United States v. Councilman: An Appropriate Expansion of Internet Privacy Rights?

by
*Robert Roll**

The technological advances of the last quarter century that permitted the explosion of the Internet simultaneously generated significant abuses of this technology. Congress and the courts responded to each innovation by creating what has become a broad patchwork of remedies intended to deter Internet crime. Though e-mail does not enjoy the same expectation of privacy as other mediums of communication, these remedies overlap to provide recourse in the event of unauthorized access or viewing. To date, the Electronic Communications Privacy Act ("ECPA") represents one of the most effective of these deterrents by imposing civil and criminal penalties on those who attempt to capture the Internet communications of others.[1] For several federal circuits, however, adapting the language of the Act to the shifting landscape of Internet communication has been a cumbersome effort.[2]

The most recent and most perplexing of these cases is the First Circuit's attempt to untangle the statutory language in *United States v. Councilman*.[3] The defendant, Bradford Councilman, served as Vice President of Interloc, Inc., a rare books business on the Internet.[4] As an ancillary service to the rare books business, Interloc offered its customers e-mail addresses to which it acted as the Internet service provider (ISP).[5] To gain a competitive edge, Councilman instructed Interloc employees to write a program that would gather incoming e-mails sent to Interloc's customers from Amazon.com.[6] This program successfully captured its target e-mails by removing them from the random access memory within Interloc's computer system.[7] After e-mails were collected by the program, Councilman and others read many of the messages, allegedly gaining a commercial advantage.[8] On July 11, 2001, Councilman was indicted for conspiracy to violate the ECPA.[9] Facing the indictment, Councilman argued that the government's construction of the

---

* Mr. Roll received a bachelor's degree from the University of Texas at Austin in May 2004, and he is a candidate for Juris Doctor, class of 2007, at Southern Methodist University Dedman School of Law.

1. 18 U.S.C. § 2511 (2006) (effective Nov. 25, 2002).
2. *See, e.g.,* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874-80 (9th Cir. 2002).
3. (*Councilman IV*), 418 F.3d 67 (1st Cir. 2005) (en banc).
4. *Id.* at 70.
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.* at 70-71.

ECPA's relevant provisions, under which he was charged, ran contrary to the interpretation settled on by the courts.[10] To understand Councilman's contention, some background on the ECPA is necessary.

Congress enacted the ECPA in 1986, broadening the existing Wiretap Act to provide similar protection for electronic communications.[11] Under its two titles, the ECPA provides broad coverage for electronic communication.[12] Title I of the ECPA applies to wire communication and electronic communication; whereas, Title II provides protection for "electronic storage."[13] The amended version of the Wiretap Act basically comprises Title I of the existing ECPA. Making a case under this title, the government must show "that a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device."[14] Of these five elements, the two implicated in Councilman's defense are "interception" and "electronic communication."[15]

At trial, the district court had determined that the various circuits previously interpreting these elements had so narrowed their applicability to the instant facts that Councilman could not be charged under the Wiretap Act.[16] Validating Councilman's argument, the court accepted as law the transit-storage dichotomy which had recently been adopted by the Ninth Circuit.[17] This distinction narrowed the meaning of "interception" under the Act by limiting the definition to acquisitions which occur in real-time while an electronic communication is en route to its destination and not when it is in any "electronic storage."[18] This rationale grew out of the Fifth Circuit's application of its pre-ECPA rulings to the amended statutory language of the Wiretap Act.[19] Subsequently, the Third, Ninth and Eleventh circuits adopted this reading of the statute.[20] Though the transit-storage dichotomy might seem insignificant,

10. *Id.*

11. Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 (2d Cir. 2005).

12. Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 460 (5th Cir. 1994).

13. *Id.*

14. *In re* Pharmatrak, 329 F.3d 9, 18 (1st Cir. 2003).

15. *Councilman IV*, 418 F.3d at 72.

16. United States v. Councilman (*Councilman I*), 245 F. Supp. 2d 319, 320-21 (D. Mass. 2003).

17. *Id.* (citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002)).

18. *Konop*, 302 F.3d at 878.

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

20. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2004); *Konop*, 302 F.3d at 876-78; United States v. Steiger, 318 F.3d 1039, 1047-49 (11th Cir. 2003).

it is the simplest form of statutory interpretation: plain text reading of parallel provisions.

An argument favoring the transit-storage dichotomy is rooted in the structure of the ECPA. That is, "wire communication" and "electronic communication" share parallel definitions in the statute.[21] After its amendment and inclusion in the ECPA, the original Wiretap Act remained in place except for the addition of protection for "any electronic storage of such communication" under the definition of "wire communication."[22] Notably, this language was not included in the definition of "electronic communication" at this time, and, its absence provides the genesis of the transit-storage dichotomy.[23]

As mentioned above, however, the ECPA is not devoid of protection for electronic storage outside of wire communication. Indeed, the Stored Communications Act, comprising Title II of the ECPA, provides expansive protection for "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[24] Given this statutory structure, other circuits have taken "a strict view of the phrase 'in storage' and found that no violation of the Wiretap Act occurs when an electronic communication is accessed during storage, even if the interception takes place during a nanosecond 'juncture' of storage along the path of transmission."[25] Adopting this rationale, the district court announced that "'[s]torage' means storage, in whatever form and for however long," and as a result the charges against Councilman under the Wiretap Act were dismissed.[26]

On appeal, the First Circuit accepted the lower court's reasoning. The majority, authored by Judge Torruella, traced in more detail the evolution of the law to its current state. Applying this construction of the statute, the court asserted, "it is clear that the electronic communications in this case were in a form of electronic storage," noting that it is possible "the protections of the Wiretap Act have been eviscerated as technology advances."[27] Ultimately, while the court recognized that the statute "may be out of step with the technological realities of computer crimes," it determined that "it is not the province of this court to graft meaning onto the statute where Con-

21. *See* 18 U.S.C. § 2510 (1), (12)(a) (2002).

22. *Steve Jackson Games*, 36 F.3d at 460.

23. *Id.*

24. 18 U.S.C. § 2510(17)(A) (2002).

25. United States v. Councilman (*Councilman I*), 245 F. Supp. 2d 319, 321 (D. Mass. 2003) (citing *Konop*, 302 F.3d at 878).

26. *Id.*

27. United States v. Councilman (*Councilman II*), 373 F.3d 197, 203 (1st Cir. 2004), *vacated*, 385 F.3d 793 (1st Cir. 2005).

gress has spoken plainly."[28] Thus, the First Circuit originally affirmed the district court, relying on the law as interpreted by all circuits having heard the issue.[29] Subsequently, however, the court voted to rehear the case en banc, withdrawing the panel decision and vacating the judgment.[30]

Upon rehearing en banc, the First Circuit found that the district court erred in dismissing the indictment against Councilman.[31] Though there is nothing extraordinary about this result, the means used to achieve it are surprising. That is, the court did not overturn on appeal because of some minor technicality; it distinguished or disavowed an entire line of cases, encompassing the entire jurisprudential wisdom of the federal circuits on this particular issue. The court held that the Stored Communications Act's protection of electronic storage does not operate to the exclusion of the Wiretap Act's protection of electronic storage incidental to electronic communication.[32]

To achieve this result, the court divided the case into two issues, causing its decision on the first to moot Councilman's argument on the second. Under the first issue, the court set out to define "electronic communication" under the Wiretap Act.[33] Although the statute provides a broad, definition of the phrase, the court determined that an ambiguity exists and reviewed legislative history in an attempt to resolve that ambiguity.[34] Finding the history illuminating, the court ruled that electronic communication "includes transient electronic storage that is intrinsic to the communication process for such communication," drawing support from dicta in a previous First Circuit decision.[35] Given its decision on the first issue, the court easily disposed of the second. [36]

Essentially, the court framed the second issue as whether under the Wiretap Act an electronic communication's acquisition must be "contemporaneous with transmission" to be an interception.[37] Councilman's argument regarding this issue relied on a definition of electronic communication distinct from electronic storage. As a result, the court did not have to address

28. *Id.* at 204.

29. *Id.*

30. United States v. Councilman (*Councilman III*), 385 F.3d 793 (1st Cir. 2005) (per curiam) (withdrawing panel opinion and dissent released on June 29, 2004 and vacating judgment entered on June 29, 2004).

31. United States v. Councilman (*Councilman IV*), 418 F.3d 67, 85 (1st Cir. 2005) (en banc).

32. *Id.* at 79.

33. *Id.* at 72.

34. *Id.* at 73-74.

35. *Id.* at 79 (citing *In re* Pharmatrak, 329 F.3d 9 (1st Cir. 2003)).

36. *Id.*

37. *Id.*

the question.[38] Nonetheless,[39] it offered a statement on this issue which may have far-reaching implications: "we think it highly unlikely that Councilman could generate a winning argument in the circumstances of this case. Any such argument would entail a showing that each transmission was complete at the time of acquisition and, therefore, that the definition of 'intercept' does not cover the acquisitions."[40]

The First Circuit's decision suggests a desire to construe the ECPA so that gaps in the statute, which are created over time and caused by the development of technology not in existence or not understood when the statute was created, are filled in support of the expansion of privacy rights on the Internet. This case provides refuge for the average Internet user in light of the gaps left in the EPCA, as a result of previous interpretations of the ambiguous statutory language adopted by Congress. However, a number of questions arise when following the meandering path which leads to this desired result.

Does the First Circuit Appropriately Delve into Legislative History?

The en banc majority opinion goes to great lengths to justify using legislative history to interpret the ECPA's definition of "electronic communication." Any justification is inappropriate because the court should never have gone beyond the plain language of the statute. The court begins its analysis appropriately with the plain text, noting that while the definition of "wire communication" makes reference to electronic storage, "the definition of 'electronic communication' does not mention electronic storage."[41] Of course, this point is correctly stated, and it makes up a crucial aspect of Councilman's argument, but does not constitute his entire argument. At this point, the court's approach to this question takes an unexpected turn. The court states that Councilman "*infers* that Congress intended to exclude communications in transient storage from the definition of 'electronic communication,' regardless of whether they are in the process of being delivered, simply because it did not include the term 'electronic storage' in that definition."[42] By misstating Councilman's argument, the court actually creates the very ambiguity that it attributes to the statutory language

By couching Councilman's argument in these terms, the court is then able to assert that the defendant makes an inferential leap. Far from a bald recitation of the statute's language,[43] the foundation of Councilman's argu-

38. *Id.*

39. *Id.*

40. *Id.* at 80.

41. *Id.* at 73.

42. *Id.* (emphasis in original).

43. *Id.*

ment borrows from the reasoning settled on by several circuits. Principally, the EPCA must be viewed with its entire structure in mind.[44] Rather than taking a myopic view of the relevant provision, this argument recognizes that Congress allocated the levels of protection deemed necessary to each form of communication by placing these very disparate entities in different titles of the Act.[45] The argument, when articulated properly, does not make an inference and still results in a reasonable reading of the statute without resorting to legislative history.

Nonetheless, it should be pointed out that a review of the legislative history, however ill advised, does contain some illuminating information. For example, legislative history suggests that the "electronic storage" clause in the definition of "wire communication" was originally intended as a protection for voice mail.[46] The court reasons that this discovery in large part invalidates Councilman's argument,[47] when in fact the two concepts are not mutually exclusive. When the USA PATRIOT Act[48] was enacted, one of its effects was to amend the Wiretap Act by removing the "electronic storage" clause.[49] Apparently, the First Circuit does not place much importance on this action;[50] however, another circuit found it enlightening:

> [w]hen Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term "intercept" with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make the definition applicable to voice mail messages as well. Congress, therefore, accepted and implicitly approved the judicial definition of "intercept" as acquisition contemporaneous with transmission.[51]

This argument offered by the Ninth Circuit represents another construction of the ECPA based on sources other than the statute's plain text. Though the argument appears convincing, it must be subjected to the same criticism as the First Circuit's argument because it relies on more than the language of the statute. Judge Torruella aptly makes this point in his vigorous dissent to majority's en banc opinion, pointing out that "[j]udicial investigation of leg-

44. *See* Hall v. EarthLink Network, Inc., 396 F.3d 500, 504-05 (2d Cir. 2005).

45. Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461 (5th Cir. 1994).

46. *Councilman IV*, 418 F.3d at 77.

47. *Id.*

48. *See* USA PATRIOT Act § 209, 18 U.S.C. § 2510 (2002).

49. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002).

50. *Councilman IV*, 418 F.3d at 78.

51. *Konop*, 302 F.3d at 878.

islative history has a tendency to become. . .an exercise in 'looking over a crowd and picking out your friends'."[52]

DOES THE COURT CORRECTLY DISPOSE OF *COUNCILMAN*'S INTERCEPTION ARGUMENT?

As previously mentioned, the court divided Councilman's argument into two issues: electronic communications and interception.[53] The court is able to opt out of making any binding pronouncements on the interception issue, since Councilman's argument on this issue relies on a definition of "electronic communication" not inclusive of any electronic storage.[54] While the majority was satisfied to avoid the question, it is unclear whether they did so successfully because in some respects, Councilman's argument survives the court's new definition of "electronic communication." Essentially, the First Circuit added "transient electronic storage that is intrinsic to the communication process" to that which is protected under the Wiretap Act's electronic communication clause.[55] Taken to its logical extension, this rule suggests that a residual category of electronic storage intrinsic to this communication is not covered by the Wiretap Act. The Wiretap Act may not cover electronic storage intrinsic to electronic communication that is not entirely transient in nature.

As the data in Councilman's case was stored completely in the random access memory of Interloc's computer system, this data can only be characterized as transient with great difficulty given that it could remain on the computer for quite some time. That said, the e-mails at issue in Councilman's case arguably fit outside of the court's definition and the residual category of electronic storage created would seem to fit within the broad coverage of the Stored Communications Act.

DID POLITICAL PRESSURE AND PUBLIC OUTCRY NECESSITATE REHEARING OF *COUNCILMAN*'S CASE?

Immediately following the First Circuit's initial panel decision in *Councilman*,[56] the volume of public outcry was overwhelming. For instance, one commentator asserted that "privacy will be seriously eroded if e-mail is not protected by" the Wiretap Act.[57] Others suggested that doomsday scenarios

52. *Councilman IV*, 418 F.3d at 88 (Torruella, J., dissenting).

53. *Id.* at 72.

54. *Id.* at 79.

55. *Id.*

56. United States v. Councilman (*Councilman II*), 373 F.3d 197 (1st Cir. 2004), *vacated*, 385 F.3d 793 (1st Cir. 2005).

57. Editorial, *Intercepting E-mail*, N.Y. TIMES, July 2, 2004, at A18 (calling for congressional action to remove the debate embodied by *Councilman* from control of the courts).

would result from the First Circuit's ruling.[58] While presumably reflecting the general public's emotions relating to online privacy, the force of this criticism betrayed a misunderstanding of both the ECPA and the constraints of the courts.

Far sharper rhetoric originated from the floor of the Senate. Soon after the panel's decision, one of the ECPA's original sponsors, Senator Leahy, implored the Senate to remedy the "instant and enormous gap in privacy protection" caused by the decision.[59] Senator Leahy argued that electronic communication should include all e-mail "acquired contemporaneously with its transmission."[60] In fact, the First Circuit adopted this broad interpretation upon rehearing.[61] Further, he asserted that Councilman's action represents "precisely the type of behavior that Congress wanted to prohibit."[62] Assuming the Senator's statements accurately reflect the intent of Congress, one conclusion seems clear: Congress' revision of the Wiretap Act, embodied by the ECPA, inadequately manifests its intent, leaving the courts with difficult constitutional decisions.

As Senator Leahy remarked, Congress has "an obligation to ensure that our laws keep up with technology and it may be that advances in communications warrant change."[63] By passing an ambiguous piece of legislation, Congress shifted this obligation to the courts. Inevitably, it seems that such legislation either results in misinterpretation of congressional intent or accusation of activist jurisprudence. However unfair this criticism may be, it would be even more unfair to ignore the effect that this pressure had on the eventual outcome of Councilman's case. Senator Leahy's statements, though made in hindsight, did give the First Circuit some insight into the intent of Congress, undoubtedly playing a role in the court's decision to reverse.

DOES THE FIRST CIRCUIT'S PANEL DECISION POSE A SIGNIFICANT THREAT TO INTERNET PRIVACY?

Despite arguments to the contrary made by the en banc majority and numerous political commentators, the panel decision in *Councilman* did "not require that we assume that Congress contemplated the complete evisceration

58. *See, e.g.,* Editorial, *Derail E-Mail Snooping*, WASH. POST, July 2, 2004, at A14 (suggesting that law enforcement would abuse the more permissive standard arguably created by the panel decision). *See generally* Yvette J. Liebesman, *The Potential Effects of United States v. Councilman on the Confidentiality of Attorney-Client E-Mail Communications*, 18 GEO. J. LEGAL ETHICS 893 (2005) (predicting that the panel decision would require an overhaul of attorney-client privilege rules).

59. 150 CONG. REC. S7893-01, S937894 (2004).

60. *Id.*

61. *Councilman IV*, 418 F.3d at 79.

62. 150 CONG. REC. S7893-01, S7893 (2004).

63. *Id.* at S7894.

of the privacy protections for e-mail."[64] Such a position ignores the multitude of overlapping protections available to the average Internet user. While Councilman's actions were not punishable under these alternative protections, failing to convict one man does not alone foster the creation of a 'snoopers' heaven' as one commentator has suggested.[65] The inapplicability of these protections to Councilman's scheme does not justify the extra-judicial result reached by the en banc majority.

Seeking conviction of Councilman, the government "attempted to fish with a net that has holes in it and is thus in need of repair."[66] This said, the numerous alternative "nets" available to the government should not be ignored merely because they were not utilized in this case. Primarily, public overreaction to the panel decision stemmed from the lack of protection available to Amazon.com and its customers in this particular case; however, in most cases, the government or a private party has a myriad of remedies at its disposal.

Among these remedies, the Computer Fraud and Abuse Act provides an Internet user a remedy should another person gain access to the user's computer or network.[67] Overlapping this protection, the Stored Communications Act protects electronic storage on the network of an ISP from being accessed without authorization.[68] This statute protects e-mails remaining on an ISP's server even after their download by the intended recipient.[69] In *Councilman*, the Computer Fraud and Abuse Act did not provide a remedy because the computer accessed was Interloc's own. Nevertheless, in a similar case, the First Circuit held that the very same practice of "scraping," used to gain a commercial advantage, was unauthorized when a competitor's website was accessed.[70]

Additionally, the government chose not to charge Councilman under the SCA because Interloc presumably fell within the statute's service provider exemption.[71] This exemption does not give an ISP free-reign to read its subscribers e-mails as has been suggested. To the contrary, two major protections curtail the ability of an ISP to view a customer's e-mail should it seek to do so. First, the courts have recognized the application of several common

64. *Councilman IV*, 418 F.3d at 87.

65. Kim Zetter, *Court Creates Snoopers' Heaven*, WIRED NEWS, July 6, 2004, http://www.wired.com/news/privacy/0,1848,64094,00.html.

66. *Councilman IV*, 418 F.3d at 88.

67. 18 U.S.C. § 1030 (2004).

68. 18 U.S.C. §§ 2701-2712 (2002).

69. *Councilman IV*, 418 F.3d at 80.

70. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001).

71. *Councilman IV*, 418 F.3d at 81.

law torts as a supplement to statutory protections.[72] These principles are more adaptable to the unique and evolving scenarios presented by the Internet and, if widely utilized, ably protect the interest of Internet users where statutory coverage lapses. Second, in a general attempt to limit their liability, ISPs provide customers with detailed privacy policies actionable through contract.

While these contracts have tended to focus on the abuses prohibited by ISPs,[73] their terms do provide additional coverage to the Internet user, perhaps representing the best solution to the problem presented by *Councilman*.[74] In fact, the launch of Google's G-mail represents an example of the effectiveness of ISP-consumer contracting.[75] In exchange for substantial amenities, Google's customers permit Google to inspect their e-mail allowing the company to tailor advertisements to customers' interests. Google's ability to use this technology should be called into question, given the First Circuit's en banc decision in *Councilman*. Because of the patchwork of protection available under the First Circuit's panel decision, neither Google's customers or other Internet users are at risk of significant privacy losses.

WHAT IMPACT DOES *U.S. v. COUNCILMAN* HAVE ON THE FUTURE OF PRIVACY RIGHTS ON THE INTERNET?

The decision of the majority in Councilman appears rooted in public policy concerns and public outcry stemming from the court's withdrawn opinion. If the result in this case is in fact the will of Congress as the First Circuit suggests,[76] the remaining statute is stronger and more capable of surviving the continuous onslaught caused by developing technology. The circuits that heard arguments on this issue, prior to the First Circuit, read and interpreted the plain text of the Wiretap Act, as amended by the ECPA, and faithfully applied precedent as it related to the question at hand. Although these circuits executed their obligations under the Constitution and remained true to the limitations it imposes, obvious deficiencies were left without remedy in a statute intended to protect the privacy rights of Internet users.

---

72. *See generally* Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421 (2002) (detailing the application of trespass to chattels from common law property to the Internet).

73. *See generally* Keith J. Epstein & Bill Tancer, *Enforcement of Use Limitations by Internet Services Providers: "How to Stop That Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber"*, 19 HASTINGS COMM. & ENT. L. J. 661 (1997) (suggesting ideas for more effective ISP-customer contracts).

74. *Councilman IV*, 418 F.3d at 88.

75. Saul Hansell, *You've Got Mail (and Court Says Others Can Read It)*, N.Y. TIMES, July 6, 2004, at C1.

76. *Id.*

In contrast, the en banc majority of the First Circuit issued a decision that may not have honored the text of the ECPA and may well have been decided erroneously; however, this decision and the conflict that it will necessarily foster suggests some resolution to the issue. Due to the circuit split created here and the boldly asserted understanding of Congress's implicit intent, a review of this outdated statute is imminent. Whether Congress revisits the statute, updating its language for the new millennium, or the Supreme Court resolves the circuit split now in effect,[77] the result of the First Circuit's ruling is to place the spotlight on a subject that concerns many Internet users by demonstrating that stopgap measures will no longer suffice.

77. *Councilman IV*, 418 F.3d at 88.