, the House Committee on the Judiciary and the Senate Committee on Governmental Affairs asked the Office of Technology Assessment (“OTA”) to undertake a study to explore the threat to civil liberties posed by unregulated intrusions into electronically transmitted communications. OTA’s report, Electronic Surveillance and Civil Liberties, published in 1985, found, among other things, that

- data communications between computers were not protected by existing statutes;
- electronic mail messages were subject to interception at several points; and,

40 See generally OTA REPORT, supra note 8; Steere, supra note 38, at 247–49 (discussing e-mail technology).
41 See, e.g., ACLU v. Reno, 929 F. Supp. at 834.
42 See REGAN, supra note 8, at 132 (“By this time in the process, there was virtually no disagreement about the problems that were identified in the OTA report. Indeed, almost all of the other witnesses testifying before the subcommittee used the OTA report as their point of departure. At the congressional hearings, it was generally agreed that Title III needed to be updated.”).
43 See OTA REPORT, supra note 8, at 45.
44 Id.
45 Id. (finding that electronic mail messages could be intercepted: “1) at the terminal or in
• existing law provided little or no protection at most of these points.46

The OTA report proposed three policy options for congressional consideration to address the privacy of electronic mail.47

The first alternative afforded e-mail the same level of protection as conventional first-class mail. Law enforcement would require a warrant based on probable cause to access content and a court order based on a lesser test to authorize access to the addressing information (the equivalent of a mail cover).48 In addition, this option would include a general prohibition against interception (by amendment of Title III), and the adoption of the "Subscriber Privacy" provisions of the Cable Communications Policy Act of 198449 to limit corporate use of individuals' personal information.50

The second option required a probable-cause-based warrant for access to e-mail at the sender's terminal and the recipient's mailbox, but would leave the courts to resolve the scope of Title III's prohibition against interception of aural communications and the scope of protection afforded e-mail held by service providers and intermediaries.51 The rationale of the latter is that Congress might want all personal information held by third parties to receive uniform treatment.52

Finally, the last proposal suggested that Congress do nothing and see how the Court and markets respond.53

Interestingly, the OTA report did not consider, or make recommendations on, the remote storage of electronic records on third-party servers generally.54 Instead, it covered only electronic mail.

In 1986, Congress adopted the ECPA,55 amending Title III to generally extend the prohibitions on interception to e-mail and crafting new protections for stored communications and stored records held by third parties.56 Congress designed the Act to protect privacy interests in the emerging realm of electronic communication services and remote electronic processing and storage of information.57 As to e-mail, Congress charted a fourth alternative to the OTA's recommendations, choosing to require a probable-cause-based warrant for access to e-mail at the sender's terminal and recipient's mailbox, but creating a scheme of weaker protections for e-mail held by service prov-

the electronic files of the sender, 2) while being communicated, 3) in the electronic mailbox of the receiver, 4) when printed into hardcopy, and 5) when retained in the files of the electronic mail company or provider for administrative purposes ").

46 Id.
47 See id. at 51-52.
48 See id. at 51.
50 OTA REPORT, supra note 8, at 51.
51 Id. at 52.
52 Id.
53 Id.
54 Id.
57 See S. REP. No. 99-541, at 1.
iders and intermediaries. The backdrop, as discussed above, clarifies that the ECPA was both a proactive and reactive statute.\textsuperscript{58} It was a proactive effort to provide a predictable privacy framework, spurred by the recognition that individuals would be reluctant to use new technologies unless privacy protections were in place.\textsuperscript{59} At the same time, the ECPA was a reactive piece of legislation.\textsuperscript{60} It was to no small degree an effort to head off the possibility of courts concluding that the Fourth Amendment did not protect electronic communications and electronic records on third-party servers. Civil liberties organizations, computer and communications companies, and law enforcement supported the ECPA’s passage.\textsuperscript{61}

\section*{II. The Structure of the ECPA}

The body of electronic surveillance laws created by the ECPA breaks down into three statutes: the Wiretap Act, 18 U.S.C. §§ 2511–2522;\textsuperscript{62} the Pen Register statute, 18 U.S.C. §§ 3121–3127;\textsuperscript{63} and the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701–2711.\textsuperscript{64} The Wiretap Act and Pen Register statute regulate prospective surveillance of Internet communications (communications “in transit”),\textsuperscript{65} and the SCA governs retrospective surveillance (stored communications).\textsuperscript{66} Each of the titles operate in the same basic way:

\begin{itemize}
\item \textsuperscript{58} See supra text accompanying notes 8–54.
\item \textsuperscript{59} See \textit{Regan}, supra note 8, at 136–37 (discussing congressional testimony articulating the risk to businesses and society if Congress failed to establish clear privacy rules for e-mail: “lack of clear standards for the disclosure of electronic mail information retards not only the growth of our industry, but the productivity of the entire economy”).
\item \textsuperscript{60} See \textit{supra} text accompanying notes 30–41 (discussing court cases interpreting Title III and outlining business records cases).
\item \textsuperscript{63} 18 U.S.C. §§ 3121–3127 (2000).
\item \textsuperscript{66} See 18 U.S.C. § 2701 (Stored Communications Act). A recent First Circuit decision may destroy the applicability of the Wiretap Act to electronic communications altogether by calling into question when an electronic communication is “in transit.” See United States v. Councilman, 373 F.3d 197 (1st Cir. 2004). In \textit{Councilman}, the court held that communications temporarily in the random access memory (RAM) on their way to the recipient are in electronic storage. \textit{Id.} at 200–04. The court rejected the Justice Department’s argument that “the legislative history
generally prohibiting unauthorized access to communications and other personal information, but permitting specified exemptions, one of which provides the government with the ability to obtain direct access or to compel a third party to turn over information.

The Wiretap Act and Pen Register statute break down the world of prospective surveillance into two broad types: surveillance of content and surveillance of noncontent information, respectively. To a large degree, the Wiretap Act extended the protections of Title III to the in-transit interception of wireless voice communications and to nonvoice electronic communications, most importantly for our purposes, e-mail. The Wiretap Act addressed a range of rulings that had limited the reach of Title III to exclude coverage of voice communications over new media and to information in digital form. These additional protections cover electronic communications in transit over all networks, including private and common carriers. The ECPA, however, did not extend all of Title III's protections to electronic communications. Unlike Title III, which restricts the use of wiretaps to a limited list of crimes, court orders authorizing interceptions of electronic communications can be based upon the commission of any federal felony. While constitutional challenges to the introduction of information obtained in violation of the ECPA may succeed, the ECPA contains no statutory exclusionary rule for wrongfully acquired electronic communications. Regardless of these important variations, the Wiretap Act provides strong privacy protection for e-mail while it is in transit, requiring law enforcement to obtain a warrant-like order based on probable cause to access it.

Based on the Supreme Court's holding in Smith v. Maryland that telephone numbers were not covered by the Fourth Amendment, the Pen Register statute established weak protections for transactional data generated by regular phone calls. This was, of course, a direct response to Smith and reaffirms the distinction between privacy expectations in relation to phone numbers and content. The USA PATRIOT Act ex-
pen registers and trap and trace devices, which capture outgoing and incoming phone numbers respectively. To obtain a pen register order, the government must merely certify that it believes "the information likely to be obtained [by installation of the pen/trap device] is relevant to an ongoing criminal investigation." So long as the issuing court has jurisdiction over the offense being investigated, and the government has made the appropriate certification, the court must authorize installation and use of the device anywhere in the United States.

The SCA covers retrospective surveillance of both content and non-content information. The SCA covers the area where Congress had the least guidance from the Court and where the technical differences between electronic data and voice communications are most pronounced. It established rules governing law enforcement access to subscriber-identifying information, transactional data about a subscriber's use of the service, and the content of electronic communications that are maintained either "incident to transmission" or in general storage. Transactional data is broken down into two categories: basic subscriber information, and records or other information pertaining to the subscriber. Content information is the actual information stored in the account. Such information is broadly defined to include "any information concerning the substance, purport, or meaning of that communication."

In 1986, networked computing services were used for two dominant purposes: (1) individuals, primarily academics, military personnel, and some business people, used computing services to send and receive electronic

---

75 Id. § 3122(b)(2); see also CCIPS MANUAL, supra note 29, ch. 4.C.2.
76 18 U.S.C. § 3127(2); see also CCIPS MANUAL, supra note 29, ch. 4.C.2.
77 18 U.S.C. § 3123(a)(1); see also United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (noting that "the judicial role in approving the use of trap and trace devices is ministerial in nature"); CCIPS MANUAL, supra note 29, ch. 4.C.2.
79 Id. § 2703.
80 Basic subscriber information includes:
   "name, address, local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment of such service (including any credit card or bank account number)."
   Id. § 2703(c)(2).
81 Id. § 2703(c)(1) (defining the scope of application to include "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications")). This category functions as a catchall for transactional information other than subscriber information. CCIPS MANUAL, supra note 29, ch. 3.C.2.
communications such as e-mails; and (2) businesses, and perhaps a few individuals, outsourced large computing tasks. The SCA provides two different levels of protection to the content of electronic communications. The variations in the protection reflect this bifurcated view of electronic communications. The level of protection varies depending upon whether the content is held by an “electronic communication service,” in “electronic storage,” or like other records, by a “remote computing service.” The provisions, however, do not apply to electronic communications held by a private company that does not provide electronic communication services to the public (for example, an employer that stores employee e-mail on its servers). The SCA thus divides the world into three groups of networked computing service providers: electronic communication service (“ECS”) providers, remote computing service providers (“RCS”), and service providers that fall into neither category (all other businesses).

The classification of the entity maintaining an electronic communication is a central factor in determining the law enforcement access standards under ECPA. A service provider can only be an ECS if it provides another with the ability to send or receive wire or electronic communications. In contrast, a “remote computing service” provides to the public a service that transmits, and stores or processes communications. In short, an ECS provides a service that supports communications by others, while an RCS provides a service that supports communications to its systems that either store and/or process information on the senders’ behalf. If an electronic communication is held by an ECS, the next step in determining the standards for law enforcement is to ask whether the communication is in “electronic storage.” “Electronic storage” is defined as “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.” An electronic communication is in “electronic storage” when it is at an intermediate point on its way to its final destination. The final question deter-

---

85 As discussed supra Part I, it implicitly created three levels by leaving some electronic communications outside its reach.
86 See CCIPS MANUAL, supra note 29, ch. 3.B.
88 “[E]lectronic communication service” is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15) (2000).
93 See, e.g., Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 442-43 (W.D. Tex. 1993), aff’d, 36 F.3d 457 (5th Cir. 1994) (finding that the Secret Service and the government had not violated the Wiretap Act because their seizure did not constitute an “interception”
Reasonable Expectations in Electronic Communications

mining the coverage for an electronic communication held by an ECS is whether it has been in storage for more than 180 days.

For example, e-mail that has been received by a service such as Yahoo! but has yet to be opened by its intended recipient would clearly be in "electronic storage" and Yahoo! would be a provider of ECS for that e-mail. For another e-mail addressed to the same subscriber but already opened by the intended recipient, it is unclear whether Yahoo! would be an ECS or, as the Department of Justice ("DOJ") asserts, an RCS provider, or whether it would fall outside of the SCA all together. While the message is no longer in storage incident to transmission, it may still be considered as maintained for backup protection, as one circuit court recently held, and therefore still considered to be in "electronic storage." On the other hand, because the message is no longer on its way to its final destination it may be, as the DOJ contends, that the message should be considered to now be held in storage for the recipient by an RCS. Given that when Congress was drafting the SCA, e-mail had to be actively moved into storage if it was to be maintained longer than a few months, it may be that an e-mail retained on the server of an electronic communication service provider simply falls outside the scope of the SCA. Finally, consider the initial e-mail being held but not opened for 180 days. Under the SCA it is now available to law enforcement under the lower standards governing access to electronic communications held by an RCS. Note, however, that if the service provider, instead of being Yahoo!, were a private company providing e-mail service to its employees, it would not become an RCS provider for a saved e-mail message because it does not provide services to the public. In this instance, the e-mail would certainly fall completely outside the ECPA's framework.

The SCA rules governing access to the contents of stored electronic communications differ dramatically from the protections provided for those same communications while in transit. Under the SCA, the government can compel production of basic subscriber information and any communications that are not protected under the ECPA generally by means of any trial or administrative subpoena. For all other information held by electronic

under the terms of the Act, as "interception" of a message in electronic storage is not "contemporaneous acquisition of the communication").

94 See generally CCIPS MANUAL, supra note 29.
95 See Theofel v. Farey-Jones, 341 F.3d 978, 984-85 (8th Cir. 2002).
96 The rationale for this is that when the SCA was passed electronic communication services and remote computing services were two distinct offerings. Although considering e-mail held for greater than 180 days by an ECS as covered under provisions applicable to RCS's does prevent such e-mails from falling out of the statute, it is not clear that this is what the statute requires.
97 See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting "providing . . . to the public" to exclude an internal e-mail system that was made available to a hired contractor but was not available to "any member of the community at large").
98 See CCIPS MANUAL, supra note 29, ch. 3.D.1.
99 Id. For example, opened e-mails stored by a private company not offering services to the public, or information belonging to a person who is not a "subscriber" or "customer," are not generally protected under the ECPA. Organizacion JD Ltda. v. U.S. Dep't of Justice, 124 F.3d 354, 359-61 (2d Cir. 1997) (discussing the scope of the word "customer" in the context of the ECPA).
communication services, the stored communication provisions of the ECPA set out a complicated set of substantive and procedural protections.\textsuperscript{100} The substantive standards and procedures for law enforcement access to e-mail weaken as the e-mail ages on a third party’s server. Following the discussion in the previous paragraph, under the SCA, the only instance in which a government official is clearly required to meet the probable cause standard of the Fourth Amendment and obtain prior judicial approval is where she seeks access to unopened e-mail residing with an ECS for less than 180 days.\textsuperscript{101} And even when the government seeks copies of a person’s e-mail messages from the Internet service provider (“ISP”) server where they sit waiting to be read, an ordinary search warrant is sufficient under the SCA without the Wiretap Act’s special protections of minimization, judicial supervision, and notice.\textsuperscript{102} The search warrant need only be issued by a federal court with jurisdiction over the offense under investigation, even if the records are held in another district.\textsuperscript{103} Once the warrant is obtained, it is served upon the third-party holder of the information much like a subpoena.\textsuperscript{104} Unlike other methods of compelling the disclosure of e-mail discussed above, the warrant process does not require notice, prior or delayed, to be given to the individual.\textsuperscript{105} If an e-mail message is held by an RCS provider or an ECS provider for more than 180 days the government may access it pursuant to a subpoena if it provides notice to the subscriber or customer, or complies with the delayed-notice provisions of 18 U.S.C. § 2705(a).\textsuperscript{106} The standard for issuing a subpoena is mere relevance and many subpoenas are issued without any judicial oversight.\textsuperscript{107} Information can be turned over without notifying the subscriber under the delayed notice provisions if a supervisory official certifies that notification would jeopardize a pending investigation or endanger the life or physical safety of an individual.\textsuperscript{108}


\textsuperscript{101} The DOJ argues that opened contents are accessible under the lower standards discussed above, asserting that once an e-mail has been opened it is no longer in “electronic storage” and is therefore covered, if at all, under the RCS provisions. See supra note 94 and accompanying text.


\textsuperscript{103} See CCIPS MANUAL, supra note 29, ch. 3.D.5 (noting state courts may also issue warrants under 2703(a), but the effects of such warrants are limited to territorial jurisdiction of the court).

\textsuperscript{104} See United States v. Bach, 310 F.3d 1063, 1066–67 (8th Cir. 2002) (discussing process of serving court order).


\textsuperscript{106} Id. § 2703(b).

\textsuperscript{107} Subpoenas that may be used under this provision of the SCA include “administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena.” Id. § 2703(b)(1)(B)(i). Administrative subpoenas are typically authorized by someone within the agency seeking the information and involve no judicial review. See generally Office of Legal Policy, U.S. DEP’T OF JUSTICE, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES: PURSUANT TO PUBLIC LAW 106-544 (2002), http://www.usdoj.gov/olp/intro.pdf.

\textsuperscript{108} 18 U.S.C. § 2705(a); see also CCIPS MANUAL, supra note 29, ch. 3.D.2.
According to the DOJ, even within the initial 180-day time period, the protections weaken depending on whether the e-mail has been opened or remains closed. The conclusion that opened mail, less than 180 days old, held by an ECS is accessible without a warrant was rejected by a Ninth Circuit ruling finding that such messages fit neatly within the definition of "electronic storage" because they are held for backup and therefore require a warrant for law enforcement access; this interpretation, however, is at odds with other case law. This contrasts with the protection afforded an e-mail message stored on a home computer, which is covered by the Fourth Amendment regardless of whether it is opened or unopened and no matter how long it is kept. Under the dominant interpretation of ECPA, a large quantity of personal e-mail—everything except unopened e-mail, according to DOJ's interpretation, 180 days old or younger—can be accessed with a subpoena issued on a relevance standard, without judicial oversight, and at times without contemporaneous notice to the individual whose e-mail is being seized.

III. Changing Uses and Reasonable Expectations

Whenever I tell a layperson, or even a lawyer unfamiliar with electronic privacy laws, that the protections for e-mail vary depending upon the duration and location of its storage and whether it has been opened, and that the statutory protections afforded their remotely stored private Web diary or calendar falls short of Fourth Amendment protections, they look at me with

---

109 CCIPS MANUAL, supra note 29, ch. 3.D.3. The current edition of the CCIPS manual and the primary author of the 2001 edition, Orin S. Kerr, offer a functional approach to ECPA's construction. Under this construction of the ECPA, the analysis of the appropriate standard for government access to an e-mail turns on the definition of "electronic storage" which in their construction is limited by § 2510(17)(A) to communications in "temporary, intermediate storage," "incidental to the electronic transmission." CCIPS MANUAL, supra note 29, ch. 3.B. ("As a practical matter, whether a communication is held in 'electronic storage' by a provider governs whether that service provides ECS with respect to the communications. The two concepts are coextensive: a service provides ECS with respect to a communication if and only if the service holds the communication in electronic storage. Thus it follows that if a communication is not in temporary, intermediate storage incidental to its electronic transmission, the service cannot provide ECS for that communication. Instead, the service must provide either 'remote computing services' . . . or else neither ECS nor RCS.").

110 Theofel v. Farey-Jones, 341 F.3d 978, 984–85 (9th Cir. 2003).

111 Because subsection (A) applies only to messages in "temporary, intermediate storage," several courts have limited the coverage of 18 U.S.C. § 2701(a)(1)(B) to messages not yet delivered to their intended recipient. See In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001) (finding that "long-term residence" of cookies on hard drives take them outside the "temporary, intermediate storage" definition of "electronic storage" under the ECPA); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d, 623, 636 (E.D. Pa. 2001) (finding 18 U.S.C. § 2510(17) covers undelivered e-mail in temporary storage prior to retrieval by the recipient as well as "back-up protection storage" in the event the system crashes before transmission is completed).

112 In the alternative, a government official may use a § 2703(d) court order, which requires the governmental entity to offer "specific and articulable facts showing there are reasonable grounds to believe" that the e-mails are "relevant and material to an ongoing criminal investigation" and provide notice or meet the delayed-notice requirements of 18 U.S.C. § 2705(a). 18 U.S.C. § 2703(d) (2000 & Supp. 2001); 18 U.S.C. § 2711(3); see United States v. Kennedy, 81 F. Supp. 2d 1103, 1109–10 (D. Kan. 2000) (holding that a conclusory application for a § 2703(d) order did not meet the requirements of the statute); CCIPS MANUAL, supra note 29, ch. 3.D.3.
disbelief. While clearly not a rigorous assessment, I believe their disbelief is indicative of a major gap between society's expectation of privacy and the privacy provided by current statutory law.

One reason for the current disconnect between privacy expectations and the statutory protections of the ECPA is that Congress was drafting legislation in the early stages of a technology that has fundamentally changed the way we communicate, store, and use information. E-mail links to commercial mail carriers, such as MCI Mail and Compuserve, would not be available until 1989. The first commercial provider of Internet dial-up access would not emerge until 1990. The World Wide Web and Web browsing functionality was released in 1991. The first cyberbank came online in 1994, at the same time electronic commerce sites began to appear. Private companies would not fully host the Internet backbone until 1995. Congress, with good reason, did not envision the pervasive role communications technology would come to play in our daily lives. Congress was, however, far from alone in its perspectives; the pace of technology and the inventive uses to which it has been put continues to challenge many, including those in the legal arena.

The importance of e-mail and the use of the World Wide Web, particularly for personal use, for example, were not in Congress's sights. Congress did not envision a time when the private sphere of personal communications and interactions would extend beyond the end-points (the computer in the home, on the desktop, or in the office) and into the medium itself (Web sites, blogs, chat, search engines). The thought of life occurring within the medium itself was foreign. No prior technology had been called a "place," but this became an accepted, and now debated, label for the Internet: we speak of "cyberspace" as casually as we speak of parks, malls, or art galleries.

Today, sixty-three percent of U.S. adults—126 million people—use the Internet. Internet users are found in every segment of the population. In-

---


114 Zakon, supra note 18.

115 Id. (noting that "[t]he World comes on-line (world.std.com), becoming the first commercial provider of Internet dial-up access").

116 Id.


118 See generally Orin Kerr, The Problem of Perspective in Internet Law, 91 GEO. L.J. 357 (2003) (discussing how different perspectives about the "Internet's facts" can lead to confusion in applying the law to the Internet).


120 PEW INTERNET & AM. LIFE PROJECT, AMERICA'S ONLINE PURSUITS: THE CHANGING PICTURE OF WHO'S ONLINE AND WHAT THEY DO (2003), http://www.pewinternet.org/reports/
Individuals use the Internet to communicate with friends, family, and colleagues. They use it to seek out information about every imaginable topic. They use it to store photos, documents, and diaries. They use it to organize rallies and demonstrations. Individuals use it to shop, to bank, and to barter. They use it from home and from work, and for work and for play.

The information flowing across the Internet reflects this diversity of activity. Broken into tiny packets of data, text, voice, sounds, and images flow...
across the Internet backbone.\textsuperscript{125} Forty-three million individuals in the United States reported that they listened to music online in 2001.\textsuperscript{126} On a typical day, over 7.5 million individuals will listen to a video or audio clip.\textsuperscript{127} Online gaming is responsible for nine percent of Internet traffic. With over eleven percent of long-distance telephone calls passing over the Internet at some point in their journey,\textsuperscript{128} many individuals will be engaged in real-time voice communications online.\textsuperscript{129} Wedding, birth, graduation, vacation, and other personal photos are part of the 880 million photos available using Google's image search.\textsuperscript{130}

The use of the Internet for personal activities has grown steadily over the past eighteen years. Home is now the dominant site of Internet access for U.S. Internet users.\textsuperscript{131} Increasing numbers of individuals report using the Internet for fun and for leisure activities.\textsuperscript{132} Gaming, listening to and downloading music, and searching for information about personal interests are popular activities.\textsuperscript{133} Forty-two million individuals reported that they played games online in July 2002.\textsuperscript{134} Over 112 million individuals use the

\begin{footnotesize}
\textsuperscript{125} See ACLU v. Reno, 929 F. Supp 824, 832 (E.D. Pa. 1996) (finding that “[m]essages between computers on the Internet do not necessarily travel entirely along the same path. The Internet uses ‘packet switching’ communication protocols that allow individual messages to be subdivided into smaller ‘packets’ that are then sent independently to the destination, and are then automatically reassembled by the receiving computer. While all packets of a given message often travel along the same path to the destination, if computers along the route become over-loaded, then packets can be re-routed to less loaded computers.”). The technology called “packet switching” made the modern Internet possible. Leonard Kleinrock, Professor Emeritus, Computer Science Department, UCLA, was the first to develop the underlying principles of data packet switching, and has been hailed as the father of modern computer networks. He published the first paper on Packet Switching Theory, \textit{Information Flow in Large Communication Nets}, and the first book on packet switching, \textit{Communications Nets}. Leonard Kleinrock, Brief Summary of Firsts, Key Accomplishments and Contributions for Len Kleinrock, http://www.tk.cs.ucla.edu/LK/inet/keys.html. (last visited July 5, 2004).

\textsuperscript{126} CHANGING PICTURE OF WHO'S ONLINE, supra note 120.


\textsuperscript{129} A router called a “soft switch” is used to break telephone calls into bits of data using the Internet Protocol (IP), which can then be sent over the Internet thousands at a time using any open pathway to reach their destination, just like text data travels.


\textsuperscript{131} Eighty-seven percent of Internet users have access at home and forty-eight percent have access at work. Pew Internet & Am. Life Project, \textit{PIP Data Memo: Use of the Internet in Places Other than Home or Work}, http://www.pewinternet.org/reports/toc.asp?Report=115 (last modified Mar. 3, 2004).

\textsuperscript{132} CHANGING PICTURE OF WHO'S ONLINE, supra note 120.

\textsuperscript{133} Daily Internet Activities, supra note 5 (noting that “on an average day, about 72 million American adults go online” and that various surveys show that on an average day, nine percent of American adults used the Internet to: play a game (March–May 2003), four percent to listen to music online at a Web site (August–October 2001), one percent to download music files to a computer (November–December 2003), six percent to download other files such as games, videos, or pictures (June 2003), twenty-three percent to surf the Web for fun (March–May 2003), and twenty-one percent to look for information on a hobby or interest (March–May 2003)).

\textsuperscript{134} CHANGING PICTURE OF WHO'S ONLINE, supra note 120.
\end{footnotesize}
Internet to search for information:135 ninety-one million to seek out information about personal interests; seventy-three million to seek out health information; sixty-six million to seek out government information; forty-seven million to seek out political information; and thirty-five million to seek out information on religion.136

E-mail remains the dominant online activity engaged in by Internet users surpassing purchasing activities by thirty-two percent.137 Approximately 102 million U.S. individuals use e-mail, with about 60 million using it on any given day.138 Fifty-two million US individuals have used instant messaging, with over 10 million using it on a typical day.139 Twenty-one million U.S. individuals have created content on the Internet, including pages for Web sites, "blogs," online diaries, or postings to bulletin boards or newsgroups.140 The content individuals create ranges from movies,141 short stories,142 and news reports143 to journals,144 family trees,145 and photo albums.146

A third of U.S. Internet users have high-speed access in their homes.147 High-speed access is equated with more regular use of the Internet to search for information, in some instances doubling daily searches.148 Moreover, high-speed Internet access is strongly correlated with the creation of content.149 As the number of homes with high-speed access increases, it appears that overall use of the Internet will continue to grow, as will the number of Internet users creating and contributing content.150

135 Daily Internet Activities, supra note 5 (noting that survey shows eighty-eight percent of American adults with Internet access used a search engine on an average day in June 2003).
136 Changing Picture of Who's Online, supra note 120.
137 Id.
138 Id.
139 Id.
140 Id.
142 Changing Picture of Who's Online, supra note 120.
143 Id.
144 Id.
145 Id.
146 Id.
147 Id.
148 Id. (noting that "home broadband users are more than twice as likely to look for information relating to their hobby on an average day compared to dial-up users"). The study showed forty-one percent of broadband users sought information about their hobbies, compared to eighteen percent of dial-up users in February 2002. Id.
149 Thirty-four percent of Internet users with high-speed connections create content compared to four percent of all users.
150 Legislation in the 108th Congress is pending (or has been incorporated into law) regarding tax incentives for broadband use: H.R. 267, a bill to amend the Internal Revenue Code of 1986 to provide an incentive to ensure that all Americans gain timely and equitable access to the Internet over current and future generations of broadband capability, sponsored by Representative Phil English (R-PA), H.R. 267, 108th Cong. (2003); S. 905, a bill to amend the Internal Revenue Code of 1986 to provide a broadband Internet access tax credit, sponsored by Senator Jay Rockefeller (D-WV), S. 905, 108th Cong. (2003); S.A. 593 to S. 1054, a bill to amend the Internal Revenue Code of 1986 to allow the expensing of broadband Internet access expendi-
These data points and trends illustrate the extent to which the Internet has infiltrated personal life. They speak to the increasingly personal nature of individuals' online activities, conversations, and information searches.\textsuperscript{151} The Internet is now used as a storage site for personal photos, a meeting place for social clubs, and is a primary personal communication system for millions of individuals.\textsuperscript{152} If an activity can be done without leaving the house and physically interacting with another individual, someone somewhere has found a way to do it online. As broadband connections are available in more homes, the use of the Internet for personal, rather than business, activities will accelerate. In analyzing the adequacy of existing privacy protections and proposing revisions, the personal nature of today's online activities should be a core consideration.

\section*{IV. The Business Records Cases: The Search for Limiting Principles}

The other reason for the disconnect between actual privacy expectations and those protected under ECPA, discussed above, is that Congress accepted an interpretation of Supreme Court precedent suggesting that these technical differences between e-mail and telephone conversations placed the contents of e-mail messages outside the scope of the Fourth Amendment.\textsuperscript{153} Based on this interpretation, Congress crafted a framework that assumed the mode of transmitting a private communication or the medium in which records stored

\textsuperscript{151} Daily Internet Activities, \textit{supra} note 5 (noting that "on an average day, about 72 million American adults go online" and that various surveys show that on an average day, six percent of American adults used the Internet to look for health or medical information (December 2002), four percent to look for religious or spiritual information (March-May 2003), four percent to go to a Web site that provides information or support for a specific medical condition or personal situation (December 2002), one percent to go to a dating Web site or other sites where you can meet other people online (June 2003), and one percent to research a family's history or genealogy (March-May 2003)).

\textsuperscript{152} Notably, this is true with America's older segment of the population. \textit{See} Andrea Coombes, \textit{Retired and More Wired: Older Americans Ramp up Internet Use}, http://cbs.marketwatch.com/news/story.asp?guid=%7BE5A6935D-1B46-4252-B07B-A58C143ADC50%7D&siteid=google&dist=google (last modified Nov. 23, 2003) ("The online presence of Americans aged 65 and older jumped 25 percent this year, to a total of almost 10 million surfers, while 55- to 64-year-olds upped their numbers by 15 percent, to almost 16 million, according to a new study by Nielsen/NetRatings, a market research firm. 'This segment of the population is becoming much more comfortable with the medium,' said Charles Buchwalter, vice president of analytics at Nielsen/NetRatings. Women led the charge, with those 65 and older increasing their Internet presence by 30 percent, to 4.6 million, while men's use increased by 20 percent, to about 5 million, according to Nielsen/NetRatings. Overall, 35- to 49-year-olds continue to maintain the largest online presence at almost 40 million, followed by those 25 to 34, at 21 million. Those numbers represent increases of 1 percent and 3 percent year over year, respectively. Still, once they're connected, wired seniors are more likely to go online daily, with 69 percent of those 65 and older doing so, compared with 56 percent of all Internet users, according to a separate study, to be released soon by the Pew Internet and American Life Project.").

\textsuperscript{153} \textit{Hearing before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary}, 99th Cong. 234 (1986) (statement of James Knapp, Deputy Assistant Attorney General, Criminal Div.).
with a third party are held is the overriding factor in the Court’s determination of the privacy afforded.\textsuperscript{154} Congress crafted a statute based on the premise that the content of electronic communications, as well as records intentionally stored in space leased from third parties, would be considered by the Supreme Court as akin to telephone toll records.\textsuperscript{155}

To understand why I question Congress’s decision to adopt the traditional reading of the business records cases as a baseline in the ECPA debates, it is necessary to start with the Supreme Court’s 1967 ruling in \textit{Katz v. United States}\textsuperscript{156} that established that wiretapping a private telephone call placed from a public phone booth is a search governed by the Fourth Amendment.\textsuperscript{157} There, the Court held that the Fourth Amendment protects “people not places,” and said in determining whether a search violated the Fourth Amendment that the crucial question is whether the individual has a “reasonable expectation of privacy.”\textsuperscript{158} Whether an individual has a reasonable expectation of privacy is a two-part inquiry.\textsuperscript{159} The first step is to ask whether the individual’s conduct reflects “an actual (subjective) expectation of privacy.”\textsuperscript{160} If the answer is yes, the next question is whether the actual expectation is “one that society [objectively] is prepared to recognize as reasonable.”\textsuperscript{161}

The “reasonable expectation” test established by \textit{Katz} dominates the last thirty-seven years of the Supreme Court’s privacy jurisprudence.\textsuperscript{162} By decoupling privacy expectations from the trespass doctrine, the “reasonable expectation” test expanded the scope of Fourth Amendment protection for privacy.\textsuperscript{163} Its subsequent application, however, undermined its initial prom-

\begin{itemize}
  \item \textsuperscript{154} H.R. REP. NO. 99-647, at 23, 72–73 (1986).
  \item \textsuperscript{155} Id.
  \item \textsuperscript{156} Katz v. United States, 389 U.S. 347 (1967).
  \item \textsuperscript{157} Id. at 353. The \textit{Katz} case, along with \textit{Berger v. New York}, 388 U.S. 41 (1967), set the stage for passage of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (current version at 18 U.S.C. §§ 2510–2522 (2000)). The wiretap provisions of Title III authorized law enforcement wiretapping of telephones within a framework designed to protect privacy and compensate for the uniquely intrusive aspects of electronic surveillance. Id. (imposing criminal sanctions against the interception of wire communications and regulates wiretapping by law enforcement). Title III broadly prohibits the interception of oral communications and wire communications. See 18 U.S.C. § 2511(1). The enactment of the detailed and quite protective statutory provisions of Title III limited the opportunity, and arguably the need, for further judicial statements on the contours of the Fourth Amendment as applied to government interception of voice communications. Because Title III prohibits the “aural” acquisition of voice communications, there was little disagreement that intercepting voice communications that traveled across an electronic network were covered, because like wire line interception it would be an “aural” acquisition. See OTA REPORT, supra note 8, at 46.
  \item \textsuperscript{158} Katz, 389 U.S. at 362. (Harlan, J., concurring).
  \item \textsuperscript{159} Id. at 361.
  \item \textsuperscript{160} Id.
  \item \textsuperscript{161} Id.
  \item \textsuperscript{157} Id. at 360–61; see Richard W. Walinski & Thomas J. Tucker, \textit{Expectations of Privacy: Fourth Amendment Legitimacy Through State Law}, 16 HARV. C.R.-C.L. L. REV. 1, 2 (1981) (noting that “Justice Harlan’s concurrence in \textit{Katz v. United States} set forth the standard that the Supreme Court has applied ever since for determining when the fourth amendment affords protection”).
  \item \textsuperscript{163} Morgan Cloud, \textit{The Fourth Amendment During the Lochner Era: Privacy, Property, and...}}}
The business records cases, for example, each undermined the reach of the \textit{Katz} reasonable expectation test by finding some information, due to its nature and the individuals' voluntary disclosure of it to a third party, failed to meet even the subjective prong of the \textit{Katz} reasonable expectation test. In \textit{Couch v. United States},\footnote{Couch v. United States, 409 U.S. 322 (1972).} the Court held that subpoenaing an accountant for records provided by a client for the purposes of preparing a tax return raised neither Fifth nor Fourth Amendment concerns.\footnote{Id. at 335–36.} In \textit{United States v. Miller},\footnote{United States v. Miller, 425 U.S. 435 (1976).} the Court held that records of an individual's financial transactions held by his bank were outside the protection of the Fourth Amendment.\footnote{Id. at 440–41.} Lastly, in \textit{Smith v. Maryland},\footnote{Smith v. Maryland, 442 U.S. 735 (1979).} the Court held that individuals have no legitimate expectation of privacy in the phone numbers they dial, and therefore the installation of a technical device (a pen register) that captured such numbers on the phone company's property did not constitute a search.\footnote{Id. at 745–46.}

While these cases greatly reduced the ability of individuals to claim Fourth Amendment protection for transactional records generated by their activity with, and maintained by, a business, as well as records provided to a business for use in providing a service, they do not support the broader statement that all personal communications and information held by business entities is outside the scope of the Fourth Amendment. Several factors play an important, if somewhat subtle, role in shaping and limiting the Court's reasoning in these cases, including the business's independent interest in the transaction and information at issue, the individual's intent to disclose the information to the business, and the distinction between content and noncontent data. A review of the holdings in the business records cases illustrates the limits of the Court's reasoning and the lack of support they provide to key provisions of the SCA.
A. Limiting Principle: The Independent Interest Factor

The records containing personal information sought by law enforcement in Couch, Miller, and Smith were records in which the business had an independent interest. The information a taxpayer provided to his accountant in Couch was intended for the accountant’s use. In analyzing the Fourth Amendment claim, the Court noted the accountant’s independent interest in using and disclosing the information, given his professional and legal obligations. Likewise, the bank records at issue in Miller were clearly of independent interest to the bank. Banks are an integral party to financial transactions and must maintain records about patrons’ account activity for financial integrity, tax purposes, and other reasons. Finally, the phone numbers at issue in Smith were used both to connect the callers and for billing purposes. The Court found that the phone company could not provide its service without storing and using those phone numbers. In some instances, although ironically not in the case of the local calling records at issue in Smith, the financial relationship between the customer and the phone company is predicated on billing systems that make distinctions based on dialed numbers.

In these cases, the businesses did not merely act as conduits or storage facilities for the records; they acted upon the records independently. It was this independent interest that the Court emphasized in finding that the Fourth Amendment provides no protection from government access. For example, in Couch, the Court found that the Fourth Amendment provided no protection from government access because the taxpayer turned the information at issue over to his accountant for the accountant’s use in preparing a tax return with an understanding that much of the information would be disclosed in due course to the government. While acknowledging that there could be instances where entrusting information to a third party would not eliminate an individual’s reasonable expectation of privacy, the Court found that in this instance, the accountant’s independent interest made it clear that the individual had assumed the risk that the information provided to the accountant would be disclosed to others, including the government.

171 Couch, 409 U.S. at 335. The Court also noted that at least a portion of the information was intended for disclosure directly to the government. Id.
172 Id.
173 See Miller, 425 U.S. at 440–41 (holding that banks have a stake in the continued acceptance and availability of bank records) (citing Cal. Bankers Assn. v. Shultz, 416 U.S. 21, 48–49 (1974)).
174 See id. at 444 (noting that banks have traditionally kept permanent records of transactions).
175 See Smith, 442 U.S. at 742.
176 Id.
177 Couch, 409 U.S. at 335.
178 Id.
B. Limiting Principle: Intentional Nature of the Disclosure

In each of the business records cases, the individual intended to disclose the information at issue to the business.\textsuperscript{179} For example, in \textit{Couch}, the taxpayer disclosed the information to the accountant explicitly for use in preparing a tax return.\textsuperscript{180} The disclosure of the information to the accountant was not incidental to its communication to another party, but the end result of the individual's act.\textsuperscript{181}

The disclosure analyses in \textit{Miller} and \textit{Smith} are slightly less clear cut; however, both present facts where the provision of the service depends upon the intentional disclosure of information.\textsuperscript{182} In reaching its conclusion in \textit{Miller}, the Court stated that Miller's voluntary decision to convey the information to the bank left him at risk if the bank subsequently chose to disclose the information to the government.\textsuperscript{183} Similarly, in rejecting Smith's Fourth Amendment challenge, the Court held that people generally have no subjective expectation that phone numbers they dial are private, because they know the numbers are conveyed to the phone company to complete the call and are stored and tracked for billing purposes, and they are generally aware that phone companies have access to them.\textsuperscript{184} The Court concluded that even if Smith could argue that he had a subjective expectation of privacy, society would not recognize a privacy expectation where the information is voluntarily disclosed to, and routinely used by, a third party.\textsuperscript{185}

Revealingly, the \textit{Katz} Court did not consider the concept of voluntary disclosure.\textsuperscript{186} Clearly, the Court could have applied the voluntary disclosure and assumption-of-risk analysis to the wiretapping of call content at issue. Individuals disclose telephone conversations, just as they disclose telephone numbers, to the telephone company's service.

There are two ways that \textit{Smith} can be distinguished from \textit{Katz}. First, one could argue that the voluntary nature of the disclosure is of importance only where the business has an independent interest in the record.\textsuperscript{187} As dis-

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{179} \textit{See Smith}, 442 U.S. at 743–44; \textit{Miller}, 435 U.S. at 442; \textit{Couch}, 409 U.S. at 335. Many have taken issue with the notion of "voluntary disclosure" and the assumption-of-risk analysis it invites in these cases. I share the concern with the Court's reasoning, but it is not my aim here to argue it. The word "intentional" disclosure is used here, however, because it more accurately describes the distinguishing factor of these disclosures—the individual intended to hand over some piece of information to the business—the extent to which the disclosure should be considered voluntary I have set aside for future discussion. \textit{See Miller}, 425 U.S. at 451 (Brennan, J., dissenting).
\item \textsuperscript{180} \textit{Couch}, 409 U.S. at 335.
\item \textsuperscript{181} \textit{Id.} Perhaps more folks would find this disclosure to be voluntary as well as intentional.
\item \textsuperscript{182} \textit{Smith}, 442 U.S. at 743–44; \textit{Miller}, 435 U.S. at 442.
\item \textsuperscript{183} \textit{Miller}, 435 U.S. at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).
\item \textsuperscript{184} \textit{Smith}, 442 U.S. at 742–43. As additional support for the proposition that individuals knew about the availability of phone numbers to the phone company, the Court cited the pages in telephone books indicating that the phone company could assist in addressing harassing phone calls. \textit{Id.}
\item \textsuperscript{185} \textit{Id.} at 743–44,
\item \textsuperscript{186} \textit{See generally} \textit{Katz} v. United States, 389 U.S. 347 (1967).
\item \textsuperscript{187} \textit{See supra} text accompanying notes 171–77.
\end{itemize}
\end{footnotesize}
cussed above, this analysis is supported by the language of Smith and Miller.\(^{188}\)

Alternatively, one could argue that the individual's intent in disclosing the record at issue to the business is critical in determining whether such a disclosure should be considered “voluntary.” Under this approach, one would find that only where the business was one of the intended recipients of the information should the disclosure to the business be considered voluntary. This line of analysis, while not directly discussed in Smith or Miller, is consistent with case law establishing the Fourth Amendment privacy interest in postal mail in transit.\(^{189}\)

C. Limiting Principle: The Nature of the Record

Both Miller and Smith emphasize that it is important to consider the contents of the records at issue to determine if a reasonable expectation of privacy exists.\(^{190}\) In Miller, the majority stated that the government did not seek the records at issue to investigate associational activities, such that the search did not implicate the First Amendment.\(^{191}\) The Court found that the checks and deposit slips at issue were “not confidential communications but negotiable instruments to be used in commercial transactions.”\(^{192}\)

Similarly, in Smith, the Court discussed at some length the limited information that can be gleaned from a phone number, contrasting it with what may be revealed from a telephone conversation.\(^{193}\) In distinguishing the telephone toll records in Smith from the content of the telephone conversation at issue in Katz, the Court stated:

"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 purport 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."\(^{194}\)

Of course, like the telephone numbers in Smith, the content at issue in Katz was “conveyed . . . to the telephone company,” “‘exposed’ . . . to its equipment in the ordinary course of business,” and clearly the phone company “has facilities for recording” it.\(^{195}\) The Court’s discussion of the substantive nature of the records in Smith was thus meant to explain why the

\(^{188}\) See id.

\(^{189}\) See, e.g., Ex parte Jackson, 96 U.S. 727, 733 (1877).

\(^{190}\) Smith, 442 U.S. at 741; United States v. Miller, 425 U.S. 435, 444 n.6 (1976).

\(^{191}\) Miller, 425 U.S. at 444 n.6.

\(^{192}\) Id. at 442. Of course, as the dissent noted, this begs the question of whether the records reveal associational interests regardless of the investigators’ subjective intent in accessing them. Id. at 451 (Brennan, J., dissenting).

\(^{193}\) See Smith, 442 U.S. at 741.

\(^{194}\) Id. (citing United States v. N.Y. Tel., 434 U.S. 159, 167 (1977)).

\(^{195}\) See id. at 744–45.
First Amendment concerns informing the Fourth Amendment analysis in *Katz* were not at issue in *Smith*.\(^{196}\)

### V. Limiting Principles Lost

In the ECPA debates surrounding the appropriate standards to govern law enforcement access to electronic communications and electronic records stored on remote computers, the limiting aspects of the Court's business records jurisprudence received little attention. As a result, the ECPA leaves many records accessible to law enforcement under lower standards than I believe the Court would hold the Fourth Amendment requires, particularly given today's use of the Internet.

#### A. The Privacy of Electronic Communications

Originally, those supporting changes to establish statutory privacy protections for electronic communications hoped to merely add the word "electronic" to Title III, directly paralleling the protections afforded to voice communications.\(^ {197}\) The DOJ, however, was hostile to this approach. The DOJ agreed during negotiations that an electronic message in storage incident to transmission should be treated like first-class mail—accessible with a warrant based on probable cause.\(^ {198}\) The DOJ argued forcefully that an e-mail message, when it becomes "part of the records in the files of a communications... carrier," is subject to no Fourth Amendment protections at all.\(^ {199}\) It contended that, when an e-mail message is left on a third-party server after having been read by the recipient or for over 180 days, opened or unopened, it becomes a business record outside the scope of Fourth Amendment protection. Specifically, the DOJ stated that Fourth Amendment warrant requirements are inapplicable to this type of document since there is no reasonable expectation of pri-

---

196 See id. at 741.
197 Interview with John Podesta, Chief Counsel to the House Judiciary Committee during the drafting of the ECPA (Mar. 26, 2003); E-Mail Interview with Jerry Berman, legislative counsel for the ACLU during the drafting of the ECPA (Mar. 22 & 25, 2003); Telephone Interview with Jerry Berman (Mar. 27, 2003).
198 Hearing before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary, 99th Cong. 234 (1986) (statement of James Knapp, Deputy Assistant Attorney General, Criminal Div.). The DOJ argued, however, against the other limitations found in Title III, which have been critical in addressing the uniquely intrusive aspects of wiretapping. See id. Limitations in Title III that are absent from the Wiretap Act include: a limited set of specific crimes, 18 U.S.C. § 2516 (2000); application must show that the wiretap is being used as a last resort, either because other investigative techniques have failed, are reasonably unlikely to succeed, or are too dangerous, 18 U.S.C. § 2518(1)(c); that there is probable cause that the communication facility is being used in a crime, 18 U.S.C. § 2518(1)(b); and wiretaps must "minimize" the interception of innocent conversations, 18 U.S.C. § 2518(5). "Minimization" was deemed essential to satisfy the Fourth Amendment's particularity requirement, compensating for the fact that law enforcement received all of the target's communications, including those that were not evidence of a crime. Berger v. New York, 388 U.S. 41, 54–61 (1967) (striking down state statute allowing eavesdropping based on ex parte order of the Court).
199 Id. at 235.
vacy associated with it. This is a well accepted principle of law relating to documents in the possession of third persons and we know of no sound legal or policy reason why it should not apply to these types of documents.\textsuperscript{200}

In contrast, the OTA Report concluded that an e-mail message in an electronic mail box on an individual's personal computer terminal, or an electronic mail box rented by an individual on the computer terminal of an electronic mail company, should be afforded Fourth Amendment protection.\textsuperscript{201} The OTA Report noted, however, that as electronic mail companies retain copies of electronic messages for business purposes, it was "possible that an individual would not have a legal basis from which to challenge an electronic mail company's disclosure of the contents of messages or records of messages sent."\textsuperscript{202} Still, the OTA Report indicated this might not be appropriate, emphasizing the significant distinction between records of electronic communications and other business records, particularly in light of an electronic record's ability to reveal a substantial amount of information about an individual, including the substance of the communication, as well as the parties to the communication, and their location.\textsuperscript{203}

As discussed above, Congress ultimately adopted the DOJ's position, sharply departing from traditional conceptions of individuals' right to privacy in personal communications. The House report stated that "to the extent that the record (including e-mail message) is kept beyond that point (180 days) it is closer to a regular business record maintained by a third party and, therefore, deserving of a lesser standard of protection."\textsuperscript{204}

While the decision was made by Congress to analogize e-mail to first-class mail, ECPA is not faithful to the analogy. First-class mail is accorded a high degree of protection from government access. While mail covers\textsuperscript{205} are allowed under postal regulations at the request of law enforcement,\textsuperscript{206} access to the contents of first-class mail requires a warrant just "as is required when papers are subjected to search in one's own household."\textsuperscript{207} The standards for

\textsuperscript{200} Id.
\textsuperscript{201} See OTA REPORT, supra note 8, at 49.
\textsuperscript{202} Id. at 50.
\textsuperscript{203} Id.
\textsuperscript{204} H.R. REP. NO. 99-647, at 68 (1986).
\textsuperscript{205} A "mail cover" is defined as:
[T]he process by which a record is made of any data appearing on the outside cover of any class of mail matter, including checking the contents of any second-, third-, or fourth-class mail matter as now sanctioned by law, in order to obtain information in the interest of (i) protecting the national security, (ii) locating a fugitive, or (iii) obtaining evidence of commission or attempted commission of a crime.
\textsuperscript{206} Id. § 233.2(e)(ii) (providing that postal inspectors may order mail covers "where written request is received from any law enforcement agency of the Federal, State, or local governments, wherein the requesting authority stipulates and specifies the reasonable grounds that exist which demonstrate the mail cover would aid in the location of a fugitive, or that it would assist in obtaining information concerning the commission or attempted commission of a crime" (emphasis added)).
\textsuperscript{207} 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
access to first-class mail have never varied because the mail has been sitting in a mailbox for longer than a particular period of time. Nowhere is there support for the notion that leaving a piece of mail in a postal or personal mailbox for over six months time will, on its own, reduce the substantive and procedural requirements governing law enforcement access.\textsuperscript{208} Even where law enforcement is able to subpoena a letter in transit from sender to recipient, it must obtain a warrant to open and examine its contents.\textsuperscript{209} Even though the letter is voluntarily conveyed to the carrier, its contents remain protected by the full force of the Fourth Amendment. Once delivered, the letter can be shared by the recipient with whomever they choose, including the government, without raising Fourth Amendment concerns.\textsuperscript{210}

Yet, the ECPA provides for the complete opposite. The statute accepts that an e-mail message—the metaphoric equivalent of first-class mail—can be transformed into a potentially accessible business record.\textsuperscript{211} If e-mail is in storage "incident to transmission" for 180 days or less—because it is waiting to be retrieved, or is passing through servers on its way to its destination—the government must have a regular warrant to access it.\textsuperscript{212} If the e-mail is in storage on a third-party server for more than 180 days, however, the statute allows law enforcement access with a subpoena based on a mere relevance standard.\textsuperscript{213} If opened e-mail less than 180 days old is maintained by an individual on a service such as Yahoo!, it is currently debatable as to whether law enforcement must obtain a warrant to access it or may use a subpoena.

An understanding of contemporary business practices provides additional insight into the weaker protection for e-mail messages that remain in storage for over 180 days. During the legislative process, Congress found that existing e-mail services did not retain e-mail messages automatically, nor did they retain them for long periods of time.\textsuperscript{214} The standard retention period for e-mail by electronic communication system providers was six months.\textsuperscript{215} Thus, in order for an individual to save a message beyond this point she had to actively move it to storage. Accordingly, standard business practice indicated that limiting law enforcement access to e-mail during the

\textsuperscript{208} See United States v. Barr, 605 F. Supp. 114, 116 n.1 (S.D.N.Y. 1985) (rejecting the notion that the defendant's failure to retrieve mail for six weeks indicated an intent to abandon it or had any bearing on the reasonable expectation of privacy in personal mail).

\textsuperscript{209} See id. at 116 (noting a grand jury subpoena was used to compel production of mail from a private company; the government subsequently secured a search warrant to open the mail).


\textsuperscript{213} Id. § 2703(b).


first 180 days of its existence would in effect cover it long past the time it could be reasonably expected to be retrieved from an e-mail service provider. If an e-mail was available on a third-party server after that date it was because the individual or business would have chosen to store it with a remote data processing and storage center. This is significant because it suggests that it is possible to reconcile the repeated congressional references to first-class mail-like protection with the statute’s distinction between mail 180 days old or younger and other records, including e-mail records. Importantly, it also suggests that the question of whether an e-mail has been opened or not may not be the essential question in determining whether it is held in electronic storage and protected by the stronger warrant requirement. The United States Court of Appeals for the Ninth Circuit has recently come to this conclusion, declining to adopt the position taken by lower courts and advocated by the DOJ that, once opened, an e-mail is no longer in storage incident to transmission and therefore is no longer subject to the warrant requirement of electronic storage because it is no longer in “temporary intermediate storage.” In doing so, the Ninth Circuit found that opened e-mails left on an ISP’s server easily fall within the ordinary meaning of the terms “backup protection,” and concluded that, in order for the two separate clauses of § 2701(a)(1) to have separate meaning, “backup protection” must mean something other than “temporary intermediate storage . . . incidental to transmission.”

The Supreme Court has not considered whether individuals have a reasonable expectation of privacy in e-mail held by their Internet service provider; the Court’s decisions exploring reasonable expectations of privacy, however, generally provide a useful framework for considering the question. As discussed above, the Court analyzes Fourth Amendment questions by asking first whether the individual has manifested a subjective expectation of privacy, and then whether society is willing to recognize this expectation as reasonable. In deciding whether society considers an individual’s privacy expectation reasonable, “the Court has given weight to such factors 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.” The Court approaches its analysis of the objective reasonableness prong of the reasonable expectation of privacy test from a rights-based approach rooted in real and personal property and social custom. The factors the

---

217 See Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004) (discussing the DOJ’s position).
218 See id. at 1075–77.
219 Id. at 1076.
221 O’Connor v. Ortega, 480 U.S. 709, 715 (1987) (holding that public employee had a reasonable expectation in his office, his desk drawers and his file cabinets and establishing a reasonable test for considering whether a public employer’s search of such areas violate the Fourth Amendment) (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)).
Court considers, regardless of the theory applied, favor privacy expectations tied to personal and real property or to long-standing traditions of confidentiality. These factors weigh in favor of a finding that individuals have a reasonable expectation of privacy in e-mail maintained on their behalf on an Internet service provider or the equivalent.

First, the Fourth Amendment makes direct reference to papers and effects. E-mail and other electronic files are modern-day papers. In these files reside the musings, arguments, philosophical theories, and love letters of modern individuals. The change in form, while technically significant, should not override the shared nature of paper correspondence and electronic correspondence. The legislative history of ECPA, with its comparisons between

223 Melissa Arbus, A Legal U-Turn: The Rehnquist Court Changes Direction and Steers Back to the Privacy Norms of the Warren Era, 89 VA. L. REV. 1729, 1735–43 (2003) (discussing the importance of private property and the trespass doctrine in post-Katz cases despite the Court's rejection of the primacy of trespass analysis in Katz); see also Helen Nissenbaum, Privacy as Contextual Integrity, 79 WASH. L. REV. 119, 125–32 (2004) (identifying three principles that dominate public deliberations, including court decisions, about privacy: limiting surveillance of citizens and use of information about them by agents of government; restricting access to sensitive, personal, or private information; and curtailing intrusions into places deemed private or personal).

224 The Fourth Amendment to the United States Constitution 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

225 ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996) (finding that e-mail is "comparable in principle to sending a first class letter"), aff'd, 521 U.S. 884 (1997); id. at 836 (World Wide Web is "most advanced information system" used to allow "information sharing" in scientific, academic, nonprofit, and business community, as well as by individuals); id. at 837 (World Wide Web is a series of stored documents; documents range from "the hastily typed idea, to the professionally executed corporate profile"; publishers can choose to make them open to all or to restrict access).

226 At least one court has allowed law enforcement warrantless access to copies of telegrams held by telegraph companies. Newfield v. Ryan, 91 F.2d 700, 703 (5th Cir. 1937) (dismissing Fifth and Fourth Amendment objections to a subpoena for telegrams). I believe, however, that this is factually distinct from e-mail. In the case of telegrams, an individual must give the text of their message to the operator in order for it to be sent. For this reason it was not uncommon for individuals seeking privacy to send coded messages. See Orin S. Kerr, The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?, 33 CONN. L. REV. 503, 526 (2001) (citing David Kahn, The Codebreakers 189–90 (2d ed. 1996); Simon Singh, The Code Book 60–79 (1999)). With respect to e-mail, however, the text of the message need not be shared with an individual for the purpose of furthering the communication. Like telephone communications, the business provides the pipe that allows the message to be conveyed, and nothing more. While the business needs to handle the routing information in a manner analogous to the telephone numbers at issue in Smith, it has no interest in the content.
e-mail and first-class mail, follows this reasoning. As discussed above, the content of postal mail is squarely within the zone of privacy protected by the Fourth Amendment and as such enjoys a high degree of protection from government access. \(^{227}\) *Katz* shows the Court adapting the Framers' expressed concerns with the privacy of an individual's papers—and the thoughts and communications therein—to a new form of communication that took conversations outside the curtilage of the home into a more public place and onto a technology that provided greater opportunities for third-party access. \(^{228}\) Despite the fact that similar communications took place either in person or through paper correspondence at the time of the Constitution's drafting, the Court in *Katz* recognized the essential similarity between telephone conversations and earlier forms of protected communication.

Second, the Court has repeatedly affirmed our societal understanding that privacy protections for the content of communications have particularly strong Fourth Amendment roots. Beginning with *Boyd v. United States*, \(^{229}\) where the Court stated that

> [i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . [including] any forcible and compulsory extortion of a man's own testimony or of his private papers

that amounts to an offense \(^{230}\) the Court has consistently placed communications (papers, telephone conversations) within the zone of privacy. \(^{231}\) While the holding of *Boyd*, prohibiting government searches for, and seizures of, private papers was abandoned, the unique relationship of communications to personal privacy was not abandoned. \(^{232}\) The decisions above discussing postal mail and the *Katz* ruling discuss the particular importance of shielding the contents of private communications from government access. In addition, the Court calls for exacting scrutiny under the Fourth Amendment when First Amendment interests are implicated. Tellingly, the reasonableness of privacy expectations in, and therefore Fourth Amendment protection for, the content of communications is set out as a foil in the *Smith* case, which found that dialed phone numbers in the hands of the phone company lacked such protection.

Although the Court's repeated statements that papers are at the core of Fourth Amendment protection and its willingness to extend protections to

---

\(^{227}\) See supra text accompany notes 205–10.


\(^{229}\) *Boyd v. United States*, 116 U.S. 616 (1886).

\(^{230}\) Id. at 630.

\(^{231}\) See, e.g., *Weeks v. United States*, 232 U.S. 383, 393 (1914) ("[I]f letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the Fourth Amendment . . . is of no value, and . . . might as well be stricken from the Constitution.").

\(^{232}\) See *Cloud*, supra note 163, at 575–76 (discussing the Court's use of indefeasible rights under the Fourth and Fifth Amendment to create a zone of privacy that limited government power to preserve individual liberty).
voice communications over the telephone system suggest that individuals would be found to have a reasonable expectation of privacy in e-mail, two technical issues raise questions that must be addressed. First, e-mail, unlike first-class mail, travels in a form that allows the entities which handle it to read it; for this reason it has been functionally equated with a postcard.233 As discussed above, however, phone conversations also travel without the equivalent of an envelope and where a telephone communications carrier desired to listen in there would be no opaque barrier concealing the conversation traveling across the carrier's line. While much has been made about the postcard-like nature of e-mail, the Court rejected such technological determinism in 1967 when it overruled Olmstead v. United States,234 and replaced it with the reasonable expectation test of Katz. Second, e-mail, because of many of the factors discussed above, is often more vulnerable to interception. Whether this technical vulnerability would be a decisive factor in the Court's consideration of the privacy interest, is an open question.235 Several courts declined to find reasonable privacy expectations in cordless telephone conversations236 because the technology they rely upon—radio waves—broadcasts the conversation in all directions. This suggests that the actual security of the technology matters. The security risks of e-mail—to hackers and eavesdroppers—is, however, more akin to the security risks of telephone calls, in that each is directed to a specific individual but can be accessed by a motivated adversary. This is different from cordless phones where, unfortunately, the conversation can be inadvertently picked up by those in the vicinity.237

Few courts have considered whether individuals maintain a reasonable expectation of privacy in e-mail held by an ISP.238 The lower courts that have

---

233 See, e.g., ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), aff'd, 521 U.S. 884 (1997) (finding that unlike postal mail, simple e-mail generally is not "sealed" or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)).


235 See generally Max Guiruis, Electronic Mail Surveillance and the Reasonable Expectation of Privacy, 8 J. TECH. L. & POL'Y 135 (2003) (discussing Fourth Amendment cases addressing reasonable expectations of privacy in other technological advancements, including cellular telephones, fax communications, telex transmissions, and e-mail messages).


237 If it is encrypted it may not be readily accessible.

looked at the issue either explicitly find a reasonable expectation of privacy or implicitly, in the specific fact scenarios for which protection is denied suggest that such a reasonable expectation of privacy exists. Importantly, courts that have considered the question have not blindly adopted the business records jurisprudence. For example, in United States v. Maxwell, the court stated that (1) "e-mail is extraordinarily analogous to a telephone conversation"; (2) the ECPA "afford[s] protection from disclosure of intercepted communications absent a duly issued search warrant"; (3) the "contractual obligation [between the ISP and the subscriber] . . . insured . . . privacy"; and (4) "the tenor and content" of the e-mail revealed a subjective and reasonable expectation of privacy in the e-mail conversations at issue. Moreover, the court noted that "AOL's policy was not to read or disclose subscribers' e-mail." In rejecting the voluntary disclosure and assumption-of-risk analysis of the business records cases in the context of e-mails stored with AOL, the court reasoned:

In a sense e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police. The fact that an unauthorized "hacker" might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way.

While recognizing that AOL employees who had direct access to the network might violate AOL's policy and read or redistribute private e-mails, the court did not find that this undermined the subscriber's reasonable expectation of privacy.

Somewhat at odds with the Maxwell holding, but quite limited in scope, is United States v. Geter, where the court held that a military employee had no reasonable expectation of privacy in e-mail remotely stored on a government network. Emphasizing that the U.S. government owned and operated the system, and that individual e-mail accounts are provided for official use only, the court held that, even if the employee took steps to manifest a subjective expectation of privacy, it would not be objectively reasonable to do so. The court went on to state that even if the employee had been granted limited personal use privileges, he would have no reasonable expectation of privacy. Importantly, the court also stated that even if the employee introduced evidence that his e-mail messages had not yet been

---

239 See Maxwell, 45 M.J. 406 at 416-17; Proetto, 771 A.2d at 831.
241 Id. at 416-17.
242 Id. at 417.
243 Id. at 418
244 Id.
246 Id. at *5.
247 Id. at *3-4.
248 Id. at *4.
received by the intended recipients, and were therefore arguably analogous
to unopened mail in transit, the fact that the system's server immediately
saved a copy of each message would undermine any expectation of privacy in
the unopened e-mail in transit.\textsuperscript{249} Still, although the court adopted the volun-
tary disclosure and risk analysis reasoning of the business records cases in the
later part of its decision, the core of its reasoning focuses on the nature of the
relationship between military personnel and services provided to them for
use in carrying out official duties.\textsuperscript{250}

Other cases have rejected Fourth Amendment challenges to searches
and seizures of e-mail and chat communications for reasons consistent with
case law rejecting defendants' Fourth Amendment challenges to the use of
undercover police\textsuperscript{251} and informants and disclosures by recipients.\textsuperscript{252} Like
other forms of communication, individuals lose their control over, and there-
fore their reasonable expectation of privacy in, communications once they
are opened or received by the intended recipient. Similarly, where an indi-
vidual chooses to confide in an individual who turns out to be unworthy of
trust because they are an undercover officer or an informant, their privacy
expectations will not protect them from the risk they assumed. The cases
find no Fourth Amendment protection for misplaced confidences or bad
judgment, consistent with holdings in other areas of Fourth Amendment
law.\textsuperscript{253}

While the business records cases have not been a central factor in the
lower courts' consideration of the privacy of e-mail, they have been relied
upon in cases holding that individuals do not have a reasonable expectation
of privacy in basic personal information, such as name and address, given to
an ISP to obtain service.\textsuperscript{254} In applying the risk-analysis approach of the bus-
ness records cases to the information necessary to establish an Internet ser-
vie account, one court stated that the defendant “knowingly revealed his
name, address, credit card number, and telephone number,” and “employees
had ready access to these records in the normal course of . . . business . . . for

\textsuperscript{249} Id. at *5.
\textsuperscript{250} Id. at *3–4 (noting that “appellant’s case deals specifically with a U.S. government
owned, operated, and maintained network and electronic communication system”).
\textsuperscript{251} See State v. Evers, 815 A.2d 432, 440 (N.J. 2003) (finding that defendant had no reason-
able expectation of privacy in the content of e-mail he forwarded to fifty-one intended recipi-
ents, one of whom happened to be an undercover police officer).
the forwarding of a message by a victim recipient to the police did not violate the Wiretap Act).
\textsuperscript{253} See United States v. White, 401 U.S. 745, 752 (1971) (holding that the government's use
of agents who may reveal the contents of conversations with the accused does not violate the
Fourth Amendment); Hoffa v. United States, 385 U.S. 293, 302 (1966) (finding no Fourth
Amendment violation where defendant revealed confidences to a government informant).
See generally Kerr, supra note 226.
\textsuperscript{254} See, e.g., Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001) (holding that plaintiffs
lacked a Fourth Amendment interest in subscriber information communicated to the administra-
tor of a computer bulletin board); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan.
2000) (holding that when a criminal defendant entered into a service agreement for Internet
access he “knowingly revealed” information to the service provider eliminating his Fourth
1999), aff'd, 225 F.2d 656 (4th Cir. 2000).
example, in the keeping of its records for billing purposes.” In considering whether the defendant had an objectively reasonable expectation of privacy, the court also cited the ability of the ISP to disclose information to nongovernmental parties, stating that where “dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.” In this situation, the subscriber information at issue is a necessary part of the business relationship between an individual and an ISP. The ISP has several obvious business uses of this information, the foremost of which is billing, in addition to ancillary business uses, such as marketing, which are frequently declared in terms of service agreements. The facts of these cases fit neatly into the “pure business records” analysis; therefore the reasoning of Miller and Smith is more compelling.

The law enforcement access standards set out in the ECPA are incongruent with the Fourth Amendment and reflect a misplaced reliance on the business records case law. While the Supreme Court has not considered whether the Fourth Amendment protects e-mail held by an ISP, the lower courts that have looked at the issue either explicitly find such protection or implicitly, in the specific fact scenarios for which protection is denied suggest that such a reasonable expectation of privacy exists. The lack of reliance on the business records cases in these decisions is not surprising, for it is difficult to imagine a record less like those at issue in Couch, Smith, and Miller than a record of an e-mail message. An e-mail message’s content does not relate to, or reflect, a relationship between the individual and the service provider. Further, the service provider’s lack of interest in the contents of the message is bolstered by rules protecting them from liability for content created by users, and by terms of service which disavow any interest in private communications. Unlike the information provided to the accountant in Couch, the individual has no intent to disclose the actual contents of their messages to the service provider. Similarly, to distinguish the numbers at issue in Smith from the content of the telephone call at issue in Katz, the Court first pointed to the substantive differences in the records. Unlike the phone numbers at issue in Smith, the contents of communications reveal the senders’ thoughts and ideas. Finally, unlike the financial records at issue in Miller, on which the bank itself relies to execute its customers bidding and to protect itself against fraud, service providers have no independent stake in the content of subscribers’ personal communications.

Service providers are mere conduits or pipes. By statute, they can have no interest in the communications to qualify as either an ECS or an RCS.

---

255 Hambrick, 55 F. Supp. 2d at 508–09.
256 Id. at 509.
While individuals assume the risk that an intended recipient of an electronic communication may turn it over to the government, the service provider is not the recipient. As an entity that merely maintains a mailbox for the individual, service providers are similar to telephone companies or private mail carriers. Simply put, the service provider is not the person with whom the sender is communicating; therefore, the concept of voluntary disclosure that underlies the Court's rationale in the business records cases is inapplicable in the electronic communication context. Although a voluntary disclosure occurs in the electronic communication context, the disclosure is based on the understanding that the service provider has no interest in the information itself, but is merely supporting the transmission or storage irrespective of the information contained. This type of disclosure is directly analogous to the disclosure that occurs during a telephone conversation or the sending of postal mail, and therefore the same protection that applies to the content of telephone conversations should apply to the content of electronic messages. E-mail, like the content of a phone call, reveals the "purport of any communication between the caller and the recipient of the call, [and] their identities." Individuals consider their e-mail private, and the Court has consistently reiterated the importance of protecting the privacy of private communications. The personal and revealing nature of an e-mail record calls for the highest form of protection from unreasonable government access. Even if law enforcement were able to access the message using a subpoena, the government should not be allowed to examine its content without a warrant based on probable cause.

Further, driven by the Berger v. New York decision, which articulated additional precautions necessary to bring wiretapping within the Fourth Amendment due to its uniquely intrusive nature, Title III places additional requirements on warrants for wiretaps. These additional protections of minimization, notice after the investigation concludes, and the opportunity prior to introduction of the evidence for an adversarial challenge to both the adequacy of the probable cause and the conduct of the wiretap all appear relevant to electronic communications in storage. Minimization designed to compensate for the fact that law enforcement receives all of the target's communications in the interception context, and therefore is acting outside the Fourth Amendment's particularity requirement, is partially addressed by the ability of the record keeper to reveal only specified e-mails or records. However, rather than just thirty days worth of communications, potentially years of communications may be obtained and they may reveal a host of unrelated information. Title III requires delayed notice to be given to targets of the investigation and further requires that other means of obtaining the evidence have been exhausted for the wiretap in part to compensate for the lack of

---

262 See Ex parte Jackson, 96 U.S. 727, 733 (1877) (finding protectable privacy interest in postal mail); Katz v. United States, 389 U.S. 347, 353 (1967) (finding protectable privacy interest in content of telephone calls).
264 See id. at 55–63.
265 See supra notes 102, 198 and accompanying text.
B. Privacy Expectations in Electronic Records in Remote Storage

Under the ECPA, records in remote storage include any information stored with a public provider of remote computing services solely for the purpose of providing storage or computer processing. Such information includes any form of data, such as an individual's records, photos, journals, date books, and other personal effects. Although Attorney General Guidelines limit the seizure of confidential information from nonparties such as doctors, lawyers and clergy, the statute itself draws no such distinction. Looking back, it is clear that Congress did not foresee what would be at stake in 2004 with widespread personal reliance on the Internet as a communications and storage tool when it created a rule that takes as its premise that any record found to be in remote storage is without intrinsic Fourth Amendment protection.\(^266\) Again, the backdrop of *Miller* and *Smith* provided the DOJ with fodder to argue for limited protections for stored records.\(^267\) Under ECPA, such records can thus be accessed by law enforcement through a variety of processes. A warrant may be used, in which case notice is not provided to the individual whose records are accessed.\(^268\) Alternatively, a subpoena issued on the lower “mere relevance” standard can be used, in which case notice is required, although it may be delayed if certain procedural requirements in 18 U.S.C. § 2705 are met.\(^269\) Moreover, the warrant and subpoena are served on the remote computing service provider, not on the individual whose records are sought.\(^270\)

Today the records individuals store on the Internet are not reminiscent of the records in *Couch*, *Smith*, and *Miller*. First, these stored records do not reflect an interaction between the business and the individual, as the records at issue in the business records cases did. Rather, by statute they are records that are provided to the business for storage or processing.\(^271\) Consequently, the service provider has no independent business interest in the records. The transactional records in which the business and individual have a mutual in-

---


\(^{267}\) Berman & Mulligan, *supra* note 100.

\(^{268}\) *See supra* Part III.


\(^{270}\) *Id.*

\(^{271}\) *Id.*

\(^{272}\) *Id.* § 2703(b)(2)(B) (defining rules about disclosing content in an RCS with respect to communications held solely for the purpose of storing and processing and excluding other access to RCS owner).
terest related to the service purchased and any records exchanged to support the provision of such service, similar to the records at issue in the business records cases, are covered by another provision and accessible under an even weaker standard.\textsuperscript{273}

The RCS is not an intended recipient of the records.\textsuperscript{274} Frequently, remote electronic storage services are used to store records that the individual intends to keep entirely to herself, such as diaries and journals. At other times, the individual intends to share the records with a small group of friends or colleagues, as with family photos. Finally, the revealing nature of some of the records individuals store on an RCS distinguishes them from the records at issue in the business records cases. The records and information placed on third-party servers include pictures, diaries, personal correspondence, and backup copies of date books. Many of the records reveal the individual's thoughts and associations. While businesses continue to store business records with RCSs, the records stored on an RCS by individuals are distinct from the records at issue in the business records cases and due to their personal, communicative nature, more akin to the content at issue in \textit{Katz}.

It is possible that the Court would analyze electronic records such as diaries, journals, and family photos stored on remote servers under the business records cases. Considering the availability of a more directly analogous area of Fourth Amendment case law, addressing the privacy expectations of individuals in personal effects stored in property rented for exclusive use, it seems more likely that the Court would adopt this alternate approach.\textsuperscript{275} The case law in this area focuses on searches of rented rooms, apartments, and lockers, and is substantially more protective of privacy than the business records case law.\textsuperscript{276} The rental analogy is more appropriate than the business record analogy for, as discussed above, the RCS that is providing record storage has no separate interest in the records—they neither reflect interactions with a customer, nor provide information needed to render an independent service. In addition, from the perspective of the individual who houses documents on a remote server it is likely to be perceived as an arrangement similar to renting a room or locker to store personal goods rather than handing data over to a business to be used in furtherance of his relationship with that business.

A lessee who rents property for exclusive use is entitled, generally, to Fourth Amendment protections in that property.\textsuperscript{277} A lessor who rents exclusive possession of an area to another generally cannot consent to a police

\textsuperscript{273} \textit{Id.} § 2703(c) (providing standards for accessing noncontent data including name, address, and billing records).

\textsuperscript{274} \textit{See id.} § 2703(b)(2)(B).

\textsuperscript{275} United States v. Fultz, 146 F.3d 1102, 1105 (9th Cir. 1998) (holding that guest had privacy interest in boxes stored in owner's garage).

\textsuperscript{276} \textit{See id.}

\textsuperscript{277} \textit{See Stoner v. California,} 376 U.S. 483, 487–88 (1964) (holding that hotel clerk did not have authority to consent to search of hotel room); Chapman v. United States, 365 U.S. 610, 616–17 (1961) (holding that a landlord lacks authority to consent to search of property used by tenant).
search of that area.\textsuperscript{278} The factual determination of whether a third-party lessor can consent to such a search rests on questions about the extent of exclusivity granted the lessee and whether the lease has been terminated for reasons of abandonment, failure to make payment, or illegal activity.\textsuperscript{279} The question of exclusivity goes to whether the lessor has authority to consent to a search of the property. Where the lessor has "common authority" over the space, it can consent to a search.\textsuperscript{280}

Remote computing services that offer services to the general public frequently have terms of services that affirm their disinterest in the content users store there. While Web hosting and other remote computing services system administrators often have broad rights to access records in order to protect their own interests, these access rights are unlikely to provide the requisite access or control for the system administrator to be able to consent to law enforcement access.\textsuperscript{281} A useful, if limited analogy, is the law dealing with searches of computers and files turned over to third parties for repair or safekeeping. Like other closed containers, where an individual leaves a computer with someone for safekeeping she retains a reasonable expectation of privacy in the files it contains.\textsuperscript{282} While a repair technician who comes across questionable files may report it to the police, and the police under the private search doctrine can generally reenact the search without a warrant, the individual's expectation of privacy in the files contained in a computer left for repair remains.\textsuperscript{283} With respect to files on third-party servers, the case law supporting reasonable expectations of privacy in rented physical spaces and in computers and files stored on them, turned over for repair, suggest that

\textsuperscript{278} See Wayne R. LaFave, 3 Search and Seizure: A Treatise on the Fourth Amendment § 8.5 (3d ed. 1996).

\textsuperscript{279} United States v. Poulsen, 41 F.3d 1330, 1331 (9th Cir. 1994) (holding that renter does not have a legitimate expectation of privacy in the contents of a rental unit if the rent is not paid); United States v. Reyes, 908 F.2d 281, 286 (8th Cir. 1990) (holding that there is no reasonable expectation of privacy in storage locker where rental contract expired).

\textsuperscript{280} LaFave, supra note 278, § 8.5.

\textsuperscript{281} See Stoner, 376 U.S. at 487-88 (holding that hotel clerk did not have authority to consent to search of hotel room); Chapman, 365 U.S. at 616-17 (holding that a landlord lacks authority to consent to search of property used by tenant). For a thorough examination of the privacy expectations in "timesharing records," see C. Ryan Reetz, Note, Warrant Requirement for Searches of Computerized Information, 67 B.U. L. Rev. 179, 200-06 (1987) (arguing that certain kinds of remotely stored computer files should retain Fourth Amendment protection, distinguishing Miller).

\textsuperscript{282} See United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (finding a reasonable expectation of privacy in computer files on hard drive turned over to repair technician for purpose of fixing computer); see also United States v. Most, 876 F.2d 191, 197-98 (D.C. Cir. 1989) (finding a reasonable expectation of privacy in contents of bag left with store clerk); United States v. Barry, 853 F.2d 1479, 1481-83 (8th Cir. 1988) (finding a reasonable expectation of privacy in locked suitcase stored at baggage counter); cf. Poulsen, 41 F.3d at 1331 (finding no expectation of privacy in computer tapes in storage facility where rent has not been paid because property has been abandoned).

\textsuperscript{283} See United States v. Jacobsen, 466 U.S. 109, 115 (1984) (establishing scope for warrantless police searches following a private search as not beyond the scope of the private search). But see United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001) (allowing police search of all files under rationale that private party search of one file on computer allows police to search all).
electronically stored personal files on an RCS would fall within the zone of privacy protected by the Fourth Amendment.

The choice between the business records and rental property cases is significant for both the analysis and outcome of cases. The business records cases lead to findings that no search occurred, and thus that there is no Fourth Amendment protection, while the storage and leased-space line of cases finds that searches have occurred and consider whether the third party has the authority to consent to a search. Moreover, the use of the voluntary nature of the disclosure and the assumption-of-risk analysis of the business records cases to place personal calendars, photos, journals, and the like outside the scope of Fourth Amendment protection is difficult to square with cases like *Katz*. There, the conversation at issue was voluntarily disclosed to the phone company, and potentially could have been captured by a phone tap, yet the Court still found that the contents of the call were protected by the Fourth Amendment. Approaching the privacy analysis under the case law addressing privacy expectations in property rented for exclusive use would create an opportunity to distinguish the “pure business records” cases from the problematic issues presented by other remotely stored personal records.

The analogy to the business records cases was arguably appropriate in 1986 when the Internet was used primarily for businesses and business information. Today, however, the growth in personal use of the Internet and the routine use of hosting services to store personal communications and records strongly suggests that the leased space analogy is more appropriate. Given that hosting services have no independent interest in these personal effects, are not the intended recipient, and given the personal nature of many of the files, it is quite difficult to fit them under the business records cases.

**Conclusion**

The passage of the ECPA limited the Court’s consideration of the many issues concerning reasonable expectations of privacy in electronic communications and remotely stored electronic records. Case law has begun to address the scope of the business records cases in the world of electronic communications and storage; relatively little has been said, however, about whether there is, or should be, a reasonable privacy expectation in e-mail stored on third-party servers or in documents placed on third-party servers.

---

284 See *United States v. Matlock*, 415 US 164, 171 (1974) (finding third-party consent to search requires that the third party have joint access or control of the property for most purposes).


286 As with e-mail service providers, Web hosting services often affirm their lack of interest in what users store with them. While admonishments to abide by the law are standard fare, terms of services also include statements such as, “*Ofoto does not control the content of any user’s album and does not have any obligation to monitor such content for any purpose. All content provided by a user of this service is the sole responsibility of that user, not Ofoto.*” *OFOTO, INC., TERMS OF SERVICE*, http://www.ofoto.com/TermsOfService.jsp?UV=943673090043_123268590105 (last visited July 5, 2004).

287 See *supra* Part III.

288 See *id.*
for safekeeping.\textsuperscript{289} The existence of this comprehensive statutory scheme has no doubt limited the willingness of parties to raise Fourth Amendment challenges to seizures of stored communications and records. Moreover, the lack of an exclusionary rule under the ECPA further reduces the incentive of criminal defendants to litigate these issues.\textsuperscript{290}

The key architects of the ECPA were visionary in their understanding that electronic communication networks needed privacy protections. They drafted one of the most comprehensive privacy statutes enacted in the United States. But, as individuals have taken up residence in cyberspace, using it to communicate and store their personal effects, the protections of the ECPA, based on the strained reading of the business records case law advocated by law enforcement during the ECPA debates, are inadequate as a matter of policy and unsupported by the Court's Fourth Amendment case law. ECPA should be revised to reflect the expectations of individuals using the Internet today. Privacy advocates concerned about the protections ECPA affords to stored records should also consider direct challenges to the provisions of the SCA as applied to e-mail messages and personal effects, such as family photos. In the case of e-mail in storage, individuals' long-held, socially reinforced expectations are that the contents of communications are not accessible without a search warrant.\textsuperscript{291} Nothing in our personal or societal understanding of privacy would lead an individual to believe that such protections would wither away if the mail is left in a mailbox (electronic or otherwise) rented for the purpose of receiving and storing personal communications. Given that e-mail is a replacement for telephone communications as well as postal mail, the additional protections of minimization, notice, and postintroduction exclusionary procedure, based on the \textit{Berger} decision, found in Title III should be considered by Congress when, and if, they revisit the SCA. At a minimum, prior or contemporaneous notice to the individual whose e-mail is to be seized should be required. Where individuals rent space on an RCS to store their personal effects, they have not chosen to disclose anything to the service provider. While users of e-mail and remote

\textsuperscript{289} See id. For commentary on the issue, see United States v. Ross, 456 U.S. 798, 822 (1982); Patricia Bellia, \textit{Surveillance Law Through Cyberlaw's Lens}, 72 GEO. WASH. L. REV. 1375, 1385–88 (2004); Max Guirguis, \textit{Electronic Mail Surveillance and the Reasonable Expectation of Privacy}, 8 J. TECH. L. & POL'Y 135, 153–54 (2003) (suggesting that the Court may use the technical lack of security to find no reasonable expectation of privacy under the public exposure doctrine progeny of \textit{Katz}, but arguing that if this is the case that the use of encryption could address the technical problem and provide a reasonable expectation of privacy); Kerr, supra note 226, at 524 (arguing that encryption cannot create a reasonable expectation of privacy because the Court has rejected the notion that creating a high likelihood of secrecy does not create a legitimate expectation of privacy, quoting United States v. Ross, 456 U.S. 798, 822 (1982) (footnotes omitted): "[A] constitutional distinction between 'worthy' and 'unworthy' containers would be improper... For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attache case."); Steere, supra note 38, at 231 (calling on Congress to modify the ECPA to protect reasonable expectations of privacy in e-mail).

\textsuperscript{290} See Kerr, supra note 66, at 806–07.

\textsuperscript{291} See supra Part II.
computing services may expect the administrators of the system to have a limited right to access their files to protect the systems functionality, they in no way assume that such access includes the right to share the contents of their communications and files with the government. The contents of files stored on an RCS should be protected by a warrant requirement and contemporaneous or prior notice to the individual should be required.

As Representative Kastenmeier, a key architect of the ECPA, so aptly stated:

When the Founders added the fourth amendment's protection against unreasonable searches and seizures to the Constitution, they did so to protect citizens' papers and effects. In those days an individual's private writing and records were kept within the home. That situation has changed drastically today. Many Americans are now using computer services, which store the bank records, credit card data, electronic mail and other personal data. If we fail to afford protection against governmental snooping in these files, our right of privacy will evaporate. Moreover, if we fail to protect the records of third-party providers, there will be a tremendous disincentive created against using these services.\footnote{132 CONG. REC. 14,886 (1986) (statement of Rep. Kastenmeier).}

It is time to revisit the ECPA armed with a more critical reading of the business records cases and an understanding of how individuals currently use e-mail and remote servers. The assumption that all records maintained by third parties on an individual's behalf are at some point outside the scope of Fourth Amendment protection—an assumption that influenced the structure of the ECPA—is eroding privacy to an extent not imagined or intended by the Court in the business records cases.