What Online Activity Does the Wiretap Act Protect? The Ninth Circuit Holds that Unauthorized Access of a Secure Website Does Not Violate the Federal Wiretap Act
Konop v. Hawaiian Airlines, Inc.

by
*Thomas P. Ludwig**

I. INTRODUCTION

Throughout the last half-century, there has been constant tension in the communication arena between individual privacy interests and the interests of law enforcement in proactively combating crime and terrorism. The difficulty in maintaining a balance between these interests has been compounded by the explosive development in electronic communication technology over the last several decades. In an attempt to bring the state of privacy protection law up to date with modern technology, Congress enacted the Electronic Communications Privacy Act of 1986 ("ECPA").[1] While the ECPA was enacted "to update and clarify Federal privacy protections and standards,"[2] both the usage and the sophistication of electronic communication have soared dramatically since that time, thus rendering the ECPA currently outmoded.[3] Courts have described the intersection of the Wiretap Act and the Stored Communications Act as a "complex, often convoluted, area of the law."[4] More specifically, "[c]ourts and scholars have struggled to determine the precise boundaries of and also the intended relationship between these two acts."[5] The judiciary has traditionally narrowly construed the term "interception," as used in the Wiretap Act, to require acquisition that is contemporane-

---

* The author received a B.A. in Mathematical Economic Analysis and Managerial Studies from Rice University in May 2001 and is a candidate for Juris Doctor, class of 2004, at Southern Methodist University Dedman School of Law. The author would like to thank his family for their support and his friend, Ryan Idzior, for his suggestions.

1. Pub. L. No. 99-508. 100 Stat. 1848 (1986). Title I of the ECPA amended the federal Wiretap Act, expanding its protection against "interception" of wire and oral communication to include protection of electronic communication. 18 U.S.C. §§ 2510-2522 (2000 & Supp. 2002). Title II of the ECPA, the "Stored Communications Act," added protection against the unauthorized "access" of electronic communications while in electronic storage. *Id.* §§ 2701-2711.

2. S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

3. Robert Zakon, *Hobbes' Internet Timeline*, *at* http://www.zakon.org/robert/internet/timeline. At the time of the ECPA's enactment in October 1986, there were approximately 5,000 host computers connected to the Internet. Today there are more than 160 million host computers with Internet access in the United States.

4. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

5. Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 625, 633 (E.D. Pa. 2001).

ous with the transfer of the communication.[6] This narrow construction has meant that the increased protection of the Wiretap Act has only applied to communications acquired en route in the transfer, while communications located in any type of electronic storage are only afforded the lesser protection of the Stored Communications Act.[7] Such an interpretation opens the door for unconscionable privacy invasion by judicially unsupervised law enforcement agencies without providing serious deterrence to cyber-criminals. Recently, in *Konop v. Hawaiian Airlines, Inc.*,[8] the Ninth Circuit followed this traditional approach and, in doing so, exhibited the extent to which electronic communication privacy law must be clarified and modernized to afford any meaningful privacy protection for online communication in today's technologically advanced world.

II. BACKGROUND

Robert Konop, a pilot for Hawaiian Airlines ("Hawaiian"), maintained a password-protected website, on which he posted bulletins critical of his employer, its officers, and the incumbent union, who were not allowed access to the site. Konop required visitors to log in with a user name and password. He created a list of individuals, mostly employees of Hawaiian, who were eligible to access the website. To obtain a password, eligible persons were required to register and consent to a non-disclosure agreement. Other terms and conditions clearly displayed on the sign-on page prohibited members of either Hawaiian or union management from viewing the website.

Hawaiian vice-president James Davis was able to gain access to Konop's restricted website by obtaining passwords from two eligible Hawaiian pilots, Gene Wong and James Gardner. The two pilots freely provided their information when Davis asked for their permission to access the website using their names. In signing on, Davis accepted the terms and conditions of the website, despite the prohibition against management access. Davis continued to view the website under both pilots' identities for several months and also shared information from the website with other management and union employees.

Upon becoming aware of this unauthorized viewing, Konop filed suit against Hawaiian in the U.S. District Court for the Central District of Califor-

6. Recent Case, 114 HARV. L. REV. 2563 (2001).

7. *Compare* 18 U.S.C. § 2511(4)(a) (imposing criminal penalties of up to 5 years' imprisonment and a $10,000 fine under the Wiretap Act) *with* 18 U.S.C. §§ 2701(b)(1)(A) (imposing lesser criminal penalties of up to 1 year's imprisonment and a $1,000 fine under the Stored Communications Act). *Compare also* 18 U.S.C. § 2511(2)(a) (requiring a specially approved court order to intercept a communication under the Wiretap Act) *with* 18 U.S.C. § 2703(d) (requiring only a search warrant for disclosures of stored electronic communications to law enforcement).

8. 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 123 S. Ct. 1292 (2003).

nia, alleging that Hawaiian's unauthorized viewing and use of his secure website violated both the federal Wiretap Act, as amended by Title I of the ECPA, and the Stored Communications Act. Konop also brought several other claims under the Railway Labor Act ("RLA") and state tort law. The district court granted summary judgment to Hawaiian on the entire action except one of the RLA claims, on which the court entered judgment against Konop after a short bench trial. Konop appealed the district court's granting of summary judgment to the Ninth Circuit.

III. Procedural History

In its original opinion, the Ninth Circuit reversed and remanded, holding that a narrow interpretation of the Wiretap Act, limiting the term "intercept" to mean contemporaneous acquisition, was not consistent with the purpose, language, or text of the ECPA.[9] The court reasoned that because electronic storage is necessarily a part of the entire communication process, the definition of "electronic communication" impliedly covers electronic storage, even if not specifically referenced.[10] Although the Ninth Circuit attempted to fit its opinion within the framework of legislative intent and precedent from its own jurisdiction and the Fifth Circuit, its conclusions lay diametrically opposed to those of the earlier cases, which have all basically followed in line with the first case to introduce the narrow interpretation of "intercept," *United States v. Turk*.[11] The Ninth Circuit avoided the implications of *Turk* with the argument that the ECPA had subsequently amended the Wiretap Act, and the Act's new structure and definition of "wire communication" to include stored information did not harmonize with the older, narrower definition of "intercept" in *Turk*.[12] This opinion was withdrawn, however, and the court subsequently filed a new opinion in its place.

In this second opinion, the Ninth Circuit panel affirmed the district court's summary judgment ruling with regard to the Wiretap Act claim, but reversed and remanded the Stored Communication Act claim on a technical-

9. Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1043-44 (9th Cir.), *withdrawn,* 262 F.3d 972 (9th Cir. 2001). This decision created a significant stir in the legal community when it was released early in 2001 because the holding was contrary to traditional judicial interpretation of the ECPA, which is that the Wiretap Act does not protect communications while in electronic storage.

10. *Id*. at 1045 (citing Tatsuya Akamine, *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 (1999)).

11. 526 F.2d 654, 658-59 (5th Cir. 1976) (holding that police had not unlawfully intercepted a communication when they played back a tape of a telephone call that had been previously recorded by a third party because the Wiretap Act required acquisition contemporaneous with the transmission).

12. *Konop*, 236 F.3d at 1043.

ity.[13] Following more in line with precedent, the court adopted the narrow definition of "interception," requiring acquisition contemporaneous with the transfer of the communication for a violation of the Wiretap Act.[14] The court concluded that because Konop's website constituted a *stored* electronic communication, which is not included in the Wiretap Act's definition of "interception," summary judgment on the Wiretap Act claim was proper.[15] With regard to the Stored Communications Act claim, the court held that summary judgment was not appropriate because a question of fact existed as to whether Davis's viewing of Konop's website fell under the user authorization exemption of Section 2701(c)(2).[16]

IV. The Ninth Circuit's Decision

Judge Boochever, writing for the majority a second time, began his analysis with a summary of the Wiretap Act and its treatment by the courts. The Wiretap Act, as amended by the ECPA, makes it an offense to "intentionally *intercept* . . . any wire, oral, or electronic communication."[17] "Interception" is defined as "the . . . acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic . . . or other device."[18] Looking at the definition alone, it would seem "that an individual 'intercepts' an electronic communication merely by acquiring its contents, regardless of when or under what circumstances the acquisition occurs."[19] Based on precedent and the context of the Wiretap Act in the ECPA, however, the majority concluded that Congress intended a narrower meaning for "intercept" with regard to electronic communication.[20] In coming to this conclusion, the court found it critical that the definition of "electronic communication" in the Wiretap Act did not include electronic storage of such communication, while the definition of "wire communication" ex-

13. *Konop*, 302 F.3d at 879-80.

14. *Id*. at 878 (citing Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (holding that Congress's use of the word "transfer" and its omission of the term "electronic storage" in the definition of electronic communication reflects Congress's intent that "intercept" not apply to electronic communications while they are in electronic storage)).

15. *Id*. at 879.

16. *Id*. at 880. The court found that a material question of fact existed as to whether Wong and Gardner were actually users of Konop's website, and thus able to authorize Davis's access to the website.

17. 18 U.S.C. § 2511(1)(a).

18. *Id*. § 2510(4).

19. *Konop*, 302 F.3d at 876.

20. *Id*.

plicitly encompassed communications in electronic storage.[21] By including the electronic storage of wire communications within the scope of the Wiretap Act, but declining to do so for electronic communications, Congress evinced its intent to make the interception of electronic communication unlawful under the Act only if it occurs contemporaneously with the transmission.[22] The majority maintained that this reasoning was employed by the Fifth Circuit in *Steve Jackson Games, Inc. v. United States Secret Service*,[23] and endorsed by the Ninth Circuit in *Smith*.[24] The majority found further support for this reasoning in the fact that Congress later amended the Wiretap Act, eliminating storage from the definition of wire communication.[25] "When Congress passed the USA PATRIOT Act, which amended the Wiretap 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."[26] Instead, Congress modified the statute so that the narrower definition applied to wire communications as well, implying implicit legislative acceptance and approval of the judicial definition of "intercept" as "acquisition contemporaneous with transmission."[27] Finally, the majority in *Konop* also found that such a narrow definition of "in-

21. *Id*. at 877. At the time of *Konop*, "electronic communication" was defined as "any transfer of signs, signals, writing, images, sounds, data . . . transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system." 18 U.S.C. § 2510(12). "Wire communication" was defined 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 . . . *and such term includes any electronic storage of such communication*." 18 U.S.C. § 2510(1). The emphasized portion of the definition of "wire communication" was later removed by the USA PATRIOT Act, as discussed below.

22. *Konop*, 302 F.3d at 877 (citing Wesley Coll. v. Pitts, 974 F. Supp. 375, 386 (D. Del. 1997), *aff'd*, 172 F.3d 861 (3d Cir. 1998)); *see also* United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) ("Taken together, the definitions thus imply a requirement that the acquisition of [electronic communications] be simultaneous with the original transmission of the data.").

23. 36 F.3d 457 (5th Cir. 1994) (holding that the government's acquisition of email messages stored on an electronic bulletin board system, but not yet retrieved by the intended recipients, was not an "interception" under the Wiretap Act because it was an acquisition of stored communications not contemporaneous with their transmission).

24. *Smith*, 155 F.3d at 1057. Relying on this same textual distinction, the court held that *wire* communications in storage could be "intercepted" under the Wiretap Act, but that the narrower definition of "intercept" requiring contemporaneous acquisition was still appropriate with regard to *electronic* communications.

25. *Konop*, 302 F.3d at 878; USA PATRIOT Act, § 209, 115 Stat. 272, 283 (2001).

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

27. *Id*.

terception" under the Wiretap Act was more consistent with the structure of the ECPA.[28] The ECPA created the Stored Communications Act separately from the Wiretap Act "for the express purpose of addressing 'access to stored . . . electronic communications and transactional records.'"[29] The court concluded that if the Wiretap Act included the acquisition of electronic communications in storage, the lower degree of protection and less restrictive procedures for law enforcement access provided by the Stored Communications Act would be redundant and meaningless.[30]

Dissenting from the majority's opinion regarding Konop's Wiretap Act claim, Judge Reinhardt raised the strong argument that, based on the technological characteristics of the transfer of electronic communication, such a narrow interpretation of the scope of the Wiretap Act would render the Act virtually ineffectual.[31] He noted that storage is necessary and incidental to the transmission of electronic communications; they are temporarily stored in various computers along the transfer route before arriving at their destinations. In addition, the actual transfer of an electronic communication occurs at the speed of light, and the communication is usually broken into many different "packets" and reassembled only upon reaching its final destination. Interception during the instant of transfer—the only time included in the narrow definition of "interception"—is virtually impossible.[32] Judge Reinhardt argued that a narrow, contemporaneous interpretation ignores these practical aspects of electronic communication and makes the Wiretap Act meaningless with respect to such communication.[33] Judge Reinhardt also disagreed with the majority's opinion that "it was reasonable that the term 'intercept' describe different conduct with respect to wire and electronic communication because different actions are required to intercept different kinds of communications."[34] Judge Reinhardt argued that "although wire communications and electronic communications are quite different, stored wire communica-

28. *Id*. at 878.

29. *Id*. at 879.

30. *Konop*, 302 F.3d at 879; *see also* 18 U.S.C. § 2703(a).

31. *Konop*, 302 F.3d at 887.

32. *Id*. at 888. Note, however, that the FBI's "Carnivore" program, which is described in more detail below, *can* intercept electronic communications during the actual transfer period. It is generally not used for this purpose, however, but merely to obtain the addressing information of those communications.

33. *Id*. at 887. The majority's only response to this argument was that in defining "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," Congress made it clear that it understood that electronic storage was an inherent part of the transmission process, but still chose to provide less protection for communication in such a phase. *Id*. at 879; 18 U.S.C. § 2510(17)(a).

34. *Id*. at 888.

tions are technologically equivalent to stored electronic communications," and so it would make little sense to treat them differently.[35]

Judge Reinhardt's dissent raised an entirely different basis for defining the boundary between the Wiretap Act and the Stored Communications Act that was originally proposed in the first *Konop* opinion. Rather than imposing a temporal distinction between the two acts with regard to the acquisition, he suggested that a qualitative distinction between them would eliminate the conflict and confusion of their intersection.[36] While the Wiretap Act deals with "interception" requiring "acquisition" of electronic communications, the Stored Communications Act regulates "access" to communications and the facilities where they are stored.[37] Judge Reinhardt observed that the "access" prohibitions of the Stored Communications Act, contrary to the "interception" prohibitions in the Wiretap Act, do not mention actually acquiring the communication or its contents, but merely prohibit gaining access to them.[38] This interpretation would imply that "Congress intended that *only* [the Wiretap Act] prohibit the actual *acquisition* of the contents of a communication," while Congress intended that the Stored Communications Act set out the parameters by which "governmental authorities can gain 'access' to the 'contents' of stored electronic communications."[39] Judge Reinhardt argued that the "access" prohibited by the Stored Communications Act is merely a lesser offense that is antecedent to and qualitatively different from the "interception" offense proscribed in the Wiretap Act, giving a broader range of protection to the privacy of electronic communications.[40] He maintained that such an interpretation would not cause the Stored Communications Act to be duplicative because unauthorized users and hackers are very often able to do significant damage to stored communications and the facilities they are stored in and law enforcement authorities are often able to access and search electronic communications, both without ever acquiring the contents of those communications.[41]

---

35. *Id*.

36. *Konop*, 302 F.3d at 889. This qualitative interpretation was actually first addressed in *Smith*, when the majority used it to support its holding that an interception of a *wire communication* need not be contemporaneous with its transmission. *See Smith*, 155 F.3d at 1058.

37. *Compare* 18 U.S.C. § 2510(4) *with* 18 U.S.C. § 2701(a)(1).

38. *Konop*, 302 F.3d at 889. Judge Reinhardt argued that the majority's interpretation of these two definitions implies no difference between them other than the point in time at which the acquisition of the communication occurs.

39. *Id*. (emphasis added).

40. *Id*.

41. *Id*. at 890.

V. Analysis

From a practical standpoint, this qualitative interpretation of the dissent harmonizes the intersection of the Wiretap Act and Stored Communications Act in a manner that gives much more effect to the ECPA's primary purpose of privacy protection. It fits the structure of the ECPA much more applicably to the functional aspects of electronic communication and to the current state of technology. The dissent's interpretation would improve the federal protection of private electronic communications by eliminating the distinctions between the somewhat arbitrary stages of their transmission.[42] By providing consistent protection across both the transmission and storage stages of the communication transfer process, the ultimate goal of privacy is much more effectively achieved.[43] This qualitative interpretation avoids the situation in which a hacker or similarly unauthorized party can circumvent the harsher penalties of the Wiretap Act by simply waiting to acquire the contents of an electronic communication until it rests either permanently or temporarily in electronic storage where, ironically, the communication is most vulnerable to unlawful acquisition.

The dissent's interpretation also does not unnecessarily hinder law enforcement agencies' ability to patrol the Internet for criminal or threatening activity. The Department of Justice's infamous "Carnivore" program is able to identify and gather specific addressing information sought under court order without actually acquiring electronic communications or their contents.[44] Under the dissent's qualitative interpretation, this non-intrusive *accessing* of online communication by law enforcement would only be subject to the minimal procedural requirements of the Stored Communications Act, while hackers who unlawfully *acquire* the contents of a communication or secure website would be subject to the much more severe penalties of the Wiretap Act. The dissent's qualitative differentiation between the prohibitions of the

42. Recent Case, 114 Harv. L. Rev. 2563, 2566 (2001).

43. *Id.*

44. Ill. Inst. of Tech. Res. Inst., Independent Review of the Carnivore System: Final Report (2000), *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf (last visited Nov. 9, 2002). The recently enacted USA Patriot Act expressly equates this acquisition of addressing information with the acquisition of the phone numbers of incoming and outgoing calls with the use of what are known as pen registers/trap and trace devices. Because the courts and the legislature found that individuals do not have a reasonable expectation of privacy with respect to phone numbers dialed, the Wiretap Act prescribed very minimal requirements (easily obtained court order) for installing such devices. The Patriot Act now applies those same requirements to the acquisition of addressing information of *electronic* communications. The Carnivore program also possesses the capability to acquire the contents of an electronic communication, but this more intrusive and less common type of acquisition would be subject to the much more stringent procedural requirements of a Title III court order under the Wiretap Act.

Wiretap Act and the Stored Communications Act enhances the privacy protection afforded by the ECPA without impeding the efficacy of law enforcement.

On the other hand, the practical effect of the majority's narrow, temporal interpretation is the virtual elimination of the heightened protection and safeguards of the Wiretap Act from the field of electronic communication because the acquisition of electronic communication during the transmission phase is almost impossible with current technology.[45] Nearly any unlawful acquisition of electronic communication that presently occurs does not take place during the brief instant of actual transfer, but rather during latent storage periods. The resulting deterrent effect on potential cyber-criminals is significantly less due to the considerably weaker repercussions for those convicted of unlawful acquisition of electronic communication.

At the same time, law enforcement has been granted investigative powers that are overly broad and insufficiently subject to judicial oversight. Obtaining what is known as a Title III court order, which is necessary for the acquisition of the contents of an electronic communication under the Wiretap Act, requires that law enforcement successfully convince a judge that there is "probable cause" that the acquisition would produce evidence of a crime.[46] The narrowing of the scope of the Wiretap Act to practical nonexistence means that law enforcement is only required to obtain a § 2703 search warrant under the Stored Communications Act to acquire an electronic communication.[47] The requirements for obtaining a § 2703 warrant are essentially non-existent: "the government must only certify to a judge—without having to prove it—that such a warrant would be 'relevant' to an ongoing criminal investigation."[48] The judge does not even have the authority to reject the application.[49] Basically, under the majority's interpretation of the ECPA, law enforcement has unsupervised power to invade private electronic communication without any evidentiary basis whatsoever. Such a result is in direct opposition to the safeguards and purpose of the ECPA.

Judge Reinhardt's dissent is persuasive from a practical perspective and provides a well-developed model for where privacy protection should be, but unfortunately it lacks legislative and judicial support. He almost casually

45. Again, the hi-tech Carnivore program is an exception, as it is able to filter through all of the individual packets of electronic communication for relevant addressing information *during transmission* by the particular Internet service provider to which the program is attached.

46. American Civil Liberties Union, *More Detail on ACLU Objections to Selected Provisions of Proposed Anti-Terrorism Legislation*, *available at* http://www.aclu.org/congress/Patriot_Links.html (last visited Nov. 9, 2002).

47. David B. Walker, *Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action,* 1999 STAN. TECH. L. REV. 3, at *12 (1999).

48. ACLU, *supra* note 47.

49. *Id*.

dismissed sixteen years worth of precedent and the critical fact that Congress—understanding the courts' interpretation of the ECPA—completely eliminated storage from the prohibitions of the Wiretap Act with the USA PATRIOT Act.[50] In *Steve Jackson Games*, the Fifth Circuit, analyzing the structure of the ECPA, found that Congress clearly intended that the definition of "intercept" require that the acquisition be contemporaneous with the original transmission.[51] The Fifth Circuit found that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage' " for two reasons: (1) Congress's use of the word "transfer" in the definition of "electronic communication," and (2) Congress's omission in the definition of "electronic communication" of the phrase "any electronic storage of such communication," which was part of the definition of "wire communication" until the USA PATRIOT Act eliminated electronic storage from the Wiretap Act altogether.[52] Judge Reinhardt's dissenting opinion simply rejected *Steve Jackson Games* and its precedential authority, stating that it was the only circuit court case involving electronic communication and it was in a different jurisdiction.[53] The holding in *Steve Jackson Games*, however, has been followed by the district courts in every other jurisdiction dealing with electronic communication. Indeed the Ninth Circuit itself endorsed the reasoning of *Steve Jackson Games* in *Smith*.[54] Although the *Smith* court held that the contemporaneous interpretation of the term "intercept" was not appropriate with regard to the acquired wire communication at issue in that case, it cited precedent from several jurisdictions, noting that such a definition "fits like a glove" in cases involving electronic communication.[55] Judge Reinhardt's opinion attempted to harmonize his qualitative interpretation of the prohibitions in the Wiretap Act with the holding in *Smith*, but in reality such an interpretation was a rejection of the holding in that case.[56] The dissenting opinion simply does not fit in the framework of legislative intent and judicial precedent. While Judge Reinhardt's argument that the growth of the Internet has rendered the precedent

50. *See Konop*, 302 F.3d at 891.

51. *Steve Jackson Games, Inc*., 36 F.3d at 461-62.

52. *Id*.

53. *Konop*, 302 F.3d at 891-92.

54. *Id*. at 877; *Smith*, 155 F.3d at 1057.

55. *Smith*, 155 F.3d at 1057; *see also Reyes*, 922 F. Supp. at 836 (following the decision in *Steve Jackson Games* in finding a requirement in the Wiretap Act that the acquisition of an electronic communication be simultaneous with its original transmission); Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996) (requiring acquisition during transmission).

56. *Konop*, 302 F.3d at 891-92. Judge Reinhardt asserted that *Smith* repudiated the contemporaneity requirement of *Turk*, but *Smith* only did so specifically with respect to wire communications, as noted above.

obsolete may be accurate,[57] the judiciary does not have the authority to stretch the plain language of the statute and the associated Congressional intent past the breaking point in order to modernize the law.

VI. Conclusion

From a strictly judicial perspective, the majority's decision in this case is the correct one, even if not the right one. The dissent presents a viable interpretation of the ECPA that is congruent with modern communications technology and provides the full range of privacy protection originally intended with the passing of the ECPA. As the court made clear at the start of its analysis, however, it is a task for Congress, not the judiciary, to bring the laws in line with modern technology.[58] Especially in an area as complex and broad as electronic communication, the courts have neither the resources nor the same access to technical knowledge to clarify and modernize privacy protection law in a case-by-case fashion through judicial interpretation. By following judicial precedent and legislative history, the court in this case remained within the bounds of its authority and reemphasized the need for legislative action. However, the conflict and confusion in the current law that has weakened federal privacy protection is not likely to be soon corrected by the legislature. The courts have been calling this problem to the attention of Congress for many years with little to no effective response. In addition, the recent domestic infiltration and attacks by perpetrators of terrorism will likely tip the policy balance between communication privacy interests and the interests of law enforcement and public safety toward the latter with regard to future legislation. Indeed, the recently passed USA PATRIOT Act has already demonstrated this shift. In light of these considerations, *Konop* is simply a further slip down a legislatively unstructured slope of weakening privacy protection for individuals in the area of electronic communication.[59]

57. *Id*. at 892.

58. *Id*. at 874.

59. Shortly before publication of this note, the Supreme Court denied Konop's petition for a writ of certiorari and recent decisions in both the First and Eleventh Circuits have followed the holding in Konop. These developments give rise to the conclusion that little will change in the current climate of favoring the interests of national security over civil liberties.