Harvard Journal of Law & Technology
Volume 19, Number 1 Fall 2005

A THINLY VEILED REQUEST FOR CONGRESSIONAL ACTION ON E-MAIL PRIVACY: *UNITED STATES V. COUNCILMAN*

TABLE OF CONTENTS

I. INTRODUCTION

Congress first responded to privacy concerns raised by the development of electronic mail with the Electronic Communications Privacy Act of 1986 ("ECPA").[1] Title I of the ECPA, which set out criminal penalties for one who "intentionally intercepts . . . electronic communications,"[2] provided a legal framework to protect text- or data-based communications from unauthorized access.[3] Nineteen years later, however, that framework is the cause of substantial legal confusion because its language does not correspond accurately to the technology used in e-mail.

---

1. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2711 (1998)). For a discussion of the state of e-mail regulation prior to the ECPA, see Ruel T. Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J. 17, 17–19 (1988).

2. 18 U.S.C. § 2511(1).

3. Robert W. Kastenmeier et al., *Communications Privacy: A Legislative Perspective*, 1989 WISC. L. REV. 715, 728 (1989).

The First Circuit waded into that confusion in its lengthy, contentious consideration of *United States v. Councilman*.[4] Originally, a divided panel held that an e-mail provider did not violate the ECPA when it copied e-mail messages held temporarily in electronic storage prior to delivery, stored those messages, and subsequently read them.[5] After withdrawing the panel opinion,[6] an en banc court reversed, concluding that the messages remained "electronic communications" and thus were covered by the ECPA, even when in temporary storage.[7] Stating that the issues were not "implicate[d]," however, the court declined to answer the more difficult questions of "whether the term 'intercept' applies only to acquisitions that occur contemporaneously with the transmission of a message from sender to recipient" and, if so, whether interference with a message in temporary storage en route to the recipient occurs contemporaneously with transmission.[8]

This Recent Developmentargues that a proper analysis of *Councilman* required a definition of "intercept" and, consequently, that the First Circuit was wrong to avoid it. It then argues that, although the First Circuit reached the correct outcome in *Councilman II*, Congress should respond to its difficulty in doing so by amending the ECPA to increase its clarity. Part II looks at the complex web of statutes governing communications privacy and considers the interpretative problems involved. Part III examines the First Circuit's attempt in *Councilman* to solve one of those problems and dodge another. Finally, Part IV makes the case for further congressional action to settle lingering legal uncertainties and evaluates existing proposals for legislative reform.

II. STATUTORY FRAMEWORK

One of the strongest recurring concerns voiced about the adoption of new technologies is their potential impact on personal privacy.[9] Recognizing both the moral force[10] and practical impact[11] of such

4. United States v. Councilman (*Councilman II*), 418 F.3d 67 (1st Cir. 2005) (en banc), *rev'g* 373 F.3d 197 (1st Cir. 2004).

5. United States v. Councilman (*Councilman I*), 373 F.3d 197, 198 (1st Cir. 2004).

6. United States v. Councilman, 385 F.3d 793, 793 (1st Cir. 2004), *withdrawing and vacating Councilman I*, 373 F.3d 197 (1st Cir. 2004).

7. *Councilman II*, 418 F.3d at 79.

8. *Id.* at 80.

9. *See, e.g.*, Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 394 (2002); R. Ken Pippen, *Consumer Privacy on the Internet: It's "Surfer Beware,"* 47 A.F. L. REV. 125, 126 (1999); Richard Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 176–77.

10. *See Surveillance Technology: Joint Hearings Before the Subcomm. on Constitutional Rights of the S. Comm. on the Judiciary and the Spec. Subcomm. on Science, Technology and Commerce of the S. Comm. on Commerce*, 94th Cong. 1 (1975) (opening statement of Sen. John V. Tunney) ("Technological developments are arriving so rapidly and are chang-

fears, Congress often tries to assuage them. Yet Congress is fighting an uphill battle: the legislative process in the United States is designed to be slow and deliberative,[12] while communications technology has developed rapidly.[13] Efforts to craft statutes "in a manner that will have continued applicability despite further technological advances"[14] have failed — Congress has, by necessity, continued to add new layers onto the stratified body of communications privacy law.[15]

A. Prehistory: The Statutory Framework Before the ECPA

Congress first addressed the issue of communications privacy in a comprehensive manner through the 1968 Wiretap Act ("1968 Act").[16] That Act simultaneously established penalties for unauthorized private interceptions of wire communications and set forth conditions under which law enforcement officers could intercept such communications. Three factors, however, prevented it from adapting to the subsequently emerging world of text and digital communication. First, the 1968 Act covered only "wire or oral" communications.[17] Second, though it defined interception to include acquisition through "the use of any electronic, mechanical, or other device," the 1968 Act limited interception to "aural acquisition."[18] Third, it applied only to wire communications "operated by . . . a common carrier," leaving out private networks.[19] Consequently, it excluded electronic communication methods almost entirely.[20]

---

ing the nature of our society so fundamentally that we are in danger of losing the capacity to shape our own destiny.").

11. *See Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the Comm. on the Judiciary*, 99th Cong. 19–27 (1986) (testimony of Philip M. Walker, Vice Chairman, Electronic Mail Association, accompanied by Michael F. Cavanaugh, Executive Director, Electronic Mail Association) (arguing that inadequate legislation protecting privacy would reduce or eliminate the commercial viability of e-mail).

12. *See* HENRY M. HART & ALBERT SACKS, THE LEGAL PROCESS: BASIC PROBLEMS IN THE MAKING AND APPLICATION OF LAW 166–67 (10th ed. 1958).

13. *See* UNITED NATIONS DEV. PROGRAMME, HUMAN DEVELOPMENT REPORT 2001, 29–35, 46–65 (2001) (cataloging the scope and impact of advances in communications technology, especially since 1950).

14. Lisa Ann Wintersheimer, *Privacy Versus Law Enforcement — Can the Two Be Reconciled?*, 57 U. CIN. L. REV. 315, 316 (1988).

15. *See id. See generally* Bruce E. Fein, *Regulating the Interception and Disclosure of Wire, Radio, and Oral Communications: A Case Study of Federal Statutory Antiquation*, 22 HARV. J. ON LEGIS. 47 (1985) (focusing on problems created by the unforeseen development of the cordless telephone).

16. Omnibus Crime Control and Safe Streets Act of 1968, tit. III, §§ 801–804, 82 Stat. 211 (codified at 18 U.S.C. § 2510 *et seq*.).

17. 18 U.S.C. § 2510(4) (1982).

18. *Id.* Courts have read that requirement literally to require acquisition "through the sense of hearing." Smith v. Wunker, 356 F. Supp. 44, 46 (D. Ohio 1972).

19. 18 U.S.C. § 2510(1).

20. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1, 165–68 (1977) (holding that the 1968 Act does not regulate use of pen registers because they do not hear or monitor

Over the next fifteen years, Congress acted to fill in relatively minor gaps left by the 1968 Act. In 1978, for example, it curbed the use of pen registers[21] and restricted access to electronic bank records.[22] Until the passage of the ECPA in 1986, however, privacy protection for data- and text-based communication, especially e-mail, remained a gaping hole in the statutory regime.[23]

B. Genesis of the Modern Law: The Electronic Communications Privacy Act

The ECPA filled the statutory hole in two ways. Title I, now itself known as the Wiretap Act, directly amended the 1968 Act to establish criminal penalties for anyone who "intentionally intercepts . . . any wire, oral, *or electronic communication*."[24] Title II, known as the Stored Communications Act, added similar penalties for anyone acting without permission[25] who "intentionally accesses without authorization [or in excess of authorization] a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage."[26]

The statute also modified the protections afforded to wire communications in two ways that have proven relevant to its treatment of electronic communications. First, it eliminated the strict requirement of a common carrier,[27] though it did retain some distinctions between public and private service providers.[28] Second, it explicitly amended the 1968 definition of wire communication to include "any electronic

---

sound); United States v. Seidlitz, 589 F.2d 152, 157 (4th Cir. 1978) (reaching same conclusion regarding a spy device that tracked computer activity).

21. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1811 (1982).

22. Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3412, 3414 (1982).

23. *See generally* Arthur R. Landever, *Electronic Surveillance, Computers, and the Fourth Amendment — The New Telecommunications Environment Calls For Reexamination Of Doctrine*, 15 U. TOL. L. REV. 597 (1984).

24. 18 U.S.C. § 2511(1) (1998) (emphasis added). The Wiretap Act proscribes solicitation and attempt as well as direct interception. *See id.* In 2001, after the events giving rise to the *Councilman* litigation but before its disposition, Congress altered the statutory language slightly through the USA Patriot Act. *See infra* notes 125–129 and accompanying text. Consequently, most citations to the Wiretap Act and Stored Communications Act refer to the 1998 codification, rather than a more recent codification.

25. Specifically, that clause "does not apply with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c) (1998).

26. *Id.* § 2701(a)(1)–(2).

27. *See* Wintersheimer, *supra* note 14, at 333.

28. *See, e.g.*, 18 U.S.C. § 2511(2)(a)(1) (2000); *cf.* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1226–27 (describing the distinction between public and non-public providers that was added with the Stored Communications Act).

storage of such communication."[29] In contrast, the definition of electronic communication does not explicitly include electronic storage.[30]

The e-mail privacy protections in the Wiretap Act differ from those in the Stored Communications Act along two major dimensions: the *type* of intrusion proscribed ("intercepts" versus "accesses") and the *nature* of communication intruded upon ("electronic communication" versus "electronic storage") (see Table 1).[31]

Table 1: Relationship Between Titles I and II of the ECPA

	Type of Intrusion	**Nature of Communication**
Wiretap Act (Title I)	*intercepting*	*electronic communication*
Stored Communications Act (Title II)	*accessing*	*electronic communication in electronic storage*

Three of the four terms have detailed, though hardly comprehensive, statutory definitions. "Electronic communication" refers to "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."[32] Likewise, "electronic storage" is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"[33] and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[34] "Intercept" means "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."[35] The statute does not define "access."[36]

---

29. 18 U.S.C. § 2510(1) (2000); *see also* Electronic Communications Privacy Act of 1986, S. 2575, 99th Cong. § 101(a)(1)(D) (1986) (noting changes from the 1968 Act).

30. *See* 18 U.S.C. § 2510(12) (2000).

31. Other micro-structural differences also exist between the Wiretap Act and the Stored Communications Act. For example, the Stored Communications Act partially exempts e-mail service providers from liability, while the Wiretap Act does not. *See id.* § 2701(c). The only large-scale differences between the two statutes are the type and nature distinctions discussed here.

32. *Id.* § 2510(12)(A) (2000). The same definition applies to uses of "electronic communication" in the Stored Communications Act. *See id.* § 2711(1).

33. *Id.* § 2510(17)(A).

34. *Id.* § 2510(17)(B).

35. *Id.* § 2510(4).

36. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 889 (9th Cir. 2002) (Reinhardt, J., dissenting in part) (noting the absence of a statutory definition), *cert. denied*, 537 U.S. 1193 (2003); *see also* Julie J. McMurry, Note, *Privacy in the Information Age: The Need for*

C. Change Destroys the Best Laid Plans: Modern Technology and New Problems in Interpreting the ECPA

Despite the drafters' attempts to craft language that would be both precise and adaptable,[37] the contours of what each title protects have become unclear.[38] That lack of clarity results primarily from the fact that the language used — "communication" versus "storage," "intercept" versus "access" — does not correspond to the technical realities of e-mail: e-mail messages can shift from transit to storage and back in nanoseconds.

E-mail, like other data transmitted over the Internet, is transmitted in small "packets" from computer to computer until it reaches its destination.[39] That destination is the Internet Protocol ("IP") address, of the recipient's mail server.[40] When an e-mail message is sent, a program called a mail transfer agent ("MTA") formats the message so that it can be broken down into packets and sent out over the Internet.[41] As each computer receives a packet, it briefly holds it in memory, retrieves the IP address of its final destination, and then determines how to route it to that address.[42] When all of the packets reach the recipient's mail server, a mail delivery agent ("MDA") reassembles them into an e-mail message, determines which individual user should receive the message, and delivers it to that user's mailbox.[43] Just as the intermediate computers briefly hold the packets in memory, the mail server must hold the complete e-mail in memory, at least momentarily, in order to deliver it.[44]

Consequently, a message is stored, in the plain sense of "placed or left in a location," [45] many times en route from sender to recipient. Similarly, because the e-mail delivery system involves such a large number of points of contact,[46] a third party can interfere with an e-mail transmission in many different ways. This system of delivery

---

Clarity in the ECPA, 78 WASH. U. L.Q. 597, 619 (2000) (supporting the creation of a statutory definition of "access").

37. *See* H.R. REP. NO. 99-647, at 30 (1986) (discussing the ECPA's drafting objectives).

38. *See* Kerr, *supra* note 28, at 1224–32; Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (calling the Wiretap Act "famous (if not infamous) for its lack of clarity").

39. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 613–14 (2003).

40. *See* PRESTON GRALLA, HOW THE INTERNET WORKS 90–92 (6th ed. 2002). In the e-mail address "addressee@mail.com," mail.com is the mail server.

41. *See id.*

42. *See id.*

43. *See id.*

44. *See id.*

45. MERRIAM-WEBSTER COLLEGIATE DICTIONARY 1159 (10th ed. 2002).

46. *See* John Christopher Anderson, *Transmitting Legal Documents Over the Internet: How to Protect Your Client and Yourself*, 27 RUTGERS COMPUTER & TECH. L.J. 1, 4 (2001) (arguing that because "electronic documents travel through countless interconnected computers . . . the likelihood that their contents may be intercepted is rather high").

frustrates any attempts to establish simple categories of access and interception.[47] For example, intruders can pirate the contents of e-mail messages by monitoring the sender's keystrokes,[48] by searching mail servers for residual copies of transmitted messages,[49] or by copying messages during the short time that they are held in the random access memory of intermediate or service provider computers.[50] It is not obvious whether such situations are covered by the Wiretap Act, the Stored Communications Act, neither, or both, because the ECPA uses the language of pre-digital-age privacy protections[51] rather than terminology reflecting how e-mail functions.[52] Though momentary storage of messages incident to transmission falls within the standard meaning of "stored," it may not fall within the meaning provided by the Stored Communications Act.[53]

In this disorder, commentators agree only that *something* distinguishes the coverage of the two acts, if for no other reason than that "a statute should be construed so that . . . no part will be inoperative or superfluous."[54] They splinter significantly regarding what statutory language drives that distinction; this Recent Developmentidentifies three modes of distinguishing the Stored Communications Act from the Wiretap Act that hold some sway in academia and in the federal courts.

Commentators applying Mode 1 posit that there is a temporal difference between "accesses" in the Stored Communications Act and "intercepts" in the Wiretap Act (see Table 2). They argue that the term "intercepts" refers only to intrusions occurring while an e-mail message is en route to its destination.[55] Thus, an e-mail message is protected by the Wiretap Act during transmission, but only by the Stored

47. *See* Kerr, *supra* note 28, at 1232 (listing types of interference that do not fit clearly into the established categories).

48. *See* United States v. Ropp, 347 F. Supp. 2d 831, 838 (C.D. Cal. 2004).

49. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113–14 (3d Cir. 2003).

50. *See* United States v. Councilman (*Councilman II*), 418 F.3d 67, 85 (1st Cir. 2005) (en banc), *rev'g* 373 F.3d 197 (1st Cir. 2004).

51. *Compare* Wiretap Act, 18 U.S.C. §§ 2510–2522 (1998), *with* 18 U.S.C. § 1708 (2000) (regulating unauthorized access to U.S. mail) *and* United States v. Lavin, 567 F.2d 579 (3d Cir. 1977) (interpreting the aforementioned conventional mail statute).

52. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (stating that "the ECPA was written prior to the advent of the Internet . . . [making it] ill-suited to address modern forms of communication").

53. *See* Bradford C. Mank, *Legal Context: Reading Statutes in Light of Prevailing Legal Precedent*, 34 ARIZ. ST. L.J. 815, 828 (2002) (noting that the "dictionary [or] 'ordinary' meaning of statutory terms" may differ from their legal meaning in statute).

54. Hibbs v. Winn, 542 U.S. 88, 101 (2004) (quoting 2A NORMAN J. SINGER, STATUTES AND STATUTORY CONSTRUCTION § 46.06, at 181–86 (6th ed. 2000)) (internal quotations omitted). This principle of statutory construction is called the rule against superfluities. *Id.*

55. Within the confused web of possible distinctions, even the apparently simple Mode 1 position turns out to be less clear than this Section suggests. Different users of Mode 1 disagree as to where exactly the temporal line between "accepts" and "intercepts" lies. For an extended discussion of that disagreement and its relevance to *Councilman*, see *infra* notes 108–118 and accompanying text.

Communications Act at other times.[56] A majority of the circuits that have considered the question adopt this view, holding that only "an acquisition contemporaneous with transmission" can violate the Wiretap Act.[57]

A minority of analysts, using Mode 2, see a qualitative difference between "accesses" and "intercepts." According to this Mode, the Wiretap Act addresses only an active and intrusive practice of *acquiring the contents* of e-mail, captured by the term "intercepts," while the Stored Communications Act covers both active and passive practices, captured by "accesses."[58] Thus, the Wiretap Act protects messages after delivery as well as at the time of transmission.[59] At the extreme of this view, Ninth Circuit Judge Stephen Reinhardt described unauthorized access as a "lesser included offense" to unauthorized interception.[60]

Finally, the analysts applying Mode 3 identify a temporal difference between "electronic communication" and "electronic storage." They divide into two subsets. Mode 3, Set 1 argues that the categories of "communication" and "storage" are mutually exclusive, such that an e-mail message fits into exactly one category at any given time.[61] Conversely, Mode 3, Set 2 argues that the two categories can be conceptualized as a Venn-diagram, such that messages are sometimes only communications, sometimes only in storage, and sometimes

---

56. *See, e.g.*, Kerr, *supra* note 28, at 1231; Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 48 (2004); COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm.

57. Theofel v. Farey-Jones, 359 F.3d 1066, 1077–78 (9th Cir. 2004) (arguing that intercept applies only to "acquisition contemporaneous with transmission"); United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003), *cert. denied*, 538 U.S. 1051 (2003) (same); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994) ("[The Wiretap Act] requires participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication . . . ."); *see also Konop*, 302 F.3d at 876–79 (distinguishing "electronic storage" from "electronic communication" as well as "access" from "intercepts").

58. *See, e.g.*, Jarrod J. White, *E-Mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 Ala. L. Rev. 1079, 1083 (1997); Tatsuya Akamine, Note, *Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer Is Subject to an Interception Under the Federal Wiretap Act*, 7 J.L. POL'Y 519, 561–65 (1999).

59. Akamine, *supra* note 58, at 564.

60. *Konop*, 302 F.3d at 889 (Reinhardt, J., dissenting in part). It is not clear whether Judge Reinhardt meant to take the position that *only* this qualitative distinction differentiates the two acts, or whether he recognized an additional distinction between "accesses" and "intercepts." It is clear, however, that he rejected the idea of a temporal distinction between "electronic communication" and "electronic storage," describing such a distinction as "a tortured reading of the Stored Communications Act." *Id.*

61. *See id*., 302 F.3d at 878 n.6 (explaining that "the language and structure of the ECPA demonstrate that Congress considered and rejected" the argument that "intercept [applies] to the *en route* storage of electronic communications").

both.[62] Both sets agree that where a message falls on the communication-storage spectrum determines how the ECPA protects it.[63]

Table 2: Distinctions Between the Wiretap Act and the Stored Communications Act

	Method of Distinction	**Source of Distinction**[64]
Mode 1	*temporal*	*type of intrusion*
Mode 2	*qualitative*	*type of intrusion*
Mode 3, Set 1	*temporal, exclusive*	*nature of communication*
Mode 3, Set 2	*temporal, nonexclusive*	*nature of communication*

The three positions are not mutually exclusive. One could hold an internally consistent belief that the Wiretap Act and the Stored Communications Act differ because there are qualitative and temporal differences between "accesses" and "intercepts" as well as a temporal difference between "electronic communication" and "electronic storage." Moreover, the substance of a commentator's position depends just as much on what distinctions she rejects as on what distinction she sees as most important. For example, the majority in *Konop v. Hawaiian Airlines, Inc.* criticized the dissenting opinion of Judge Reinhardt not because he argued for a qualitative distinction between "intercept" and "access" but because he dismissed the idea of a temporal distinction.[65] Thus, *Councilman* forced the First Circuit to weigh in on the question of which *combination* of positions it found most persuasive.

III. THE *COUNCILMAN* DECISION

Bradford Councilman served as Vice President for Interloc, Inc., an online rare book listing service that also acted as an e-mail provider for its book dealer customers.[66] In January 1998, apparently

62. *See, e.g.*, Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 n.1 (2d Cir. 2005); Gregory L. Brown, Steve Jackson Games, Inc. v. United States Secret Service*: Seizure of Stored Electronic Mail Is Not an 'Interception' Under the Federal Wiretap Act*, 69 TUL. L. REV. 1381, 1390–91 (1995).

63. *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–62 (5th Cir. 1994) (holding that the Wiretap Act did not apply to post-delivery seizure of e-mail because the e-mail was in electronic storage); *id.* at 462 (declining to take a position on whether a message, on another set of facts, could simultaneously be an "electronic communication" and in "electronic storage").

64. *See supra* Table 1 and accompanying text (identifying the statutory language responsible for different possible sources of distinction).

65. *See Konop*, 302 F.3d at 878 n.6.

66. United States v. Councilman (*Councilman II*), 418 F.3d 67, 70 (1st Cir. 2005) (en banc), *rev'g* 373 F.3d 197 (1st Cir. 2004).

desperate for a competitive edge, Councilman ordered his subordinates to develop a system that would permit him to read incoming messages sent to his customers by Amazon.com, one of Interloc's main competitors.[67] Interloc's system administrator re-programmed the company's mail transfer agent to copy messages from Amazon prior to their delivery to the intended recipient, while they were contained momentarily "in Random Access Memory or on a Hard Disk within Interloc's computer system," and to divert the copies to a separate folder that Councilman could access.[68] In July 2001, a grand jury indicted Councilman for conspiracy to disclose the contents of unlawfully intercepted electronic communications in violation of § 2511(1)(c) of the Wiretap Act.[69]

A. Councilman Wins: The District Court and First Circuit Panel Decisions

The district court dismissed the indictment.[70] It found, uncontroversially, that the messages were in electronic storage when Interloc's MTA copied them, noting that the ECPA defined electronic storage to include "any temporary, intermediate storage."[71] It then adopted the legal position (used by Mode 3, Set 1) that a message can be either a communication or in storage, but not both simultaneously.[72] Based on those two conclusions, it held that Councilman's conduct fell outside the temporal scope of "electronic communication" in the Wiretap Act.[73]

A divided panel of the First Circuit affirmed.[74] Semantically, parts of the majority opinion evoked Mode 1's temporal distinction between "access" and "intercept." For example, the court stated that it supported the indictment's dismissal "on the premise that no intercept occurred in this case."[75] Its logic, however, primarily followed the trial court's Mode 3-type reasoning.[76] Relying on intra-textual comparisons, it moved directly from the conclusion that "[o]n the facts of

---

67. *Id.*

68. *Id.* at 70–71.

69. *Id.* at 71. The indictment charged Councilman under 18 U.S.C. § 371 (1998), the general federal conspiracy statute. It also included a second count, alleging conspiracy to violate the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B) (1998), which the government voluntarily dismissed. *Councilman II*, 418 F.3d at 71 n.6.

70. United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003).

71. *Id.* at 321 (quoting 18 U.S.C. § 2510(17) (1998)).

72. *See id.* at 320–21.

73. *See id.* at 321.

74. *See* United States v. Councilman (*Councilman I*), 373 F.3d 197, 204 (1st Cir. 2004). Judge Torruella wrote the majority opinion, joined by Judge Cyr.

75. *Id.*

76. As explained earlier, Mode 3 employs a temporal distinction between "electronic communication" and "electronic storage." *See supra* text accompanying notes 61–63 & Table 2.

this case, it is clear that the electronic communications in this case were in a form of electronic storage"[77] to the holding that the Wiretap Act did not apply.[78] Since its exclusive reading of the electronic-storage/electronic-communication distinction ipso facto precluded indicting Councilman under the Wiretap Act, the majority squarely rejected the government's attempt to argue the case in terms of the intercept/access distinction.[79] Thus, the court concluded that it need not speak to the scope of the term "intercept" in the Wiretap Act.[80]

The structural tidiness of the panel majority's decision belied a concededly troubling conclusion. "The Wiretap Act's purpose was, and continues to be, to protect the privacy of communications," the court wrote, but "much of the protection may have been eviscerated by the realities of modern technology."[81] In the minds of many academics, the *Councilman I* court was as much to blame for that evisceration as evolving technology: the panel decision produced a firestorm of scholarly vitriol bemoaning its "disregard [for] societal expectations of privacy."[82] But the panel majority saw no other option. Although the ECPA no longer reflected the realities of e-mail communication, "it is not the province of [the] court to graft meaning onto the statute where Congress has spoken plainly."[83]

B. Councilman Loses: The First Circuit's En Banc Decision

Sitting en banc, the First Circuit reversed.[84] The court — in an opinion written by Judge Kermit Lipez, the dissenter from the *Councilman I* panel[85] — challenged the panel's reading of the ECPA head on. It stated that "'electronic communication' includes transient elec-

77. *Councilman I*, 373 F.3d at 203.

78. *See id.* at 202–04.

79. *Id.* (stating that although "the e-mails in this case were accessed by [Interloc's MTA] as they were being transmitted and in real time, . . . the presence of the words 'any temporary, intermediate storage' in 18 U.S.C. § 2510(17) controls").

80. *Id.* at 204; *cf.* W.S. Kirkpatrick & Co. v. Envtl. Tectronics Corp., Int'l, 493 U.S. 400, 408 (1990) (stating the general principle that courts should resolve cases "on the narrowest possible ground").

81. *Councilman I*, 373 F.3d at 203–04.

82. Dorothy Higdon Murphy, United States v. Councilman *and the Scope of the Wiretap Act: Do Old Laws Cover New Technologies?*, 6 N.C. J.L. & TECH. 437, 472 (2005); *see also* Kerr, *supra* note 28, at 1231; Deidre Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1565 & n.66 (2004); Yvette Joy Liebesman, Note, *The Potential Effects of* United States v. Councilman *on the Confidentiality of Attorney-Client E-mail Communications*, 18 GEO. J. LEGAL ETHICS 893, 921 (2005).

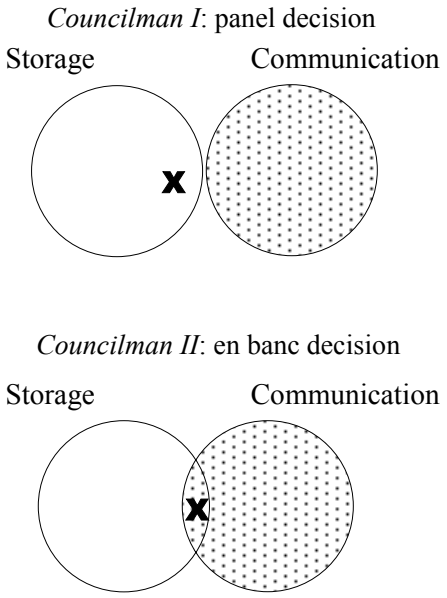
83. *Councilman I*, 373 F.3d at 204; *cf.* Hughes Aircraft Co. v. Jacobson, 525 U.S. 432, 438 (1999) (stating that language must take precedence over purpose in statutory construction).

84. United States v. Councilman (*Councilman II*), 418 F.3d 67, 69 (1st Cir. 2005) (en banc), *rev'g* 373 F.3d 197 (1st Cir. 2004).

85. Judge Lipez made arguments substantially similar to those in his *Councilman I* dissent. *Compare id.* at 69–85 *with Councilman I*, 373 F.3d at 204–19.

tronic storage that is intrinsic to the communication process for such communications" (the Mode 3, Set 2 position), rejecting an exclusive dichotomy between electronic communication and electronic storage (the Mode 3, Set 1 position).[86] It then concluded that messages temporarily held in the memory of a mail server computer before delivery were both communications and in storage, and therefore were protected by the Wiretap Act.[87]

Figure 1: *Councilman* and the Storage/Communication Distinction



On that point, the en banc majority appears to have the better argument. The dissent relies on two arguments for an exclusive storage/communication distinction. First, it contends that decisions in other circuits support an exclusive distinction.[88] All of those cases, however, involved interference with e-mails after delivery.[89] Thus, the

86. *Councilman II*, 418 F.3d at 79.

87. *See id.* at 85.

88. *Id.* at 87 (Torruella, J., dissenting).

89. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077–78 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113–14 (3d Cir. 2003); United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003); Blumofe v. Pharmatrak, Inc., 329 F.3d 9, 22 (1st Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994). All of the preceding cases address acquisitions of e-m

dissent's argument is that if some e-mail messages are covered only by "storage" (and not by "communication"), then no message may be covered by both. This argument follows the same fallacious logic as "some cars are not red, therefore no cars are red."

Second, and more persuasively, the dissent made an argument based on the principle *expressio unius est exclusio alterius* — the expression of one is the exclusion of the other.[90] It observed that the definition of "wire communication" in the Wiretap Act includes the phrase "any electronic storage of such communication,"[91] while the definition of "electronic communication" includes no reference to storage.[92] It concluded that electronic communication must *not* include electronic storage (i.e., that the two categories must be exclusive), since "it is generally presumed that Congress acts intentionally and purposely in [a] disparate inclusion or exclusion."[93] The majority responded that it does not always make sense to view disparate inclusions as intentional, especially when they occur in separate parts of a statute, and that such a presumption is not decisive in any event.[94] But the dissent's argument is slightly stronger when considered with the circumstances of the acts' enactments. Congress added the storage reference to the definition of "wire communication" at the same time that it first crafted the definition of "electronic communication,"[95] suggesting that the disparate treatment of storage for wire and electronic communications was intentional rather than accidental.

The majority offered two main countervailing arguments. First, it noted that the Wiretap Act includes four clauses explicitly excluding certain categories of communications from the definition of "electronic communication" but no clause explicitly excluding electronic storage.[96] Applying the same *expressio unius* principle, it contended that Congress likely did not intend to create an exclusive relationship between communication and storage.[97] Second, it argued that the broad definitions of electronic storage and wire communication in the ECPA reflect a desire to protect stored data and voice mail, and "not to affect e-mail at all."[98] These contentions counterbalance the dissent's *expressio unius* argument but do not provide an obvious af-

---

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878–79 (9th Cir. 2002) (addressing access to secure website stored on server).

90. *See Councilman II*, 418 F.3d at 87 (Torruella, J., dissenting); Trenkler v. United States, 268 F.3d 16, 23 (1st Cir. 2001) (describing the *expressio unius* principle as a canon of statutory construction).

91. 18 U.S.C. § 2510(1) (1998).

92. *Id.* § 2510(12)(A) (1998); *see also supra* note 32 and accompanying text.

93. *In re* Hart, 328 F.3d 45, 49 (1st Cir. 2003) (quoting Barnhart v. Sigmon Coal Co., 534 U.S. 438, 452 (2002)), *cited in Councilman II*, 418 F.3d at 87 (Torruella, J., dissenting).

94. *See Councilman II*, 418 F.3d at 74–75.

95. *See* Electronic Communications Privacy Act of 1986, S. 2575, 99th Cong. (1986).

96. *Councilman II*, 418 F.3d at 75; *see* 18 U.S.C. § 2510(12) (1998).

97. *Councilman II*, 418 F.3d at 75–76.

98. *Id.* at 76.

firmative reason to read "communication" and "storage" as non-exclusive.

Another point of intra-textual comparison ignored by both sides of the court in *Councilman*, however, would provide fairly decisive support for the majority's reading. Recall that § 2510(17) of the ECPA defines "electronic storage" in part as "any temporary, intermediate storage of a wire or *electronic communication* incidental to the electronic transmission thereof."[99] In that definition, "electronic communication" has the same meaning as it does in the Wiretap Act.[100] Consequently, if membership in the category of "electronic storage" negates membership in the category of "electronic communication" — as it must if one takes the temporal, exclusive position of Mode 3, Set 1 — then no e-mail message can ever satisfy the above portion of the definition of "electronic storage." That result turns § 2510(17)(A) into a nonsensical nullity. To avoid it, one must abandon the principle of exclusivity and adopt the Mode 3, Set 2 view of the storage/communication distinction, as the court in *Councilman II* did.

C. Legal Clarity Loses: Residual Confusion Regarding the Statutory Meaning of "Intercepts"

Like the *Councilman I* panel, the *Councilman II* court did not go on to consider whether Councilman's conduct fell within the statutory meaning of "intercepts."[101] From an uncharitable perspective, that action constitutes willful judicial error through the intentional evasion of a clearly presented and dispositive legal question. More charitably, it represents the sensible avoidance of a statutory interpretation question admitting no satisfactory answer, in the hopes of prompting Congress to repair an intractably unclear regulatory framework.

The *Councilman II* court could not claim that its interpretation of "intercepts" was irrelevant to the outcome of the case, as the panel majority in *Councilman I* did. A person violates the Wiretap Act if and only if he "intercepts" an "electronic communication."[102] The negation of either element settles the question of whether an indictment under the Wiretap Act should stand: absent either interception or an electronic communication, it should not. In contrast, the finding of one element (e.g., the conclusion that the messages with which Councilman interfered were electronic communications) does not completely resolve the question. Yet the *Councilman II* court did not address the "intercepts" issue. Instead, it found two reasons to avoid

99. 18 U.S.C. § 2510(17)(A) (emphasis added).
100. *See id.* § 2711(1); *supra* note 32 and accompanying text.
101. *Councilman II*, 418 F.3d at 80.
102. *See supra* Part II.B.

deciding whether "interception" must occur contemporaneous to transmission and, if so, whether interference with a message momentarily in storage satisfies that requirement.

First, the court asserted that "Councilman's appeal [did] not provide any other basis for finding that the acquisitions were not 'interceptions'" once it had concluded that the messages were "electronic communications" at the time of interference.[103] That assertion is incorrect. Councilman's argument that "intercept" covers only "acquisitions contemporaneous with transmission" and that "an e-mail in electronic storage . . . cannot by definition be acquired contemporaneous with transmission" does not depend on the assumption that electronic communication and electronic storage are distinct categories.[104] The intra-textual analysis that led the court to its conclusion that a message could remain a communication while in storage says nothing about the meaning of the term "intercepts," even if that meaning changes the consequences of the earlier conclusion.[105] Moreover, Councilman's brief included a separate argument that "[e]-mail interception may occur [in] the seconds or mili-seconds [sic] before which a newly composed message is saved to any temporary location following a send command."[106] That argument did not even arguably rely on an exclusive storage/communication distinction and, though somewhat of a stretch, plainly placed issues regarding the scope of "intercepts" and the "contemporaneous to transmission" requirement before the court.[107]

Second, the court opined that "it [is] highly unlikely that Councilman could generate a winning argument [that his conduct did not fall within the meaning of 'intercept'] in the circumstances of this

---

103. *Councilman II*, 418 F.3d at 79–80.

104. *Id.* at 79–80 (quoting Brief for the Defendant-Appellee, *Councilman II*, No. 03-1383, *available at* http://www.cdt.org/wiretap/20031008councilman.pdf [hereinafter Councilman Brief]) (internal quotation marks omitted).

105. In other words, the court's analysis could show only that the Venn-diagram structure on the top in Figure 1, *supra* Part III.B, accurately represents the nature of the storage/communication distinction, not that the Wiretap Act covers all conduct within the "communication" circle in that diagram. Specifically, the term "intercepts" at least hypothetically could limit the scope of the Wiretap Act to conduct within the "communication" circle and outside the "storage" circle.

106. Councilman Brief, *supra* note 104, at 47 (quoting United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003) (emphasis and internal quotation marks omitted)).

107. *See* Estate of Lisle v. Commissioner, 341 F.3d 364, 384 & n.35 (5th Cir. 2003) (stating that the court has discretion to address issues not raised in briefing). To support its decision not to address the scope of "intercepts," the *Councilman II* court cited *United States v. Moran,* 393 F.3d 1 (1st Cir. 2003), for the proposition that the appellee waived the argument by failing to raise it in briefing. *See Councilman II*, 418 F.3d at 34. However, the *Moran* court's holding was that an appellee must "raise an *error* purportedly committed by the district court" in briefing, which Councilman did by challenging the applicability of the Wiretap Act to his case, even if he did not make the specific argument. *Moran*, 393 F.3d at 11–12 (emphasis added).

case," even if the court were to consider the merits fully.[108] To assess the accuracy of that opinion, one must examine the range of interpretations of "intercept" that the court could have adopted. Had it interpreted "intercept" as a qualitative term covering only severe intrusions involving the acquisition of e-mail contents (the Mode 2 position),[109] it probably would have found an interception, since "Councilman and other Interloc employees routinely read the [diverted] e-mail messages."[110] Had it seen "intercept" as a temporal term covering all points between the time a message is sent and the time it is received (one take on the Mode 1 position),[111] it again would have found an interception, since Interloc's MTA "would intercept and copy all incoming messages from Amazon.com before they were delivered to the recipient's mailbox."[112] But had the court viewed "intercept" as a temporal term covering all points when the message was in active transit from the sender to the recipient (a different take on the Mode 1 position), it would not have found an interception, since "the messages existed in the random access memory (RAM) or in hard disks, or both, within Interloc's computer system," not in transmitting wires, when they were copied.[113]

This third interpretation represents a perfectly plausible take on the applicable sources of law. The requirement that an interception occur "contemporaneous with transmission" comes from judicial decisions, not statutory language.[114] None of the courts enunciating that requirement had occasion to consider whether momentary pauses in the transmission process were "contemporaneous with transmission."[115] Dicta from those cases send conflicting messages.[116] The statutory definition of "intercepts" sheds no light on the matter.[117] An ordinary definition of "intercept" — "to stop, seize, or interrupt in progress or course or before arrival"[118] — could justify either temporal view. A reading that emphasizes "before arrival" would cover all interference between sending and receipt, while a reading that emphasizes "in progress or course" might exclude times when the message is

108. *Councilman II*, 418 F.3d at 80.

109. *See supra* notes 58–60 and accompanying text.

110. *Councilman II*, 418 F.3d at 70.

111. *See supra* notes 55–57 and accompanying text.

112. *Councilman II*, 418 F.3d at 70.

113. *Id.* at 71 (internal quotation marks omitted).

114. *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994).

115. *See supra* note 89.

116. *Compare* United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (suggesting that the Wiretap Act does not protect messages in temporary storage because it covers only "acquisition during 'flight'") *with* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (implying that the Wiretap Act covers any interference "before arrival").

117. *See* 18 U.S.C. § 2510(4); *see also supra* note 35 and accompanying text.

118. MERRIAM-WEBSTER COLLEGIATE DICTIONARY 609 (10th ed. 2002).

not literally in progress — that is, when it is held in temporary storage.

The *Councilman* court faced two major interpretative problems.[119] It correctly resolved the relatively simple problem of how to distinguish electronic communication from electronic storage, concluding that an e-mail message could remain an electronic communication while in storage. It refused to take on the more difficult problem of how to distinguish interception from access, perhaps because it saw no analytically acceptable way to do so given the obtuse, technologically outdated language of the ECPA.[120] As a result, the parameters of interception under the Wiretap Act remain unclear.

IV. RECOMMENDATIONS FOR THE FUTURE

Faced with a case asking it to weigh in on one of the most troubling problems in communications law, the First Circuit declined to give an answer. Congress should read that refusal as a thinly veiled cry for help. Changing technology has rendered parts of the ECPA intractably unclear. Courts cannot resolve new questions arising under it without making arbitrary — or legislative — judgments.

The current lack of legislative clarity poses three significant problems for the statutory framework controlling e-mail privacy. First, vagueness imposes error costs. Forced to guess how private their e-mail messages are,[121] users either will waste resources by using less efficient alternative means of communication or by adopting needless security measures (if they underestimate the actual level of privacy protection), or will take inefficient risks with confidential information (if they overestimate it). Second, vagueness creates reliance costs. Because the judicial interpretation of "intercepts" may change as courts struggle to find a proper interpretation, users may find that rational modifications to behavior made one day no longer make sense the next day.[122] Third, vagueness produces investigation costs. In the absence of a clear statute, users who want to know how secure their e-mail messages are must devote substantial resources to legal re-

119. In addition to the main issues in the case, the court in *Councilman II* also addressed four due process-based challenges to the indictment, all based on the premise that the ECPA was too unclear to provide Councilman with adequate notice that it proscribed his conduct. *See Councilman II*, 418 F.3d at 80–85.

120. Despite disagreeing over the outcome, the en banc majority may nonetheless have agreed with the dissent that "[a]lthough nature abhors a vacuum, it has no power over legislative oversights." *Id.* at 86 (Torruella, J., dissenting).

121. *See, e.g.*, Liebesman, *supra* note 82, at 895 (noting that lawyers may or may not have a reasonable expectation of privacy on e-mail messages sent to clients for purposes of attorney-client privilege).

122. For example, a business, having invested in encryption software after the *Councilman I* panel decision created significant doubts about the vitality of e-mail privacy protection, may regret that purchase after *Councilman II* seemingly revitalized that protection.

search.[123] All three types of costs harm businesses in particular, since businesses use a high volume of e-mail.[124] Clarifying legislation may be the only good way to avoid these costs.

Before the *Councilman* decision, but after the events that gave rise to the litigation, the Patriot Act somewhat altered the statutory landscape. The Patriot Act removed stored voice mail from the set of "voice communications" protected by the Wiretap Act,[125] augmented the range of investigative actions the government could take with a subpoena rather than a warrant,[126] and reduced limitations on the use of pen registers to obtain e-mail routing information.[127] Most of its revisions apply only to government searches and seizures, not to private conduct.[128] In any event, the Patriot Act did nothing to clarify the temporal scope of "intercepts" in the Wiretap Act.[129]

Two proposed bills, however, would provide the needed clarification. House Resolution 4956, sponsored by Washington Representative Jay Inslee, would amend the definition of "intercepts"[130] applicable to electronic communication, contained in 18 U.S.C. § 2510(4), by adding the phrase "at any point between the point of origin and the point when it is made available to the recipient."[131] Senate Resolution 693, introduced by Vermont Senator Patrick Leahy and sponsored in the House by Utah Representative Chris Cannon, takes a similar but more expansive approach. It would supplement the existing definition of "intercepts" with the phrase "contemporaneous with transit, or on an ongoing basis during transit, through the use of any electronic, mechanical, or other device or process, notwithstand-

---

123. *See generally* Cass R. Sunstein, *Problems With Rules*, 83 CAL. L. REV. 953, 968 (1995) (claiming that "[v]agueness exemplifies a failure of the rule of law"); *cf.* Harvey Gelb, *The Corporate Opportunity Doctrine — Recent Cases and the Elusive Goal of Clarity*, 31 U. RICH. L. REV. 371, 374–82 (discussing costs to corporations caused by lack of clarity in the law concerning fiduciary duty).

124. *See* Steven Lorenc, *E-mail Management: The First Step in Addressing Information Overload*, INSURANCE DAY, July 18, 2005 (collecting statistics regarding corporate e-mail use).

125. Instead, the Patriot Act protected stored voice mail as a wire communication. *See* 18 U.S.C. § 2510(1) (2000 & Supp. I 2002); H.R. REP. NO. 107-236, pt. 1, at 91 (2001).

126. *See* Arthur J. Carter IV & Audrey Perry, *Computer Crimes*, 41 AM. CRIM. L. REV. 313, 320–28, 336–38 (2004) (describing the state of law under the ECPA and the impact of the Patriot Act).

127. 18 U.S.C. §§ 3123(a)(1)–(2) (Supp. I 2002).

128. *See* Freiwald, *supra* note 56, at 70.

129. *See* Aaron Burstein, *A Survey of Cybercrime in the United States*, 18 BERKELEY TECH. L.J. 313, 333 (2003). Under statutory sunset provisions, some parts of the Patriot Act will cease to be effective on December 31, 2005, unless Congress acts to renew them. *See* S. 2476, 108th Cong. (2004) (proposing extension of the sunset date). Whether or not the sunset occurs, however, will have minimal impact on e-mail privacy protections. *See* Freiwald, *supra* note 56, at 69–72.

130. The existing statute defines "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." 18 U.S.C. § 2510(4).

131. E-Mail Privacy Act of 2004, H.R. 4956, 108th Cong. (2004).

ing that the communication may simultaneously be in electronic storage."[132] Both bills would resolve the question dodged by the court in *Councilman II* in favor of the position that all interruptions occurring between the time an e-mail message is sent and the time it is received fall within the temporal scope of "intercepts." A third bill, sponsored by New York Representative Jerald Nadler, would add an explicit statement that "electronic communication" "includes any temporary, intermediate storage of that communication incidental to the electronic transmission thereof," solidifying *Councilman*'s treatment of the storage/electronic distinction.[133]

While the Nadler bill would simplify a needlessly complex statutory construction, it would merely codify the practices already established by most federal courts.[134] The Inslee and Leahy bills, on the other hand, each offer a clear and substantively appealing amendment to the definition of "intercepts."[135] Between the two, the Inslee bill holds slightly more appeal because its extreme simplicity makes it more immune to technological change: the bounding concepts of "point of origin" and "made available to the recipient" seem likely to retain coherent meaning even if the technology used in e-mail communication evolves significantly.[136] Either bill, however, would clarify the currently inadequate statutory framework, and that is the most pressing need.[137]

Since the First Circuit withdrew the panel opinion in *Councilman*, the drive for a legislative solution has lost steam; as of this writing, no action has been taken on any of the three proposals since April 2005.[138] Legislators may share the view, relatively popular in academia, that the crisis has been averted.[139] Yet the lack of clarity existing after the en banc opinion in *Councilman* threatens to create an even more severe crisis.

---

132. E-Mail Privacy Act of 2005, S. 936, 109th Cong. § 2 (2005); H.R. 3503, 109th Cong. § 2 (2005).

133. E-Mail Privacy Protection Act of 2004, H.R. 4977, 108th Cong. § 2 (2004).

134. *See* United States v. Councilman (*Councilman II*), 418 F.3d 67, 79 (1st Cir. 2005) (en banc), *rev'g* 373 F.3d 197 (1st Cir. 2004); Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 (2d Cir. 2005); Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004) (in dicta).

135. *See* Kerr, *supra* note 28, at 1231.

136. *See* Jay Campbell, Note, *Protecting the Future: A Strategy for Creating Laws Not Constrained by Technological Obsolescence*, 7 VAND. J. ENT. L. & PRAC. 533, 540 (2005) (advocating "the creation of laws independent of technology" and therefore not susceptible to the problem that new technology renders technology-specific statutes obsolete).

137. At this point, action on the Leahy-Cannon bill seems far more likely. *See* Bill Summary & Status for the 109th Congress, H.R. 3503, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:H.R.03503: (last visited Nov. 10, 2005) (summarizing committee actions). Such action is an unequivocally positive step.

138. *See* Bill Summary & Status for the 109th Congress, S. 936, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.00936: (last visited Nov. 10, 2005).

139. *See, e.g.*, Murphy, *supra* note 82, at 440 (praising the First Circuit for agreeing to rehear *Councilman*).

The panel opinion in *Councilman* generated significant concern regarding the erosion of e-mail privacy. This Recent Developmenthas argued that the First Circuit's en banc opinion may cause even greater long-term problems, since legislators probably will not respond as quickly to ambiguity and confusion as they would to an objectionable decision. To prevent ECPA jurisprudence from descending further into a muddled morass, Congress must act to clarify how the term "intercepts" in the Wiretap Act applies to e-mail messages in momentary storage en route to their recipients.