E-MAIL PRIVACY AFTER *UNITED STATES V. COUNCILMAN*: LEGISLATIVE OPTIONS FOR AMENDING ECPA

By Katherine A. Oyama

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) to update federal surveillance law and establish privacy safeguards for emerging technologies.[1] ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968[2]—the federal wiretap law—which until then protected voice, but not electronic, communications from interception. ECPA restructured the earlier law into three major sections: Title I (the Wiretap Act), Title II (the Stored Communications Act, or SCA), and Title III (the Pen Register Act).[3] Passed prior to the public adoption of the internet for daily communication purposes,[4] ECPA pro-

---

1. Pub. L. No. 99-508, S. REP. NO. 99-541, at 1, *reprinted in* 1986 U.S.C.C.A.N. at 3555 (stating that ECPA's purpose was to clarify federal privacy protections amid advances in technology and establish federal protections for electronic communications); *see also In re* Pharmatrak Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.").

2. Pub. L. No. 90-351, S. REP. NO. 90-1097 (1968); *see also* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 323 (2003).

3. *See* Wiretap Act, 18 U.S.C. §§ 2510-2522 (2000 & Supp. II 2002); Stored Communications Act, 18 U.S.C. §§ 2701-2711 (2000 & Supp. II 2002); Pen Register Act, 18 U.S.C. §§ 3121-3127 (2000 & Supp. II 2002). This Note does not address the Pen Register Act which governs the use of devices that trace "envelope information" (including "addressing and routing information" for e-mail) as opposed to the Wiretap Act and the Stored Communication's Act provisions governing "content information." Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611 (2003). This Note also does not address the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1863 (2000 & Supp. II 2002) which governs the U.S. government's "foreign intelligence" surveillance activities as opposed to ECPA's provisions governing domestic surveillance by ordinary law enforcement.

4. The number of U.S. internet users in 1986 was estimated to be 64,000 people. Roger J. Rusch & Robert Sharples, *Ten Small Technological Surprises Along The Road To The 21st Century*, SATELLITE NEWS, June 25, 2001. By 1994, only two percent of U.S. households had internet access. DIV. OF SCI. RES. STUDIES, NAT'L SCI. FOUND., THE AP-

vides the statutory framework governing the interception of electronic communications under the Wiretap Act[5] and access to stored electronic communications under the SCA.[6]

The First Circuit's recent en banc decision in *United States v. Councilman* raises concern about the continued viability of ECPA's provisions.[7] In *United States v. Councilman*,[8] a divided panel of the First Circuit held that an Internet Service Provider's real-time surveillance of its customers' e-mail during the course of transmission did not violate the Wiretap Act because the communication was obtained from temporary storage rather than a non-storage component of the internet's vast e-mail infrastructure.[9]

PLICATION AND IMPLICATIONS OF INFOR. TECHNOLOGIES IN THE HOME: WHERE ARE THE DATA AND WHAT DO THEY SAY: THE SOCIODEMOGRAPHICS OF ACCESS AND ADOPTION (2001), *available at* http://www.nsf.gov/statistics/nsf01313/pdf/front.pdf. A 2005 study found that sixty-three percent of American adults —approximately 128 million people — use the internet. PEW INTERNET & AM. LIFE PROJECT, INTERNET: THE MAINSTREAMING OF ONLINE LIFE 58, *available at* http://www.pewinternet.org/pdfs/Internet_Status_2005.pdf. The study also found that "[E]mail is still the killer app. It is the No. 1 activity and time consumer for the vast majority of Internet users." *Id.* at 63.

5. 18 U.S.C. § 2511 (2000); *see, e.g.*, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1278-79 (2004).

6. 18 U.S.C. § 2701 (2000); *see, e.g.*, Solove, *supra* note 5, at 1279; *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1557 (2004).

7. 418 F.3d 67 (1st Cir. 2005) [hereinafter *Councilman III*]; *see* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("ECPA was written prior to the advent of the Internet . . . . the existing statutory framework is ill-suited to address modern forms of communication . . . ."); United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2002) ("Until Congress brings [ECPA] in line with modern technology, protection of the Internet . . . will remain a confusing and uncertain area of the law.") (citation omitted); *see also* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1396-97 (arguing that "[s]tored communications have evolved in such a way that these provisions, often referred to as the Stored Communications Act ("SCA"), are becoming increasingly outdated and difficult to apply"); Mulligan, *supra* note 6, at 1559 (concluding that "[m]any who supported [ECPA] would agree that it has failed to keep pace with changes in and on the Internet and therefore no longer provides appropriate privacy protections").

8. 373 F.3d 197, 198 (1st Cir. 2004) [hereinafter *Councilman II*], *reh'g en banc granted* and *opinion withdrawn by*, 385 F.3d 793 (2004), *rev'd by*, 418 F. 3d 67 (1st Cir. 2005) (noting that "[i]t may well be that the protections of the Wiretap Act have been eviscerated as technology advances").

9. *See Councilman II*, 373 F.3d at 203 (stating that "the e-mails in this case were accessed by the procmail as they were *being transmitted and in real time*") (emphasis added).

Following widespread public criticism,[10] the First Circuit agreed to rehear the case en banc and reversed the decision.[11] The en banc court concluded that the Wiretap Act applies to an electronic communication in transient, electronic storage intrinsic to the communication process.[12] Thus, an electronic communication in temporary, electronic storage may be covered by both the Wiretap Act and the SCA.

Although Councilman may now be held liable under the Wiretap Act, a growing body of case law underscores the importance of the SCA for governing internet surveillance law.[13] Given the constantly changing nature of technology and the increased use of electronic communications, it is imperative that Congress amend ECPA and close the gap in privacy safeguards for e-mail highlighted in *Councilman*. The all-or-nothing disparity in privacy protection from ISP surveillance afforded to an e-mail under the Wiretap Act and the SCA results in judicial determinations of ISP criminal liability based on minor—and sometimes even arbitrary—differences in surveillance technology rather than the underlying privacy interests at stake.[14] In addition, it is equally important that courts use a principled rather than technology-dependent approach in interpreting ECPA's underlying intent.

This Note argues that the SCA's liability exemption for service providers is overbroad. Part I provides an overview of ECPA and describes key cases governing e-mail surveillance by state and private actors. Part II discusses the *Councilman* cases. Part III analyzes three statutory problems that remain despite the First Circuit's enlightened en banc decision and evaluates the arguments for and against proposed ECPA amendments to increase privacy protections for electronic communications.

This Note concludes that in the short term, Congress should amend ECPA's definition of "intercept" to protect the public interest in a secure electronic communications network and limit the broad service provider

---

10. *See, e.g.*, *Intercepting E-Mail*, N.Y. TIMES, July 2, 2004, at A18 (stating that *Councilman* "sets up a frightening precedent, one that must be reversed by the courts, if not the Congress"); *see also* Mark Jewell, *Court Allows E-Mail Interception, Raising Privacy Questions*, USA TODAY, June 30, 2004, http://www.usatoday.com/tech/news/internetprivacy/2004-06-30-scotus-e-mail-intercept_x.htm; Kim Zetter, *Court Creates Snoopers' Heaven*, WIRED NEWS, July 6, 2004, http://www.wired.com/news/privacy/0,1848,64094,00.html.

11. *Councilman III*, 418 F.3d at 69.

12. *Id.* at 79.

13. *See infra* Section I.C.

14. *See Councilman II*, 373 F.3d 197, 200 n.3 (1st Cir. 2004) ("In this appeal, we are more concerned with the mechanism used to send and receive e-mail and therefore highlight those sections of the stipulation.").

exception for ISPs. Congress should also reconsider the larger issue of electronic communications privacy generally and e-mail communications specifically to ensure that electronic surveillance law keeps pace with advancements in technology.

I. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)

This Part discusses the constitutional framework and statutory provisions that specify the conditions under which law enforcement may intercept wire, oral, and electronic communications and the penalties for unauthorized interceptions.

A. The Constitutional Framework

The Supreme Court has interpreted the U.S. Constitution as providing a fundamental "right to privacy," located within the undefined "penumbras" of the Bill of Rights[15] and the Fourteenth Amendment's concept of personal liberty.[16] The concept of personal liberty contained in the Bill of Rights guarantees a "right to privacy" encompassing both "explicit protection against government intrusion into the home and personal effects"[17] and "implicit protection of autonomy and free choice."[18]

In *Katz v. United States*,[19] the Supreme Court found that the Fourth Amendment requires law enforcement to obtain a search warrant when monitoring phone calls made from a public telephone booth. In his concurrence in *Katz*, Justice Harlan articulated the "reasonable expectation of privacy test" for determining whether the Constitution protects an individ-

15. Griswold v. Connecticut, 381 U.S. 479, 483-85 (1965) (stating that the U.S. Constitution protects the right to privacy although its text does not explicitly reference the term "privacy"). For example, privacy is protected by the First Amendment's freedom of association clause and guarantee of the right to speak anonymously, the Third Amendment's protection for privacy of the home, the Fourth Amendment's guarantee that people have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . ." and the Fifth Amendment's right against self-incrimination. DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 20-21 (2003) (citing U.S. CONST. amends. I, III-V).

16. U.S. CONST. amend. IV ("[N]or shall any State deprive any person of life, liberty, or property, without due process of the law . . . .").

17. Will Thomas DeVries, Note, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 286 (2003).

18. *Id.*

19. 389 U.S. 347, 353 (1967) (overturning Olmstead v. United States, 277 U.S. 438 (1928), in which the Court found no reasonable expectation of privacy against wiretaps, and finding that individuals have a reasonable expectation of privacy in telephone conversations).

ual's right to privacy from intrusion by the government.[20] The two-pronged test requires that (1) an individual "have exhibited an actual (subjective) expectation of privacy,"[21] and (2) "the expectation be one that society is prepared to recognize as [objectively] 'reasonable.'"[22]

In *United States v. Miller*,[23] the Supreme Court held that an individual loses her substantive due process right to information privacy[24] once information is "revealed" to a third-party service provider. Perhaps, as internet technology advances, the law will recognize a constitutionally-protected expectation of privacy in the content of e-mail messages.[25] For now, ECPA's procedural safeguards concerning stored communications address the gap left by the unclear application of the Fourth Amendment to cyberspace. ECPA's statutory framework is thus increasingly important to protecting personal privacy in the digital age.

B. The Legislative Framework

In *Councilman III*, the court analyzed two statutory schemes, the Wiretap Act and the SCA, to determine which law governed the company's e-mail surveillance activities.[26] Professor Daniel J. Solove expressed a commonly-held view concerning the scope of the Wiretap Act as follows: "[i]f a communication is being transmitted from its origin to a destination, the Wiretap Act applies; if it is stored electronically in a computer, the Stored Communications Act governs."[27] An overview of ECPA's relevant provisions is provided below.

---

20. *Id.* at 361 (Harlan, J., concurring). *See generally* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 21 (2003).

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

22. *Id.*

23. 425 U.S. 435 (1976) (holding that defendant had no reasonable expectation of privacy in personal financial records revealed to a third-party bank).

24. *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 598-600 (1977) (finding a constitutionally-protected zone of privacy that includes the interest in avoiding disclosure of personal matters).

25. Professor Bellia argues that *Miller* and *Katz* should not be read as holding that mere reliance on a third party to transmit a communication eliminates an expectation of privacy in the contents of the message. Bellia, *supra* note 7, at 1405 ("[W]ith respect to Internet communications, neither the service provider's technical ability to gain access to the contents of a communication, nor the ability of the communication's recipient to reveal the contents of the communication, should, without more, eliminate a subscriber's expectation of privacy in communications stored with a service provider.").

26. 418 F.3d 67, 80 (1st Cir. 2005).

27. Solove, *supra* note 5, at 1283.

1. The Wiretap Act

Before ECPA, the federal wiretap laws protected only wire (voice) and oral communications from interception.[28] Title I of ECPA, the Wiretap Act, extended the federal wiretap law's protections to electronic communications.[29] The Wiretap Act makes it illegal for anyone to "intentionally intercept[] . . . any wire, oral, or electronic communication"[30] and governs communications in transit.[31] The term "intercept" is currently defined in the Wiretap Act as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[32] In 2001, Congress passed the USA PATRIOT Act and amended ECPA's definition of "wire communication" by moving the protection of stored voice communications—such as voice-mail messages—from the Wiretap Act to the SCA.[33]

Under the Wiretap Act, wire and electronic service providers are exempt from the interception provisions in the Act only if the interception occurs during the normal course of business and is necessary to provide the service.[34] Specifically, the Wiretap Act states that an operator of a switchboard, or an agent of a telecommunications or electronic communications service provider, may intercept a communication in the normal

---

28. *See* Pub. L. No. 90-351, S. REP. NO. 90-1097 (1968).

29. S. REP. NO. 99-541, at 1, *reprinted in* 1986 U.S.C.C.A.N. at 1. ECPA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . but does not include . . . any wire or oral communication . . ." 18 U.S.C. § 2510(12) (2000).

30. 18 U.S.C. § 2511(1)(a) (2000).

31. *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994) (holding that interception of an "electronic communication" under the Wiretap Act requires that the acquisition of the contents of a communication occurs *contemporaneous with its transmission*).

32. 18 U.S.C. § 2510(4) (2000).

33. Pub. L. No. 107-56, 115 Stat. 272 (2001). Prior to the amendment, ECPA defined "wire communication" as:

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce *and such term includes any electronic storage of such communication.*

18 U.S.C. § 2510(1) (2000) (emphasis added). After the amendment, the reference to electronic storage was deleted from the definition of "wire communication." 18 U.S.C. § 2510(1) (2000 & Supp. II 2002).

34. 18 U.S.C. § 2511(2)(a)(i) (2000).

course of employment while engaged in an activity necessary to render the service.[35] However, the Act prohibits service providers from engaging in random monitoring and observing except in the case of service-quality control checks.[36]

A second exception under the Wiretap Act applies if one of the parties to the communication consents to the surveillance.[37] Therefore, private individuals and law enforcement agents may secretly record a communication to which they are a party. However, the consent exception does not apply when an interception is carried out for the purpose of committing a criminal or tortious act in violation of state or federal law.[38]

Communications governed by the Wiretap Act enjoy generous protection. Law enforcement must seek court orders to obtain the protected communications and offenders face serious criminal sanctions.[39] Under the Wiretap Act, a request for an electronic surveillance order must be made by a high-level official to a court under oath,[40] and a federal judge must find that (1) particular communications concerning a specific offense will be obtained through the interception (the probable cause requirement),[41] and (2) alternatives to wiretapping either failed or are unlikely to succeed (the minimization requirement).[42]

Under the Wiretap Act's exclusionary rule, "[a]ny aggrieved person . . . may move to suppress the contents of any wire or oral communication

---

35. See 18 U.S.C. § 2511(2)(a)(i) which states:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in an activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

Id. The Act also makes it illegal for a service provider to disclose a communication while in transmission. 18 U.S.C. § 2511(3)(a).

36. *Id.* § 2511(2)(a)(i).

37. *Id.* § 2511(2)(c)-(d).

38. *Id.* § 2511(2)(d).

39. Professor Orin Kerr refers to a court order under the Wiretap Act as a "'super' search warrant." Kerr, *supra* note 3, at 621.

40. 18 U.S.C. §§ 2516, 2518(1) (2000).

41. *Id.* § 2518(3).

42. *Id.* § 2518(1)(c).

intercepted pursuant to this chapter, or evidence derived therefrom."[43] However, because the exclusionary rule explicitly lists only wire and oral communications, this suppression remedy does not protect electronic communications.[44] Thus, a defendant in a criminal trial can suppress evidence obtained by the illegal interception of a phone conversation but not an e-mail.[45] Finally, violations of the Wiretap Act can result in fines of a minimum of $10,000 per violation[46] as well as up to five years' imprisonment.[47]

2. The Stored Communications Act (SCA)

Congress created the SCA to control access to stored electronic communications maintained by a service provider.[48] The SCA makes it illegal for anyone to "access[] without authorization a facility through which an electronic communication service is provided; or . . . exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system."[49] Under the SCA, violations can result in fines of up to $1,000 per violation and up to one years' imprisonment.[50] If the unauthorized access was committed for purposes of commercial gain, then the prison sentence may be increased to five years.[51]

ECPA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[52] The requirement that the electronic storage be temporary, intermediate storage "incidental" to the transmission under subsection A or for the purposes of backup protection under subsection B limits the scope of the SCA. According to the Department of Justice's narrow construction of the term "electronic storage," the contents of an e-mail

43. *Id.* § 2518(10)(a).

44. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 824 (2003).

45. *See* Solove, *supra* note 5, at 1282.

46. 18 U.S.C. § 2520(c)(2)(B) (2000).

47. *Id.* § 2511(4)(a).

48. *See id.* § 2701(a)(1).

49. *Id.* § 2701(a)(1)-(2).

50. *Id.* §2701(b)(1)-(2) (2000 & Supp. II 2002) (providing increased criminal punishment "if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act").

51. *Id.*

52. *Id.* § 2510(17)(A)-(B).

communication stop being "temporary, intermediate storage" and fall outside ECPA's scope once the recipient opens the e-mail.[53] The SCA also governs access to customer records. Customer record information includes the customer's name, address, phone numbers, and billing records and is protected less rigorously than other forms of stored communications.[54]

The SCA does not apply to "the person or entity providing a wire or electronic communications service."[55] Thus, ISPs are exempt from liability under the SCA. Unlike the Wiretap Act's service provider exemption, which is limited by a requirement that the interception occur during "the normal course of his employment while engaged in any activity . . . necessary . . . to the rendition of . . . service,"[56] the SCA's service provider exception provides an absolute exemption regardless of purpose.[57] Similar to the Wiretap Act, the SCA also contains a consent exception.[58] The SCA immunizes conduct authorized "by a user of [an electronic communication service] with respect to a communication of or intended for that user."[59]

The procedure for obtaining permission to access a stored communication that has been in storage for 180 days or less is a regular warrant supported by probable cause.[60] For a communication that has been in storage for more than 180 days, the government must provide prior notice to the subscriber and obtain "an administrative subpoena, a grand jury subpoena,

---

53. COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § III.B 86-87 (2002) [hereinafter CCIPS MANUAL], *available at* http://www.cybercrime.gov/s&smanual2002.htm; *see also* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) ("[R]etrieval of a message from post-transmission storage is not covered by the Stored Communications Act. The Act provides protection only for messages while they are in the course of transmission."), *aff'd on other grounds*, 352 F.3d 107 (3d Cir. 2003). *But see* Theofel v. Farey-Jones, 359 F.3d 1066, 1075-76 (9th Cir. 2004) (holding that the SCA applies to both read and un-read e-mail messages held in storage by an ISP).

54. 18 U.S.C. § 2703(c)(1)(C) (2000 & Supp. II 2002). The USA PATRIOT Act amended the list to include "'records of session times and durations,' 'any temporarily assigned network address,' and 'any credit card or bank account number.'" Solove, *supra* note 5, at 1283; *see* Pub. L. No. 107-56, § 210, 115 Stat. 272 (2001) (amending 18 U.S.C. § 2703(c)(2)).

55. 18 U.S.C. § 2701(c)(1) (2000). The SCA also exempts "a user of that service with respect to a communication of or intended for that user." *Id.* § 2701(c)(2).

56. *Id.* § 2511(2)(a)(i).

57. *Id.* § 2701(c)(1).

58. *Id.* § 2702(b)(3).

59. *Id.* § 2701(c). The SCA also provides exceptions for disclosures to law enforcement under certain conditions. *Id.* § 2702(b) (2000 & Supp. II 2002).

60. *Id.* § 2703(a) (2000).

a trial subpoena, or a court order."[61] In this case, the government need only offer "specific and articulable facts showing that there are reasonable grounds" to believe the communications sought are "relevant and material to an ongoing criminal investigation."[62]

Overall, the SCA is considerably less stringent than the Wiretap Act. Whereas the Wiretap Act imposes strong procedural standards and penalties against the government, service providers, and third parties who intercept electronic messages, the procedure for law enforcement to obtain permission to access stored communications is less rigorous. For example, the SCA does not require a "super-warrant" before the government can access stored messages during a criminal investigation.[63] Subpoenas require neither probable cause nor judicial approval.[64] The SCA imposes lighter penalties for violations than the Wiretap Act. Consequently, communications have a higher level of protection during the process of transmission than when stored.

Comparing the Wiretap Act to the SCA yields three major observations: (1) the government can obtain stored e-mail more easily than in-transit e-mail, (2) no suppression remedy exists for unlawfully obtained stored electronic communications, and (3) ISPs have total immunity from the primary surveillance law protecting stored communications.

C. CASE LAW UNDER ECPA

This Section discusses key cases that have contributed to the legal analysis of whether an intercept under the Wiretap Act includes only electronic communications in transit or communications in electronic storage as well. Courts' interpretation of ECPA terms such as "intercept," "electronic communication," and "electronic storage" have created a somewhat complicated and confusing body of law, which this Note recommends that Congress amend.[65]

---

61. Solove, *supra* note 5, at 1284; *see* 18 U.S.C. § 2703(b).

62. 18 U.S.C. § 2703(d) (2000 & Supp. II 2002). If the government wants to access a communication that has been in storage for more than 180 days without prior notice, then a warrant is required. *Id.*

63. Solove, *supra* note 5, at 1284; *see also* CCIPS MANUAL, *supra* note 53, at 107-36.

64. Solove, *supra* note 5, at 1284 (noting that federal subpoena power has been analogized to a "blank check").

65. *See* Bellia, *supra* note 7, at 1413 (concluding that the SCA is "complex and poorly understood").

1. Application of the Turk Contemporaneity Requirement to E-mail

Although *United States v. Turk* is a pre-ECPA case, it is important to ECPA analysis because it laid the foundation of the "contemporaneity requirement" later used by courts to determine whether an interception has occurred.[66] In *Turk*, police officers seized two cassette tapes during an arrest and later played the tapes without obtaining a search warrant.[67] The Fifth Circuit held that the officers did not violate the interception provision of the pre-ECPA federal wiretap act ("Title III").[68] The court stated that an interception occurs only when the communication is initially acquired by a recording device and heard simultaneously by the party who recorded it.[69] Thus, the court concluded that "no new and distinct interception" occurred when the officers replayed the tape recording.[70]

In *Steve Jackson Games*, the Fifth Circuit confronted the line of demarcation between the Wiretap Act and the SCA.[71] In so doing, the court examined the issue of whether an "intercept" under the Wiretap Act included only electronic communications in transit or whether it included *electronic storage* as well.[72] The district court held that, under the *Turk* rationale, the Secret Service did not violate the Wiretap Act when it seized a computer owned by Steve Jackson Games and subsequently read and deleted electronic bulletin board system ("BBS") e-mails stored on its hard drive.[73] The court found that the e-mail messages at issue were in electronic storage, and thus were not subject to interception within the meaning of the Wiretap Act.[74]

The Fifth Circuit affirmed the decision noting that, unlike the definition of "wire communication," the definition of "electronic communication" did not include electronic storage of such communications.[75] The *Steve Jackson Games* court followed *Turk* in concluding that an intercept under the Wiretap Act requires "the contemporaneous acquisition of the communication through the use of the [interception] device."[76] This is

66. United States v. Turk, 526 F.2d 654 (5th Cir. 1976).
67. *Id.* at 656-57.
68. *Id.* at 656.
69. *See id.* at 658.
70. *Id.* at 659.
71. Steve Jackson Games v. U.S. Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994).
72. *Id.*
73. *Id.* at 459.
74. *Id.* at 459-60.
75. *Id.* at 461. The Fifth Circuit also noted that ECPA is "famous (if not infamous) for its lack of clarity." *Id.* at 462.
76. *Id.* at 460 (citing United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976)).

known as the "contemporaneity requirement." The court concluded that Congress did not intend for electronic communications in electronic storage to be subject to interception within the meaning of ECPA.[77] Thus, stemming from the decision in *Turk*, the term "interception" has been interpreted to require that the communication be intercepted while in transit.[78]

The Fifth Circuit's use of the "contemporaneity requirement" from *Turk* to analyze whether an interception occurred in *Steve Jackson Games* limits Wiretap Act protection to interception of communications that are in transit. In *Konop v. Hawaiian Airlines, Inc.*, the Ninth Circuit employed the "contemporaneity requirement" from *Steve Jackson Games* and similarly found that the Wiretap Act applies only to "acquisition contemporaneous with transmission."[79] The *Konop* court reasoned that a message posted to a static, password-protected website was in electronic storage.[80] Thus, the message fell outside the purview of the Wiretap Act because it was not obtained during transmission.[81] The key issue in *Councilman* was whether an e-mail in *temporary*, electronic storage may be considered an "electronic communication" for purposes of the Wiretap Act during the course of transmission.

2. *The SCA Service Provider Exception*

In *Bohach v. City of Reno*, two police officers sent messages to one another over the Reno Police Department's paging system.[82] Following an internal affairs investigation based on the contents of the messages, the officers filed a lawsuit claiming that the City's retrieval of their stored messages violated ECPA.[83] The district court held that the plaintiffs had no claim under ECPA. It determined that the communication at issue was in electronic storage and thus not governed by the Wiretap Act's restrictions on "interception" but rather by the SCA.[84] The court also found that

---

77. *See id.* at 461-62.

78. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission.").

79. 302 F.3d 868, 878 (9th Cir. 2002).

80. *Id.* at 878-79.

81. *Id.*; *see also* United States v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004) (finding that the installation of a keystroke detector on a computer did not violate the Wiretap Act because the real-time surveillance intercepted signals confined within a computer and not the internet network).

82. 932 F. Supp. 1232, 1233 (D. Nev. 1996).

83. *Id.*

84. *Id.* at 1236.

the City, as the "provider" of the "electronic communications service" at issue, could not be prosecuted under the SCA because the SCA "allows service providers to do as they wish when it comes to accessing communications in electronic storage."[85]

In *Fraser v. Nationwide Mutual Insurance Co.*,[86] plaintiff Fraser argued that when Nationwide, his employer, conducted a search of its main file server on which Fraser's e-mail was stored, it violated the SCA.[87] The Third Circuit, however, relied on the *Bohach* analysis and exempted defendant, Nationwide, from liability due to its service provider status.[88] It concluded "[l]ike the court in *Bohach*, we read . . . [the SCA service provider exemption] literally to except from . . . [the SCA's] protection all searches by communications service providers."[89] The Third Circuit ceased its analysis of Fraser's claim upon determining that Nationwide provided the service from which the e-mail was sent rather than evaluating whether or not Fraser's expectation of e-mail privacy was reasonable within the context of his employment relationship with Nationwide.

Thus, *Bohach* and *Fraser* exemplify the degree to which a service provider receives a blanket exemption from liability once the communication at issue is considered to be in "electronic storage" under the SCA rather than "intercepted" within the meaning of the Wiretap Act. Under the SCA, service providers will not be held liable for reading their customers' e-mail.

3. *The Increasing Importance of the SCA to Electronic Communications*

In *Theofel v. Farey-Jones*, the Ninth Circuit held that the SCA governs both read and unread e-mail messages stored by an ISP.[90] The Ninth Circuit reasoned that unread e-mail messages fit comfortably within the definition of "electronic storage" because the messages were stored "for purposes of backup protection."[91] In *Theofel*, the court found that the defen-

85. *Id.* at 1236.

86. 352 F.3d 107 (3d Cir. 2003).

87. *See id.* at 114-15.

88. *Id.* at 115.

89. *Id.*

90. The Ninth Circuit acknowledged that this interpretation is contrary to the Department of Justice's interpretation that e-mail falls outside the scope of the SCA's protections when the recipient reads it. *See* Theofel v. Farey, 359 F.3d 1066, 1071 (9th Cir. 2004); *see supra* note 53 and accompanying text.

91. *Theofel*, 359 F.3d at 1075 ("[A]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the

dant, Farey-Jones, gained access to more than 339 stored e-mails from Theofel's ISP, NetGate, and thus violated the SCA.[92] The Ninth Circuit's approach in *Theofel* differs from the Fifth Circuit's holding in *Steve Jackson Games* that e-mail messages remaining on an ISP's server after delivery are not in "electronic storage" and thus fall outside the SCA's coverage.[93]

Theofel is significant for two reasons. First, the Ninth Circuit affirmed the contemporaneity requirement for claims of unauthorized interception under the Wiretap Act.[94] Second, and more importantly, the court expanded the SCA's scope beyond the Department of Justice and other courts' understanding to include e-mails that are stored by an ISP after being opened by the recipient.[95] Prior to *Theofel*, e-mail fell outside of the SCA's scope once read because storage was no longer "incidental to [transmission]."[96] However, after *Theofel*, both read and unread e-mail fall under the SCA's provisions.

II. *UNITED STATES V. COUNCILMAN*—DESCRIPTION OF THE CASE

This Part discusses the First Circuit's highly anticipated en banc decision in *United States v. Councilman*, interpreting the Wiretap Act's intersection with the SCA.[97] The en banc court reversed the First Circuit's earlier 2-1 panel decision,[98] which held that the Wiretap Act does not protect an e-mail message if it was acquired from temporary storage, illuminating the difficulty courts face when interpreting ECPA's increasingly outdated provisions. The en banc court's reversal of the problematic decision is a positive step; however, the case highlights the pressing need for Congress to revisit ECPA's confusing provisions and update the law to ensure its relevance to present-day communications technology. This Note encourages Congress to amend ECPA, with a clear statement of federal protection for e-mail privacy.

---

user needs to download it again . . . [s]torage under these circumstances thus literally falls within the statutory definition.").

92. *Id.* at 1071-72.

93. *See* Steve Jackson Games v. U.S. Secret Serv., 36 F.3d 457, 464 (5th Cir. 1994).

94. *Theofel*, 359 F.3d at 1075.

95. *Id.* at 1077-78.

96. *See* 18 U.S.C. § 2510(17) (2000).

97. 418 F.3d 67 (1st Cir. 2005).

98. *See Councilman II*, 373 F.3d 197, 203 (1st Cir. 2004), *reh'g en banc granted* and *opinion withdrawn by*, 385 F.3d 793 (1st. Cir. 2004), *reversed by*, *Councilman III*, 418 F. 3d 67 (1st Cir. 2005).

A. The First Circuit Decision (June 2004)

In *Councilman II*, a district court[99] in Massachusetts dismissed charges against Brad Councilman, former Vice President of Interloc, Inc. ("Interloc"), for copying and reading incoming messages sent to its customers' e-mail accounts.[100] Interloc was an online literary service that paired its customers, rare and out-of-print book dealers, with book buyers.[101] As part of its service, Interloc acted as an ISP and provided its customers with e-mail services.[102]

According to the indictment, Councilman directed Interloc employees to "write computer code to intercept and copy all incoming communications from Amazon.com to subscriber dealers."[103] Councilman and other Interloc employees routinely read these e-mails, seeking to gain commercial advantage over their competitor, Amazon.com.[104] The Amazon.com e-mails were monitored and copied in real-time as they entered the Interloc e-mail server, before being made available to subscribers.[105]

The government charged Councilman with conspiring to engage in conduct prohibited by the Wiretap Act.[106] However, a divided First Circuit panel found that the plain language of ECPA showed that Congress did not intend that the Wiretap Act apply to electronic communications if they were in "electronic storage."[107] According to the court, because the SCA includes the phrase "electronic storage,"[108] while the Wiretap Act's definition of "electronic communications" does not,[109] Congress did not intend the interception provisions of the Wiretap Act to apply to electronic communications in storage, whether temporary or not.

---

99. *See United States v. Councilman*, 245 F. Supp. 2d 319 (D. Mass 2003) [hereinafter *Councilman I*], *aff'd*, 373 F.3d 197 (1st Cir. 2004), *reh'g en banc granted* and *opinion withdrawn by*, 385 F.3d 793 (1st Cir. 2004), on *reh'g en banc*, 418 F.3d 67 (1st Cir. 2005).

100. *Id.* at 198. The district court reconsidered Councilman's motion to dismiss sua sponte following the Ninth Circuit's decision in Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). *See supra* Section I.C.1.

101. *Councilman II*, 373 F.3d at 198.

102. *Id.*

103. *Id.* at 199. For an overview of e-mail's history and technology, see Electronic Mail, WIKIPEDIA: THE FREE ENCYCLOPEDIA, http://en.wikipedia.org/wiki/Electronic_mail (last visited Jan. 26, 2006).

104. *Councilman II*, 373 F.3d at 200.

105. *Id.* at 199.

106. *Id.* at 198.

107. *Id.* at 213.

108. 18 U.S.C. § 2701(a)(2) (2000).

109. *Id.* § 2510(12).

The court focused on Interloc obtaining the customer e-mails while they were in "temporary storage" in a computer system, even though such storage was momentary and the e-mails were immediately made available to the users.[110] The court noted that the parties stipulated that the e-mails were not affected while they were transmitted through wires or cables between computer systems.[111] In light of these findings, the court determined that the e-mails were not "in transit" subject to the Wiretap Act protections against "interception," but were instead stored communications.[112]

In his dissent, Judge Lipez argued that the Wiretap Act and not the SCA should control *Councilman II*. Citing legislative history[113] and judicial precedent,[114] he explained that the term temporary storage in the SCA referred to e-mails sitting in a user's mailbox after transmission and prior to the user retrieving the e-mail from the mail server.[115] He concluded that the Wiretap Act, not the SCA, covered e-mails still in transmission—regardless of where the e-mails resided on the internet's complex physical infrastructure. Judge Lipez criticized the First Circuit's limitation of the Wiretap Act's protections to only e-mails traveling through cables.[116] Lipez explained that, due to the internet's decentralized architecture, e-mails stop temporarily during the delivery process when they pass through electronic switches and computers.[117] He warned that removing Wiretap Act protection from e-mails whenever they stopped momentarily during transmission negated Congress' purpose in passing ECPA: to protect electronic privacy.[118]

B. The First Circuit's En Banc Decision (August 2005)

The First Circuit's en banc decision acknowledged the "broad ramifications" of its reversal.[119] Judge Lipez, now writing for the majority, explained that an e-mail is copied and stored repeatedly as it travels across the internet.[120] The court's technical description of how e-mail works is

110. *Councilman II*, 373 F.3d at 203.
111. *Id.*
112. *See id.* at 204.
113. *Id.* at 211 (Lipez, J., dissenting) ("Councilman's approach, which would apply the Stored Communications Act to e-mails during delivery, is undermined—not supported—by legislative history demonstrating that the purpose of the ECPA was to provide greater protections to electronic communications under the Wiretap Act.").
114. *Id.* at 213-15.
115. *Id.* at 207.
116. *See id.* at 207-08.
117. *Id.* at 219.
118. *Id.*
119. *Councilman III*, 418 F.3d 67, 72 (1st Cir. 2005).
120. *Id.* at 70-72.

well-written and concise.[121] The opinion explains how data is broken into small "packets" which are then forwarded across the internet from one computer to another "until they reach their destination where they are reconstituted."[122] Providing a refreshingly adept technical explanation, the opinion discusses e-mail protocol—Simple Mail Transfer Protocol (SMTP)—and e-mail's integral "store and forward" delivery method.[123]

Of most importance, the court addressed the disparity between the inclusion of the words "electronic storage" in the definition of "wire communication" (covering phone calls) and the absence of the term from the definition of "electronic communication" (covering e-mail).[124] First analyzing the statute's plain text, the majority reasoned that although Congress inserted the term in one definition and not the other, the omission does not necessarily mean that Congress intended to exempt all electronic communications in electronic storage from the scope of the Wiretap Act.[125] The court applied the following canon of construction: "Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."[126] But the court also explained that this canon of construction "is most apt when Congress enacts a new, self-contained statute" and the two provisions are drafted with parallel language but for the use of a certain term.[127] Given ECPA's complex legislative history, the lack of uniformity between the definitions of wire communication and electronic communication, the absence of the term "electronic storage" from the explicit exceptions contained in the definition of "electronic communications," and the broad nature of the term "electronic communication," the court found that this canon's application to the statutory text is ambiguous.[128]

---

121. *See id.* at 69-70.

122. *Id.* at 69 (citation omitted). The court expressed gratitude for the assistance of several amici curiae. *Id.* at 69 n.1; *see, e.g.*, Amicus Brief of The Center for Democracy and Technology et al., United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383); Brief on Rehearing En Banc of *Amicus Curiae* Technical Experts in Support of Appellant, Urging Reversal, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383).

123. *Councilman III*, 418 F.3d at 69.

124. *Id.* at 71-72. Note that the pre-PATRIOT ACT language controls in *Councilman III*. *See supra* note 33 and accompanying text.

125. *Id.* at 76.

126. *Id.* at 73.

127. *Id.* at 74.

128. *Id.* at 72-76.

Second, the court analyzed ECPA's legislative history and reasoned that Congress included the term "electronic storage" in the definition of "wire communication" solely to bring voicemail within the Wiretap Act's scope.[129] Thus, the court found that the textual disparity was a result of congressional desire to *enhance* privacy protections for phone calls.[130] The majority of the en banc court refused to interpret the ambiguous disparity as evidence that Congress intended to remove electronic communications from the scope of the Wiretap Act for brief moments of storage during transmission.[131] Based on these findings, the court rejected Councilman's arguments and ruled that "electronic communication" includes "transient" electronic storage "intrinsic to the communication process."[132] Thus, Councilman's interception of e-mails in transient electronic storage is punishable under the Wiretap Act.

III. ANALYSIS AND RECOMMENDATIONS FOR LEGISLATIVE CHANGE

A. Analysis of the Case

The First Circuit's en banc decision to reverse should be commended. *Councilman II* created serious problems because e-mail messages always pass through temporary storage during transmission.[133] Under *Councilman II*, the legal protection afforded to an e-mail would switch between Wiretap Act protection and SCA protection as it traversed the internet, depending on whether the message was in transit between intermediate servers or stored temporarily—often for less than a second—on one of those servers.[134] First, this outcome would weaken the privacy protections for e-mail by limiting the scope of the Wiretap Act. Second, the holding would move the overwhelming majority of claims for unauthorized access to e-mail under the SCA rather than the Wiretap Act.

If intercepting an e-mail from temporary storage during transmission is not considered an "intercept" under the Wiretap Act, then at many intermediate points an e-mail would only receive the lesser protections of the

129. *Id.* at 78.

130. *See supra* note 33 and accompanying text for the definition of "wire communication."

131. *Councilman III*, 418 F.3d 67, 44 (1st Cir. 2005).

132. *Id.*

133. *See id.* at 79 (describing the "store and forward" delivery method for e-mail).

134. *Councilman II*, 373 F.3d 204 (1st Cir. 2004). The First Circuit even acknowledged this problem in *Councilman II*. *Id.* at 204 ("[ECPA] may be out of step with the technological realities of computer crimes.").

SCA. As Judge Lipez warned in his dissent from *Councilman II*, this interpretation of the Wiretap Act "would undo decades of practice and precedent regarding the scope of the Wiretap Act and would essentially render the Act irrelevant to the protection of wire and electronic privacy."[135] This result is at odds with Congress' intent in passing ECPA to provide consistent legal treatment to electronic communications across different communication technologies.[136] Hinging privacy protection on whether a packet of data is stopped momentarily almost invites a technical end-run around personal privacy. Potentially, any company that provides internet services could build its internet infrastructure such that all e-mail messages are placed in temporary storage, even for a nanosecond.

Although correct in result, the First Circuit's en banc decision in *Councilman III* highlights, and leaves unresolved, three major problems with the existing statutory regime. First, ECPA's definition of "intercept"—a key term for determining whether a violation under the Wiretap Act has occurred—is confusing and such ambiguity is likely to lead to conflicting interpretations in federal court. Second, ISPs are immune from the SCA's provisions and cannot be held liable for reading their customers' e-mail unless their actions fall under the definition of "intercept" contained in the Wiretap Act. Third, internet surveillance law provides unequal protection for the contents of an e-mail based on technical evaluations of the physical point at which it was obtained rather than the underlying privacy interest. These problems are integral to ECPA's statutory framework, regardless of the positive outcome in *Councilman III*.

B. Legislative Options for Amending ECPA[137]

Congressional reform of ECPA is overdue. Section B discusses three opportunities for Congress to improve ECPA. The legislative proposals include simple statutory amendments that can be enacted immediately. Utilizing a long-term approach, it may be helpful to reconsider the relationship between ECPA's two-tier framework and modern expectations of e-mail privacy.

---

135. *Id.* at 219 (Lipez, J., dissenting).

136. *See generally* Brief on Rehearing En Banc for Senator Patrick J. Leahy as *Amicus Curiae* Supporting the United States and Urging Reversal, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), *available at* http://www.epic.org/privacy/councilman/leahy_amicus.pdf.

137. The proposed modifications contained in Section III.B.1-2 were developed in conjunction with staff attorneys and Patrick Mueller, a participant in the Internet Public Interest Opportunities Program (IPIOP), at the Electronic Privacy Information Center (EPIC), a public interest research center in Washington, D.C., following the decision in *Councilman II*.

1. ECPA's Confusing Definition of "Intercept"

The Wiretap Act defines the term intercept as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[138] Although *Councilman III* addressed the question of "electronic storage," it remains unclear what action constitutes an "intercept" for the purposes of triggering the Wiretap Act. *Councilman III* breathed life back into the dominant view that "interception" extends *from* the point at which the message is sent *to* the final destination where it is made available to the recipient.[139] Clarification of the intended line of demarcation between the Wiretap Act and the Stored Communications Act will help courts consistently determine liability for unauthorized internet surveillance.

Congress should amend the definition of intercept to provide unambiguous protection under the Wiretap Act to an e-mail that is intercepted along the pathway by which it is being sent from one person to another. Assuming the presence of political will, amending the definition of "intercept" to include in-transit electronic storage is an extremely simple statutory change. Following the First Circuit's decision in *Councilman II*, two bills were proposed to fix the definition of "intercept" in the Wiretap Act: the E-mail Privacy Act of 2004[140] and the E-mail Privacy Protection Act of 2004.[141] Although the E-mail Privacy Act of 2004 attracted fourteen cosponsors, the 108th Congress failed to amend the definition of "intercept."[142] It is possible that Congress was waiting for the *Councilman III* ruling before determining how to proceed.

---

138. 18 U.S.C. § 2510 (2000).

139. *See, e.g.*, Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1323-24 (2005).

140. H.R. 4956, 108th Cong. (2004), *available at* http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4956:. Representative Jay Inslee (D-WA) introduced the E-mail Privacy Act of 2004 which addressed two weaknesses in ECPA—the unclear definition of "intercept" in the Wiretap Act and the broad service provider exemption in the SCA—highlighted in *Councilman*. The proposed language would clarify that "interception" of an electronic communication "includes the acquisition of the contents of the communication through the use of any electronic, mechanical, or other device, at any point between the point of origin and the point when it is made available to the recipient." *See id.*

141. H.R. 4977, 108th Cong. (2004), *available at* http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4977:. This second bill was introduced by Representative Jerrold Nadler (D-NY) to address the same two ECPA issues. Representative Nadler's proposal would amend the definition of "intercept" to include "any temporary, intermediate storage of that communication incidental to the electronic transmission thereof" within the meaning of intercept. *See id.*

142. *See* H.R. 4956, Bill Cosponsors, http://thomas.loc.gov/cgi-bin/bdquery/z?d108:-HR04956:@@@P (last visited Mar. 14, 2006).

Currently, the pending E-mail Privacy Act of 2005, would revise the definition of "intercept" to explicitly include acquisition of the contents of an electronic communication on an ongoing basis during transmission, including a "communication simultaneously in electronic storage."[143] The bill amends the Wiretap Act's protections for e-mail from unauthorized "intercept" during transit, regardless of whether the message passes through temporary storage. Such an amendment would help state and federal judges apply federal law governing unauthorized interceptions consistently across jurisdictions. For the benefit of companies, law enforcement, and private actors, Congress should approve this simple yet robust legislative amendment to minimize ambiguity.

2. The ISP Liability Loophole

This Section discusses the ISP service provider exemption, legislative options for closing the loophole, and arguments for and against statutory reform.

a) The Problem of Internet Service Provider Immunity

ISPs are immunized from liability for what would otherwise be considered unlawful activity solely on the basis of their status as electronic communication service providers. ISPs cannot be prosecuted under the Wiretap Act if they continually surveil e-mail from users' mailboxes.[144] ISPs are also exempt under the SCA for such behavior provided they do not *disclose* the contents of the communications to another party.[145] Although ISP access to customer e-mail may be justified by certain technical requirements of providing service, such as to perform quality assurance of e-mail content display, to check spelling, or to assess whether a hacker has accessed an e-mail account, the SCA grants Councilman blanket immunity from all civil and criminal liability.[146] Furthermore, the ISP exception prevents customers whose privacy was violated from filing civil causes of actions under the SCA.

The government did not charge Councilman under the SCA, presumably because of the extremely broad service provider exception. Even though the First Circuit acknowledged that the purpose of Councilman's

143. E-mail Privacy Act of 2005, H.R. 3503, 109th Cong. (2005); S. 936, 109th Cong. (2005). The proposed bills contain identical language and are sponsored by Senator Leahy (D-VT) and Representative Cannon (R-UT) in the Senate and House, respectively.

144. *See* 18 U.S.C. § 2701(c)(1) (2000).

145. *See* § 2702 in the Stored Communications Act, which states that an electronic service provider may not disclose customer content to others. 18 U.S.C. § 2702 (2000).

146. *Id.* § 2701(c)(1).

actions was to learn about competitors and obtain a commercial advantage,[147] which warrants a greater penalty under the SCA,[148] the absolute exemption for service providers makes irrelevant the purpose for which Interloc obtained its customers' communications. Furthermore, if Interloc had copied e-mails *after* they were delivered to customers' mailboxes there would be no action under ECPA.[149] Thus, a trivial change in the company's surveillance system would have prevented any cause of action under federal surveillance law.

After *Councilman II*, news media commentators downplayed the importance of the ruling by reassuring e-mail users that "most major internet providers have explicit policies against reading their customers' e-mail messages."[150] On one hand, no major ISP is known to read its customer's e-mail messages as a matter of standard policy. However, a recent class-action lawsuit filed by the Electronic Frontier Foundation accuses AT&T of collaborating with the National Security Agency's domestic surveillance program to intercept international phone and internet communications of U.S. citizens without search warrants.[151]

Furthermore, review of the terms of service for some of the largest ISPs in the United States—MSN,[152] EarthLink,[153] AT&T,[154] Google,[155]

147. *Councilman II*, 418 F.3d 67, 71 (1st Cir. 2005).

148. 18 U.S.C. § 2701(b)(1) (2000).

149. As long as a provider surveils its customer's messages after delivery to a destination server, it may do so without being subject to the Wiretap's limitation. *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) (concluding that unauthorized access to a secure web site did not constitute an interception under the Wiretap Act).

150. *See, e.g.*, Saul Hansell, *You've Got Mail (and Court Says Others Can Read It)*, N.Y. TIMES, July 6, 2004, at C2, *available at* http://www.nytimes.com/2004/07/06/technology/06net.html?pagewanted=1&ei=5070&en=2c3b981211419e5f&ex=1109307600&adxnnl=0&oref=login&adxnnlx=1109220522-46Zj4tVIhIr55MUNFHxjJw.

151. Plaintiff's Amended Complaint at 16-21, Hepting v. AT&T Corp., No. 3:06cv672 (N.D. Cal. filed Feb. 22, 2006), *available at* http://www.eff.org/legal/cases/att/att_complaint_amended.pdf; *see also* John Markoff, *AT&T Is Accused In Eavesdropping*, N.Y. TIMES, Feb. 1, 2006, at A20.

152. MSN's Website Terms of Use and Notices states: "To the maximum extent permitted by applicable law, Microsoft *may monitor your e-mail*, or other electronic communications and may disclose such information . . . ." MSN Website Terms of Use and Notices, http://privacy.msn.com/tou (last visited Mar. 13, 2006) (emphasis added).

153. EarthLink's Internet Service Agreement states: "EarthLink has no obligation to monitor the Services, but *may do so* and disclose information regarding use of the Services *for any reason* if EarthLink, in its sole discretion, believes that it is reasonable to do so . . . ." EarthLink Internet Service Agreement, http://www.EarthLink.net/about/policies/dial/ (last visited Jan. 23, 2006) (emphasis added).

and AOL[156]—reveals that self-regulation by the ISP industry creates gaps in consumer privacy protection for e-mail.[157] Many ISPs appear to reserve the right to monitor their customers' e-mail. Virtually all ISPs reserve the right to change the terms of their privacy policy.[158] Although it is possible

---

154. AT&T's Online Privacy Policy states: "The company will not read or disclose to third parties private e-mail communications that are transmitted using AT&T services except as required to operate the service or as *otherwise authorized by law*." AT&T's Online Privacy Policy, http://www.att.com/privacy (last visited Jan. 23, 2006) (emphasis added).

155. Google's Gmail Privacy Notice states:

> *Google maintains and processes your Gmail account and its contents* to provide the Gmail service to you and to improve our services. . . . Google's computers process the information in your messages for various purposes. . . . Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers *and may remain in our offline backup systems.*

Gmail Privacy Notice, http://gmail.google.com/mail/help/privacy.html (last visited Jan. 23, 2006) (emphasis added).

156. AOL's Agreement to Rules of User Conduct states: "America Online *generally* does not pre-screen, monitor, or edit the content posted by users of communications services, chat rooms, message boards, newsgroups, software libraries, or other interactive services that may be available on or through this site." AOL Agreement to Rules of User Conduct, http://www.aol.com/copyright/rules.html (last visited Jan. 23, 2006) (emphasis added). In contrast, AOL's Terms of Service for paying customers of AOL's e-mail service states:

> *[AOL does] not read your private online communications.* . . . [except] in response to legal process (for example, a court order, search warrant or subpoena); in other circumstances in which AOL believes the AOL Service is being used in the commission of a crime; when we have a good faith belief that there is an emergency that poses a threat to the safety of you or another person; or when necessary either to protect the rights or property of AOL, or for us to render the service you have requested . . . .

AOL Privacy Policy, http://about.aol.com/aolnetwork/mem_policy#2 (last visited Jan. 23, 2006) (emphasis added).

157. *See* Doug Isenberg, *Do ISPs' Policies Allow Them to Monitor E-mail?*, GIGALAW.COM, July 8, 2004, http://www.gigalaw.com/2004/07/do-isps-policies-allow-them-to-monitor.html.

158. *See* MSN Website Terms of Use and Notices, http://privacy.msn.com/tou ("Microsoft reserves the right to change the terms, conditions, and notices under which it offers the MSN Web Sites, including any charges associated with the use of the MSN Web Sites. You are responsible for regularly reviewing these terms, conditions and notices, and any additional terms posted on any MSN Web Site. Your continued use of the MSN Web Sites after the effective date of such changes constitutes your acceptance of and agreement to such changes.") (last visited Mar. 18, 2006); EarthLink Privacy Policy, http://www.EarthLink.net/about/policies/privacy ("EarthLink reserves the right to revise, amend, or modify this policy and our other policies and agreements at any time and in any manner.") (last visited Jan. 23, 2006); AT&T's Online Privacy Policy, http://www.

that ISPs will not read their customers' e-mail due to resource constraints, lack of interest, inconsistencies with their business models, or private contracting, consumers are in a weak position because it is very difficult to know whether an ISP is reading and using the contents of a customer's private communications.

A review of industry privacy policies indicates that self-regulation by the ISP industry results in a default standard of allowing ISPs to read customer e-mail. Without a statutory limitation on ISP surveillance power, customers will never know if a message to a friend, spouse, financial institution, or doctor is being read by their service provider. Furthermore, recent news reports describing the U.S. government's warrant-less domestic surveillance program raise serious concerns about ISP monitoring, use, and retention of customer e-mail content, in addition to the legality of downstream ISP disclosure to government officials absent judicial authorization.[159] Thus, the problem is not that a majority of ISPs are currently engaging in e-mail surveillance but rather—given the absence of a minimum standard in the SCA—the lack of transparency into what ISPs are or are not doing.

Furthermore, the practices of major ISPs fail to dispel concerns regarding smaller, less financially-stable, providers that may perform at the outer limits of industry practices. This uncertainty raises privacy concerns about protections afforded to e-mail and First Amendment concerns about the potential chilling effect on free speech.[160] A legal architecture that fails to ensure e-mail privacy hinders the public interest in open expression because users may modify and self-censor online communication for fear of being watched.

The SCA loophole for ISPs and their employees creates a potentially significant problem when considered in the context of corporate structures

---

att.com/privacy ("AT&T will keep this Policy current. The company will inform you of any changes that we make.") (last visited Jan. 23, 2006); Google Privacy Policy, http://www.google.com/privacypolicy.html ("Please note that this Privacy Policy may change from time to time. We will not reduce your rights under this Policy without your explicit consent. . . .") (last visited Jan. 23, 2006); AOL's Privacy Policy, http://www.aol.com/info/privacy.adp#princ8 ("Whenever we change our policy, we will give you 30 days' notice of those changes through prominent disclosures, including notification on our front screen.") (last visited Jan. 23, 2006).

159. *See, e.g.*, Eric Lichtblau & James Risen, *Domestic Surveillance: The Program; Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, at A1.

160. *See, e.g.*, Marc Rotenberg, *We Are All Privacy Fundamentalists*, *in* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 53-54 (2003) ("Without the right of privacy, there could be no public life.").

and market forces.[161] Increasingly, ISPs exist as subsidiaries of larger parent corporations.[162] The trend towards consolidation of information technology and media companies increases the probability that ISPs will have an incentive to secretly access customer e-mails for reasons unrelated to the delivery of internet service such as customer profiling and direct marketing. A large financial holding or global media corporation could have thousands of affiliates.[163] Therefore, one ISP's access to customer e-mail could translate into access for an unknown number of affiliated business units or subsidiaries under the ISP's parent company.[164]

In the absence of a statutory limitation on ISP access, the SCA provides no counter-balance to the market incentive for ISPs to capitalize on the economic value of personal information contained in e-mails. Customers have limited insight into how, and for what purposes, the personal information communicated in e-mails may be used by ISPs. Corporate data-mining for purposes of commercial gain unrelated to the delivery of ISP service is allowed, if not encouraged, by the SCA's broad ISP exemption. A default rule of complete access distorts the power balance between ISPs and customers. Furthermore, if such information is misused by one of the institution's subsidiaries for fraudulent purposes, individuals may be unable to identify the offender due to the lack of visibility of information-sharing policies.

b) Solutions for Closing the ECPA Loophole

Legislative action is required to ensure that ECPA's original purpose to provide federal privacy protection to electronic communications is not outpaced by technological advances that render the statute's privacy provisions obsolete. To close the ECPA service provider loophole, Congress should restrict the broad service provider exemption under the SCA to be consistent with the exemption under the Wiretap Act.

---

161. Recall that *Theofel* moves opened e-mail under the SCA and thus simultaneously expands the quantity of e-mail left unprotected by the ISP liability loophole. *See supra* Section I.C.3.

162. *See, e.g.*, TimeWarner Home Page, http://www.timewarner.com/corp; *see also* Press Release, News Corporation, News Corporation to Acquire Intermix Media, Inc., Acquisition Includes World's Fastest-Growing Social Networking Portal, MySpace.com, July 18, 2005, *available at* http://www.newscorp.com/news/news_251.html.

163. CitiGroup, Inc., for example, has over 2,700 corporate affiliates. *See Financial Privacy and Consumer Protection: Hearing Before the S. Comm. on Banking, Housing and Urban Affairs*, 107th Cong. (2002) (statement of William H. Sorrell, Attorney General, State of Vermont).

164. The number of business units or subsidiaries could equal tens, hundreds, or possibly even thousands.

The Wiretap Act exemption recognizes that service providers may need to monitor communication in certain circumstances, but these circumstances should be limited.[165] Thus, it enables telecommunications service providers to intercept wire communications and perform random quality-control checks for purposes of delivering service.[166] In contrast, the SCA exempts from liability conduct authorized "by the person or entity providing a wire or electronic communications service."[167]

To protect e-mail from unauthorized searches by commercial service providers, and to maintain consistency between the Wiretap Act and the SCA, Congress should amend the SCA service provider exception by modeling the Wiretap Act exception. Under the proposed amendment, ISPs would retain the right to monitor a customer's e-mail in the course of any activity necessary to providing service. For example, an ISP's engineer could log into a customer's e-mail account to analyze why e-mail messages were not being displayed correctly. However, when an ISP's access to customer e-mail is not justified by the normal course of business, such access would be limited not only by an ISP's voluntary privacy policy but by a legislative SCA requirement.

Recent e-mail privacy bills have offered promising improvements in this area. The proposed E-mail Privacy Act of 2004, which was not adopted, would have added the following limitation to the service provider exception: "to the extent the access is a necessary incident to the rendition of the service, the protection of the rights or property of the provider of that service, or compliance with section 2702 [providing exceptions for consent and disclosure to law enforcement]."[168] This language would narrow the SCA exemption to be similar to the Wiretap Act exemption and could be amended to the pending E-mail Privacy Act of 2005.[169]

---

165. 18 U.S.C. § 2511(2)(a)(i) (2000).

166. *Id.*

167. *Id.* § 2701(c).

168. *See* E-mail Privacy Act of 2004, H.R. 4956, 108th Cong. (2004), *available at* http://thomas.loc.gov/cgi-bin/query/C?c108:./temp/~c108DYA5JB.. A second bill was introduced by Representative Jerrold Nadler (D-NY) to amend the SCA service provider exception by prohibiting a provider of an electronic communications service from acquiring or using the contents of a stored communication other than for the purposes of providing the electronic communication service. Therefore, ISP snooping without a business purpose justification would be expressly prohibited. The proposed bill imposed a civil fine and a maximum prison sentence of five years. *See* E-mail Privacy Protection Act of 2004, H.R. 4977, 108th Cong., *available at* http://thomas.loc.gov/cgi-bin/query/D?c108:1:./temp/~c108xVWX2y.

169. E-mail Privacy Act of 2005, S. 936, 109th Cong; *see supra* note 143 and accompanying text.

c) Critiques of Proposed Statutory Modification: Free-Market Regulation

Information law scholar Fred Cate argues that private sector accommodation is preferable to legislative approaches.[170] Cate argues that individual responsibility, mutual agreements, and market-based accommodations are usually more effective than legal regulation in protecting privacy.[171] Free-market advocates might criticize proposed privacy regulations[172] for interfering with the private relationship between ISPs and their customers and disrupting the free-market for electronic communications service. In weighing the importance of privacy, Cate reasons that it is important to recognize that "protecting privacy imposes real costs" including higher costs of providing products and services, decreased service quality, and barriers to crime prevention and the protection of private property.[173] In the case of e-mail surveillance, free market scholars might argue that the government should encourage ISPs and customers to enter into private contractual agreements concerning customer e-mail privacy. Cate argues that national law could ensure industry accountability through legal requirements of notice and consent, without imposing the potential service "costs" on all customers.[174]

On the other hand, privacy scholars have analyzed the limits of self-regulation in the privacy context.[175] Discussing the failures in the privacy market, Professor Paul Schwartz writes:

> The emerging verdict of many privacy scholars is that existing markets for privacy do not function well. Due to such market failures, which are unlikely to correct themselves, propertization of personal information seems likely to lead to undesired results—even to a race to the bottom as marketplace defects lead

170. FRED H. CATE, PRIVACY IN THE INFORMATION AGE ix (1997).

171. *Id.* For example, Cate advises that "[i]ndividual responsibility, not regulation, is the principal and most effective form of privacy protection in most settings." *Id.* at 131.

172. H.R. 4956, 108th Cong. (2004); S. 936, 109th Cong. (2005).

173. Cate, *supra* note 170, at 102.

174. *Id.* at 108-21.

175. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 532-40 (1995); *see also* Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423-24 (2000) (arguing that market-based approaches to privacy rights treat preferences for information privacy as a matter of individual taste, but the values of information privacy are more fundamental).

> competitors to take steps that are increasingly harmful to privacy.[176]

The main concern with allowing ISP industry self-regulation is that many individuals do not know how their information is processed.[177] Schwartz references a recent report from the Annenberg Public Policy Center finding that "the overwhelming majority of U.S. adults who use the internet at home have no clue about data flows—the invisible, cutting-edge techniques with which online organizations extract, manipulate, append, profile and share information about them."[178] Schwartz argues that the unequal balance of information available to consumers and industry players, in addition to the relative vulnerability of consumers within the larger market, requires close scrutiny of and skepticism about the commodification of personal data.[179]

In the case of e-mail privacy, economic incentives alone will not pressure ISPs to adequately protect customer privacy. Private markets do not provide consumers with a meaningful choice concerning the issue of ISP e-mail monitoring because potentially invasive activities are invisible to the decision-making consumer when he or she is selecting a service provider. In addition, consumers have little insight into or oversight of ISP activity once they commence using a company's service. Furthermore, the major ISPs explicitly reserve the right to monitor their customers' e-mail.[180] Even if a customer decides to change ISPs, the switching costs are high including the hassle of changing one's e-mail address and contractual commitments to the ISP.

If Congress seeks to provide meaningful privacy protection to e-mail communications, it should correct the market imbalances and close the ISP loophole under the SCA. Under this statutory approach, customers may continue to enter into private agreements with ISPs to allow e-mail surveillance in exchange for potential service benefits. However, due to the imbalance in information available to ISPs and customers, a default

---

176. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2076 (2004).

177. *Id.* at 2078.

178. *Id.* at 2078 (citing JOSEPH TUROW, ANNENBERG PUB. POLICY CTR. OF THE UNIV. OF PA., AMERICANS AND ONLINE PRIVACY: THE SYSTEM IS BROKEN 4 (2003), *available at* http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf).); *see also* Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CALIF. L. REV. 395, 476 (2000).

179. Schwartz, *supra* note 176, at 2078-79.

180. *See supra* Section III.B.2.a.

statutory rule of no surveillance is necessary to ensure a baseline of privacy protection for e-mail.

3. *Wiretap Act v. the SCA: The Problem of Unequal Treatment*

E-mail receives "second-class" treatment under the SCA compared to the more stringent protections for telephone calls under the Wiretap Act.[181] ECPA also affords greater protection to an e-mail message *before* it reaches its destination than *after* it resides at a single destination.[182] This statutory distinction implies that minor changes in the physical point of interception will determine whether an e-mail is protected under the Wiretap Act or the SCA. Under this approach, the level of privacy protection afforded to an electronic communication is determined by a technology-dependent analysis of the point at which a communication was intercepted. For most e-mail users, neither the medium of communication nor the physical point of interception mitigates the intrusiveness or threat to civil liberties when private e-mails are surveilled. It is time to rethink the limits of ECPA's statutory regime.

The legislative proposals above offer a good start for ensuring e-mail privacy, but they are incomplete. The recommendations maintain a privacy regime for electronic communications that lowers privacy protection once a communication is made available to its recipient. Maintaining multiple statutory schemes for e-mail privacy does not solve the deeper problem of unequal privacy protection for e-mail that depends on the location of the data on the internet network. Ultimately, Congress should reevaluate the public interest in e-mail privacy and create a new regulatory scheme that provides consistent legal protection regardless of the point of surveillance.

The success of the internet as an effective medium for communication depends on public trust in the security and privacy of the network. Congress should therefore evaluate the normative reasons why e-mail is afforded privacy protection. Under ECPA, the protections of the Wiretap Act's "super" search warrant requirement end when a message is made available to its recipient. Congress should evaluate whether to adopt a default standard with stronger privacy protection, one which requires search warrants supported by probable cause for all e-mail surveillance.[183] To protect law enforcement's flexibility, Congress could draft statutory ex-

181. *See* Solove, *supra* note 5, at 1281.
182. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002).
183. For the best summary of this argument, see Solove, *supra* note 5, at 1298-1303.

ceptions for circumstances in which search warrants are inappropriate or overly burdensome.[184]

Alternatively, Congress could amend ECPA to distinguish between read and unread e-mail for purposes of privacy protection. This approach is less arbitrary than the "storage-transit" distinction because a user is afforded the opportunity to read and delete the message. Unfortunately, this approach disadvantages users who leave messages on an ISP's server for backup or storage purposes, which will likely have the greatest effect on individuals who do not own personal computers.

A third option is to protect both read and unread e-mail messages with the procedural requirement of a search warrant for a certain window of time (60 days, 180 days, 1 year, etc.). After the window of time has passed, then the messages would fall into a lower category of protection. For significant privacy protection, Congress could require a long window of time.

Ultimately, the legislative body should create a privacy framework based upon reasonable expectations of privacy for electronic communications.[185] This approach would lead to a favorable and unified regime that protects the privacy of electronic communication without raising difficult technical questions for the courts concerning the location of data at the point of interception.

IV. CONCLUSION

Throughout history, privacy law has responded to public concerns about the effect of emerging technologies on personal privacy.[186] As the use of e-mail and other electronic communications technologies such as

184. *Id.* Congress could also extend the Wiretap Act's exclusionary rule to improperly acquired stored messages under the SCA. *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 220-221 (2004).

185. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967). In the absence of judicial recognition of an individual's reasonable expectation of privacy when relying on an ISP to send electronic communications, Congress should provide adequate statutory protections for e-mail under ECPA.

186. *See, e.g.*, ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE, PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 6-7 (2000) ("First, in the years before 1890, came cameras, telephones, and high-speed publishing; second, around 1970, came the development of computers; and third, in the late 1990s, the coming of personal computers and the World Wide Web brought renewed interest in [privacy] . . . . What worried people was not so much the technology; what worried them was that it was in the hands of large and powerful organizations.").

VoIP,[187] text-messaging, and online chat increases the degree of personal information disseminated across the internet, so too does the need to analyze federal privacy protections for electronic communications. Unless Congress takes action to back with the force of law the obligations of service providers to refrain from snooping on their customers, the legal, economic, and network architecture of the electronic communications infrastructure will continue to encourage surveillance.

Councilman III teaches us that courts are struggling to apply ECPA's twenty-year-old provisions to modern-day electronic communications technology. As the amount of information collected, stored, and transferred electronically increases, coupled with the increasing use of electronic devices to communicate and monitor sensitive information, a clear statement from Congress clarifying ECPA generally and the obligation of ISPs to refrain from reading their customers e-mails particularly, is crucial to the public interest in electronic privacy.

187. Voice Over IP, also called "Internet telephony," enables telephone conversations over the internet (or a dedicated Internet Protocol (IP) network). *See* VoIP, WIKIPEDIA: THE FREE ENCYCLOPEDIA, http://en.wikipedia.org/wiki/Voip (last visited Jan. 23, 2006). Emerging technologies, such as VoIP, call into question the law's traditional distinction between voice and data communications such as e-mail.