Spring 2001


Carlos Perez-Albuerne

Lawrence Friedman

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation


http://repository.jmls.edu/jitpl/vol19/iss3/1

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
ARTICLES

PRIVACY PROTECTION FOR ELECTRONIC COMMUNICATIONS AND THE "INTERCEPTION-UNAUTHORIZED ACCESS" DILEMMA

by CARLOS PEREZ-ALBUERNE†
AND LAWRENCE FRIEDMAN‡

I. INTRODUCTION

As Americans increasingly relate to one another through electronic means, the privacy of electronic communications has emerged as a matter of concern to individuals and businesses alike. To the extent privacy protection for personal and commercial communications exists in this digital age, it is more likely to be found in statutory and regulatory direc-

† Attorney, Choate, Hall & Stewart, Boston, Massachusetts. Mr. Perez-Albuerne is a member of Choate, Hall & Stewart's Business & Technology and Government Enforcement Practice Groups.
‡ Climenko/Thayer Lecturer on Law, Harvard Law School.
Seth Aframe, Kathleen Burdette and David Englander read earlier drafts of this essay and offered excellent suggestions for its improvement. Naomi Sevilla provided unparalleled research support and editorial assistance. They should not be held responsible for any mistakes that remain.

1. It is estimated that by the year 2002 more than 1.5 billion e-mail messages will be sent daily in the United States. See Bob Tedeshi, Wary of Hackers and the Courts, E-mail Users Are Turning to Services That Keep Their Messages Secure, N.Y. Times, C11 (Jan. 31, 2000). Privacy in general, meanwhile, has become a genuine concern. A 2000 survey revealed that 61 percent of online users “are concerned that their e-mail will be read by someone else, without their knowledge or consent.” Charles Nesson, Threats to Privacy, 68 Soc. Research 105, 107 (Apr. 1, 2001) (available in 2001 WL 24181707). A 1999 survey “indicated that privacy is the issue that concerns Americans most about the twenty-first century, ahead of overpopulation, racial tensions, and global warming.” Toby Lester, The Reinvention of Privacy, Atlantic Mthly., 27 (Mar. 2001). Some commentators have speculated that public concern over privacy reflects a recognition that “[p]rivaicy of conversation is no longer, as it was 200 years ago, a fact of life.” Whitfield Diffie & Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption 3 (1998) [hereinafter Diffie].

435
tives than in constitutional or common law. In a noteworthy display of foresight, Congress, in 1986, modified the Wire and Electronic Communications Interception and Interception of Oral Communications Act ("Wiretap Act") through the Electronic Communications Privacy Act ("ECPA"), broadening the scope of prohibitions against electronic eavesdropping to encompass a range of conduct involving computer communications.\(^2\)

With ECPA, Congress substantially amended the federal Wiretap Act to prohibit unauthorized "interception" of "electronic communications."\(^3\) In addition, ECPA contained the Stored Communications Act, which prohibits "access" to "a facility through which an electronic communication service is provided."\(^4\)

Notwithstanding Congress' laudable goals in enacting statutory protection for electronic communications, the resulting law can scarcely be considered a model of clarity.\(^5\) Indeed, the United States Court of Appeals for the Fifth Circuit has noted that the Wiretap Act "is famous (if not infamous) for its lack of clarity."\(^6\) In a more recent decision construing the terms of ECPA's modifications of the Wiretap Act, the United States Court of Appeals for the Ninth Circuit remarked that the Fifth Circuit "might have put the matter too mildly."\(^7\)

Among the many complicated aspects of the ECPA regime is the intersection of the statutory concepts of "interception" and "unauthorized access" as they relate to electronic communications within the context of both the Wiretap Act and the Stored Communications Act.\(^8\) In this essay, we review attempts by two federal courts of appeals to make sense of "interception" and "unauthorized access" in a way that takes into account the technological realities of electronic communications and that comports with the goal of enhancing privacy protection for such communications. Part II recounts the history of ECPA's passage into law and Congress' intended purpose. Part III discusses the cases in which the courts have addressed the "interception-unauthorized access" dilemma. Finally, Part IV examines the practical statutory implications of the different judicial constructions of ECPA's provisions regarding "interception" and "unauthorized access," and the normative implications of those

---


3. See 18 U.S.C. § 2510(12). The statute defines "electronic communication" to include any transfer of electronic mail, digitized transmission, video teleconferencing, some radio transmissions, and transmissions consisting exclusively of data. *Id.*


5. *See infra* n. 6 and accompanying text.


constructions of ECPA. This article concludes that when, as with "interception" and "unauthorized access," the statutory scheme is unclear, courts properly should consider the nature of electronic communications and the privacy concerns associated with such communications in construing the law.

II. PROTECTING THE PRIVACY OF ELECTRONIC COMMUNICATIONS

We ground our analysis of ECPA and the cases construing ECPA in the supposition that protecting privacy is an objective worthy of legislative and judicial attention. This is because privacy has value as a necessary condition or circumstance for the conduct of ordinary human affairs. As Professor Charles Fried has explained:

[Privacy] is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable. They require a context of privacy or the possibility of privacy for their existence.\(^9\)

By establishing a context in which relationships based upon respect, love, friendship and trust can be developed, privacy allows individuals to maintain control over information in respect to, or in furtherance of, these matters.\(^10\) Absent such control, one might pause terminally before entering into these and other personally or commercially beneficial relationships.\(^11\)

While Congress may not have actively contemplated such a broad-ranging justification for maintaining the privacy of communications when considering the threats to privacy created by new technologies, the

---

9. Charles Fried, Privacy, 77 Yale L.J. 475, 477 (1968); see also Alan F. Westin, Privacy and Freedom 13 (1967) (observing that "[n]eeds for individual and group privacy and resulting social norms are present in virtually every society. Encompassing a vast range of activities, these needs affect basic areas of life for the individual, the intimate family group, and the community as a whole."); Lucas D. Introna, Privacy and the Computer: Why We Need Privacy in the Information Society, Cyberethics 188, 191 (Robert M. Baird ed., 2000) (stating that "[i]t is clear that all social relationships, relationships of collaboration or of competition, require at least some level of privacy").

10. Fried, supra n. 9, at 482; see also Diffie, supra n. 1, at 126 (equating loss of control over information with loss of privacy); Jeffrey Rosen, Out of Context: The Purposes of Privacy, 68 Social Research 209, 215 (Apr. 1, 2001) (available in 2001 WL 2418713) [hereinafter Rosen, Out of Context] (defining "privacy" as "the ability to exercise control over personal information").

11. Fried, supra n. 9, at 483–84. As Fried has reasoned:

If we thought that our every word and deed were public, fear of disapproval or more tangible retaliation might keep us from doing or saying things which we would do or say if we could be sure of keeping them to ourselves or within a circle of those who we know approve or tolerate our tastes.

Id.
statutory text and history of ECPA reveal a concern to protect a fundamental core of privacy in respect to new technologies. Congress first addressed the need to protect privacy in the context of evolving technology by regulating wiretapping and electronic surveillance in 1968, with Title III of the Omnibus Crime Control and Safe Streets Act.\(^\text{12}\) That legislation regulated the use, manufacture, possession and advertising of electronic surveillance devices and reflected a Congressional recognition that technological developments had enhanced the ability of individuals surreptitiously to intercept personal communications, increasing significantly the potential for detrimental infringement of personal privacy.\(^\text{13}\)

The legislative history of ECPA reveals that privacy protection lay at the heart of the statutory scheme.\(^\text{14}\) As the Senate Report on the statute indicated, “[n]o longer is it possible . . . for each man to retreat into his home and be left alone. Every spoken word relating to each man’s personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor’s advantage.”\(^\text{15}\) The Senate Report expressed particular concern for the potential harms the new technology posed for the protection of trade secrets and similar confidential business information.\(^\text{16}\)

Though members of Congress shared a concern for the protection of personal and commercial communications, due to the technological realities of the time, Title III’s reach was relatively limited when compared to the understanding of such issues today. Title III’s provisions prohibited only the interception of communications that could be heard and understood by humans as sound,\(^\text{17}\) but only when transmitted via common carriers.\(^\text{18}\)

Congress amended Title III several times between 1970 and 1986,\(^\text{19}\) but it did not fully address the rapid advances in telecommunications wrought by the proliferation of computers and computer technology until 1986, when it enacted ECPA. In Title I of ECPA, Congress modified the


\(^{14}\) Id. at 2153.

\(^{15}\) Id. at 2154.

\(^{16}\) See id. at 2156.


Wiretap Act to cover new communications technologies. Congress substituted “provider of wire or electronic communication service” for “communications common carrier” throughout the statutory scheme, thereby expanding the number and kind of telecommunications carriers to which the Wiretap Act’s provisions could be applied. In addition, Congress added “electronic communications” to the kinds of communications protected under the Wiretap Act. As defined by ECPA, “electronic communications” include transfers of electronic mail, digitized transmissions, video teleconferencing, some radio transmissions, and transmissions consisting exclusively of data.

In Title II of ECPA, Congress created new measures specifically designed to protect facilities storing electronic communications in response to evidence indicating an increase in efforts by individuals to access stored electronic communications without authority to do so. Congress addressed the growing problem of unauthorized access to and tampering with private electronic communications held by communications service providers by prohibiting the improper and intentional access of facilities in which electronic or wire communications are stored.

As defined by ECPA, “electronic storage” means any temporary or intermediate storage of a wire or an electronic communication incidental to its transmission, as well as storage for purposes of backup protection. Congress also created a private cause of action for individuals who claim injury as a result of alleged violations of the new restrictions governing unauthorized access to stored communications.

In total, ECPA evinces a concern to provide protection for electronic communications generated by individuals (Title I), as well as protection for certain providers of communications services (Title II). By its modifications to the Wiretap Act and creation of the Stored Communications Act, ECPA substantially expands the scope of statutory privacy protections afforded both to communications services providers and to individ-

---

20. See 100 Stat. 1848.
21. See id. at 1851–52 (1986) (amending the Wiretap Act to include private communication system providers as well as any other provider of wire or electronic communication service).
23. Id.
uals who choose to communicate through electronic means.\textsuperscript{30}

III. QUESTIONS REGARDING INTERCEPTION AND ACCESS TO STORED COMMUNICATIONS

At this writing, the \textit{Wiretap Act} prohibits the interception of any wire, oral or electronic communications,\textsuperscript{31} while the \textit{Stored Communications Act} prohibits unauthorized access to a facility that stores electronic or wire communications.\textsuperscript{32} The \textit{Wiretap Act} 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.”\textsuperscript{33} Neither the \textit{Wiretap Act} nor the \textit{Stored Communications Act} defines “access.”

Despite a statutory definition of “intercept,” issues regarding the meaning of “interception” under the \textit{Wiretap Act} and “unauthorized access” under the \textit{Stored Communications Act} have frequently arisen. Indeed, even before the issue arose in the context of electronic communications, the federal courts of appeals sought to address the


\textsuperscript{31} \textit{See} 18 U.S.C. § 2511(1)(a) (2000). Specifically, the statute provides that any person who “intentionally intercepts, endeavors to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication,” shall be subject to criminal punishment or civil suit, as the case may be. \textit{Id.}

\textsuperscript{32} \textit{See} 18 U.S.C. § 2701. Specifically, the statute provides that any person who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system” shall be subject to criminal punishment. \textit{Id.} § 2701(a).

\textsuperscript{33} 18 U.S.C. § 2510(4). The statute defines an “oral communication” as “any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.” \textit{Id.} § 2510(2). The statute defines an “electronic, mechanical, or other device” as

any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal.

\textit{Id.} § 2510(5).
meaning of "interception" in the context of oral communications. For instance, in United States v. Turk, the United States Court of Appeals for the Fifth Circuit faced the question whether law enforcement officers who listened to a cassette tape seized from an individual's car conducted an impermissible "interception" under the 1968 Omnibus Crime Control and Safe Streets Act. The court concluded that the term "interception" should be defined by reference to "the activity engaged in at the time of the oral communication which causes such communication to be overheard by uninvited listeners." In other words, "[i]f a person secretes a recorder in a room and thereby records a conversation between two others, an 'acquisition' occurs at the time the recording is made." In the alternative, the court reasoned that an "aural acquisition" – and thus an "interception" – could also occur when both the initial acquisition and the later hearing is accomplished by the person or persons responsible for engineering that acquisition. Either understanding of the statute, though, is predicated upon the participation of the individual charged with an "interception" "in the contemporaneous acquisition of the communication through the use of the device [in question]." No such "interception" occurs simply upon the replaying of a recorded oral communication by individuals who did not participate in the original recording. The court termed such replaying as "derivative acquisition."

With the advent of electronic communication, courts again faced the problem of determining when "interception" of a communication occurs for statutory purposes. In Steve Jackson Games, Inc. v. United States Secret Service, the Fifth Circuit addressed the question whether obtaining certain electronic communications should constitute an interception subjecting the actor to liability under the Wiretap Act. The electronic communications at issue in Steve Jackson Games were private electronic mail ("e-mail") messages, unread and sitting on an electronic bulletin board. The United States Secret Service seized a computer that hosted the electronic bulletin board service and, consequently, held the e-mails. Following a civil action brought by Steve Jackson Games in which the lower court determined that no "interception" had occurred

35. See id. at 657.
36. Id. at 658 (emphasis added).
37. Id.
38. See id.
39. Id.
40. Id.
41. Id.
42. 36 F.3d at 458.
43. See id.
44. See id. at 459.
within the comprehension of the Wiretap Act, the Fifth Circuit framed the question thus: "Whether the seizure of a computer on which is stored private e-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes [a proscribed] 'intercept.'"

Adhering to what it perceived to be the guidance of Turk, the Fifth Circuit imported the "contemporaneous acquisition" requirement into the electronic communications context. Relying upon a textual distinction between the Wiretap Act's treatment of oral and wire communications, on the one hand, and electronic communications, on the other, the court ruled that electronic communications must be acquired contemporaneously with transmission to be intercepted. This textual distinction flows from ECPA, which modified the Wiretap Act in 1986 to provide protection for electronically stored wire communications from unauthorized disclosure via interception, even absent contemporaneous acquisition. Thus, listening without authorization to a stored voice mail message may constitute a violation of the Wiretap Act. No similar provision exists in the Wiretap Act for electronic communications.

The Fifth Circuit viewed this differing treatment of wire and electronic communications as textual evidence that Congress intended to provide lesser protection to stored electronic communications under the Stored Communications Act than to wire and oral communications, which receive full protections from unauthorized acquisitions under the Wiretap Act. The court accordingly held that pursuant to the plain language of the two statutes, the stored electronic communications on the Steve Jackson Games server were protected from unauthorized disclosure only under the less strict regime imposed by the Stored Communications Act.

---

46. Steve Jackson Games, 36 F.3d at 460.
47. Id. at 441.
48. See id. at 461–62.
49. See 18 U.S.C. § 2510(1) (defining "wire communication" to include "electronic storage of such communication").
51. See Steve Jackson Games, 36 F.3d at 461–63.
52. See id. at 462–63. Other courts have since held likewise. See e.g. Wesley College v. Pitts, 974 F. Supp. 375, 385–88 (D. Del. 1997) (concluding that plain language and legislative history of Wiretap Act and comparison to Stored Communications Act indicate that Congress did not intend for "intercept" to apply to electronic communications in "electronic storage"); Bohach v. City of Reno, 932 F. Supp. 1232, 1235–36 (D. Nev. 1996) (concluding that statutory language of Wiretap Act distinguishes "interception" of an electronic communication "from the retrieval of such a communication after it has been put in 'electronic storage' in the course of regular operations of the business').
Construing the very same statutory provisions, the United States Court of Appeals for the Ninth Circuit, in *Konop v. Hawaiian Airlines*, rejected the Fifth Circuit’s reasoning and held that the acquisition of stored electronic communications may constitute a violation of the *Wiretap Act*. In *Konop*, the plaintiff, an employee of the defendant airline, sought money damages under the *Wiretap Act* when the airline allegedly used passwords given to other employees to access the employee’s Web site, which was dedicated to the organization of a new airline pilot’s union. The employer’s use of the third-party password violated the terms under which the other employees had been granted access to the Web site. The Ninth Circuit faced the question whether such access to electronic information (the Web site pages) stored on the computer of the employee’s Internet Service Provider constituted an “interception” thereby implicating the penalty provisions of the *Wiretap Act*, or, rather, whether the access constituted merely unauthorized access to electronic communications under the *Stored Communications Act*.

The Ninth Circuit declined to construe the *Wiretap Act* to require “contemporaneous acquisition” as a requirement for an interception of electronic communications. Focusing on the text of the provisions detailing the purposes and prohibitions of the *Wiretap Act* and *Stored Communications Act*, the court concluded that electronic communications should be treated like wire and oral communications. The court noted that the inclusion of “storage” within the definition of “electronic communications” so as to escape the contemporaneous acquisition requirement was simply unnecessary because electronic communications, unlike wire or oral communications, are necessarily subject to storage; indeed, elec-

---

53. *Konop v. Hawaiian Airlines*, 236 F.3d 1035 (9th Cir. 2001). The United States Court of Appeals for the Ninth Circuit withdrew its opinion in *Konop* in August 2001, eight months after its initial release and only weeks before this essay was scheduled for publication. See *Konop v. Hawaiian Airlines*, 2001 WL 968439 (9th Cir. Aug. 28, 2001). The court did not release a new or revised opinion. *Id.* We do not believe that the court’s withdrawal of the original opinion invalidates the useful lessons that can be drawn from it, though the reader should be aware that all citations to *Konop* herein refer to the original opinion.

54. *Konop*, 236 F.3d at 1046 (holding “the *Wiretap Act* protects electronic communications from interception when stored to the same extent as when in transit”).

55. *Id.* at 1041–42.

56. *Id.* at 1041.

57. See *id.* at 1042.

58. *Id.* at 1044–45.

59. *Id.* at 1042.
tronic communication "cannot successfully be completed without being stored." Thus, Congress had no need to include the concept of storage expressly within its definition of "electronic communication" for purposes of understanding "interception" under the Wiretap Act.

Viewing the omission of stored electronic communications from the Wiretap Act as a technical oversight, the court held that Congress could not have intended to provide materially fewer protections for stored electronic communications than for stored oral or wire communications. "An electronic communication in storage," the court reasoned, "is no more or less private than an electronic communication in transmission." Distinguishing between the two for purposes of protection from interception is 'irrational' and 'an unsupportable result given Congress' emphasis of individual privacy rights during the passage of the ECPA.' The court accordingly concluded, "[i]t is perfectly clear that the framers of the Wiretap Act's current definition of 'electronic communication' understood that term to include communications in transit and storage alike."

Importantly, the Konop court relied in its analysis on jurisprudence concerning oral and wire communications under the Wiretap Act and Stored Communications Act that differentiate between the substantive ends of each statute. The Ninth Circuit recognized that the Stored Communications Act, by its terms, prohibits only unauthorized access to a facility storing communications, and not necessarily the subsequent acquisition of the contents of those communications, which may amount to an "interception" under the Wiretap Act. Securing "access" to a stored electronic communication, in other words, involves being in a position to acquire communication from a third-party service provider through which electronic communications may be transmitted and stored, as distinguished from the subsequent acquisition of that communication through an interception under the Wiretap Act.

---

60. Id. at 1045; 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. & Policy 519, 561 (1999). As one commentator has observed, "'electronic storage' is part of the entire [electronic] communication process, and thus, the definition of 'electronic communication' impliedly covers 'electronic storage,' whether or not that definition includes the specific reference to 'electronic storage.'" Id.

61. Konop, 236 F. 3d at 1042.

62. Id. at 1045-46.

63. Id. at 1045.

64. Id. (quoting Thomas Greenberg, E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 Am. U. L. Rev. 219, 248-49 (1994)).

65. Id. at 1046.

66. See id. at 1044.

67. See Smith, 155 F.3d at 1059 (reasoning that "[o]ne assuredly can access a communications facility — such as a company voicemail system — without listening to or recording any of the messages stored within that facility"), cert. denied, 525 U.S. 1071 (1999).

68. Id. at 1058.
Wiretap Act and Stored Communications Act are complementary, and privacy protection for both electronic and wire communications is maximized.

As Steve Jackson Games and Konop demonstrate, the intersection of the Wiretap Act and the Stored Communications Act in circumstances in which electronic communications are obtained by third parties presents a challenging problem of statutory interpretation, a problem exemplified by the Fifth and Ninth Circuits' differing constructions of the same statutory text.69 This problem is exacerbated by the technological realities of modern Internet-based electronic communications and will be further complicated by the relentless evolution of communications technology.70 After all, the Internet-based communications we take for granted today barely existed when Congress enacted ECPA, and courts and commentators are simply attempting to adapt ECPA's provisions to situations and innovations that ECPA's framers likely did not contemplate.

The most significant aspect of the problem may be the storage and reproduction of message data throughout the communications pathway as part of the regular course of traffic propagation.71 Because this continuous storage and reproduction is critical to the architecture of Internet-based electronic communications, resolution of the "interception" question has important implications for both the policies that individuals and private and governmental entities should adopt in respect to Internet-based electronic communications and the larger question of the privacy that will or should attach to such communications.

---

69. See generally Steve Jackson Games, 36 F.3d 457; see generally Konop, 236 F.3d 1035.

70. To insist on comparing electronic communications technologies to their analog counterparts does not help matters. In Fraser v. Nationwide Mutual Ins. Co., the United States District Court for the Eastern District of Pennsylvania concluded that the Wiretap Act does not protect e-mails stored post-transmission from acquisition by third parties. 135 F. Supp.2d 623 (E.D. Pa. 2001). The court reasoned that "interception" can only be accomplished during transmission of the communication and that acquisition of the e-mail after transmission is akin simply to retrieving an opened letter from the desk of a recipient. See id. at 634 n. 17. On one level, the Fraser court failed to appreciate the important differences between an e-mail stored in an e-mail account and a piece of correspondence sitting in plain view to all passersby. On another, the court, like the Fifth Circuit in Steve Jackson Games failed to appreciate that, regardless of the common meaning of "interception," that term has been defined by Congress in the context of wire and electronic communications to include post-transmission obtainment. See Smith, 155 F.3d at 1057 (observing that when a word is defined by statute, "courts are not at liberty to look beyond the statutory definition").

71. See Konop, 236 F.3d at 1045 (noting that "[e]lectronic communication . . . cannot successfully be completed without being stored"); see also David J. Loundy, E-Law 4: Computer Information Systems Law & System Operator Liability, 21 Seattle U. L. Rev. 1075, 1145 (1998) (noting that at some point during transmission, all e-mails are stored).
IV. IMPLICATIONS OF THE "INTERCEPTION-UNAUTHORIZED ACCESS" DILEMMA

The question whether a particular act undertaken to acquire or to obtain an electronic communication constitutes an "interception" or "unauthorized access" for purposes of the Wiretap Act and the Stored Communications Act is significant for two reasons. First, the answer to the "interception-unauthorized access" question necessarily affects the legal limits of the ability of either the government or individuals to eavesdrop on electronic communications or otherwise to acquire electronic communications, as well as the civil and criminal consequences of doing so. Second, as a normative matter, resolution of the "interception-unauthorized access" dilemma under the Wiretap Act and the Stored Communications Act has implications for the ideal of privacy that the Wiretap Act and ECPA contemplate and that the courts should seek to protect.

A. DIFFERENT STATUTORY CONSEQUENCES OF "INTERCEPTION" AND "UNAUTHORIZED ACCESS"

Whether an act is deemed to be an "interception" or "unauthorized access" under the Wiretap Act or the Stored Communications Act, respectively, has consequences for the conduct of criminal investigations and proceedings and the potential penalties for individuals involved in the interception or acquisition of electronic communications. There are at least two issues at stake in the criminal context: the procedural requirements that serve as the predicate to law enforcement interception or access to stored electronic communications, and the sanctions available for individuals convicted of illegal "interception" of or "unauthorized access" to electronic communications. Further, the "interception-unauthorized access" dichotomy raises an issue in the civil context regarding the potential consequences for individuals who obtain electronic communications through either "interception" of or "unauthorized access."

Consider, first, the procedural issues in the criminal context when the government seeks to obtain electronic communications. The Wiretap Act contains extensive procedural requirements that must be met to obtain authorization to intercept communications under its auspices, as well as substantive limitations on the goals that interception may be used to achieve.72 In contrast, under the Stored Communications Act,
governmental entities or agents seeking to access certain electronically stored communications may do so upon securing a warrant that satisfies traditional constitutional standards.\textsuperscript{73} Given that the constitutional prerequisites for a broad array of searches are relatively low when compared to the requirements imposed by the \textit{Wiretap Act},\textsuperscript{74} widespread adoption of the Fifth Circuit's construction of the \textit{Wiretap Act} and \textit{Stored Communications Act} in \textit{Steve Jackson Games} could serve to encourage law enforcement and other governmental entities and agents to seek stored electronic communications in circumstances in which they otherwise might not – that is, in circumstances in which there may be less reason to suspect electronic communications of containing incriminating evidence than comparably stored wire communications.\textsuperscript{75} In other words, the differing treatment of electronic and wire communications advanced by the Fifth Circuit may create some additional incentive for governmental entities to intrude unnecessarily upon ostensibly private communications.

The second issue in the criminal context is the potential sanctions for the law's violation. So far as efforts by private individuals to obtain electronic communications are concerned, electronic communications are treated differently depending whether one views an individual's obtaining of the communication as "interception" or "unauthorized access."

\textsuperscript{73} See 18 U.S.C. § 2703 (2000). Specifically, the statute provides that:
[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.
\textit{Id.} § 2703(a). For electronic communications stored in a system for more than one hundred eighty days, the governmental entity may require disclosure without prior notice to the subscriber or customer of the electronic communication service with a warrant, or by means of an administrative subpoena or court order, so long as notice is provided to the subscriber or customer. \textit{See id.} § 2703(b)(1).

\textsuperscript{74} While the U.S. Supreme Court continues to voice a belief that the U.S. Constitution requires law enforcement to secure a warrant based upon probable cause to effect a search or seizure in "the ordinary case," the Court has consistently interpreted the Fourth Amendment as allowing warrantless searches on less than probable cause in a wide array of circumstances "[w]hen faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like." \textit{Ill. v. McArthur}, 121 S. Ct. 946, 949 (2001).

\textsuperscript{75} \textit{Smith}, 155 F.3d at 1058. Recall that the unauthorized acquisition of stored voicemail message is "interception" under \textit{Wiretap Act}. \textit{Id.}
The Wiretap Act provides generally for a maximum penalty of a fine and up to five years of incarceration for violations.\(^7\) The Stored Communications Act, on the other hand, provides generally for a maximum penalty of a fine and up to one year of incarceration for a first offense and two years for subsequent offenses.\(^6\) Thus, if an acquisition is deemed illegal under the Stored Communications Act, a defendant may be subject to less severe sanctions than if the communications were deemed to have been intercepted under the provisions of the Wiretap Act.

Finally, the effort to distinguish between interception and unauthorized access has specific consequences in the civil context.\(^7\) These consequences concern the statutory awards available to aggrieved plaintiffs who are able to prove that their privacy was compromised, as the Wiretap Act provides for significantly greater money awards than does the Stored Communications Act.\(^7\) For example, the Wiretap Act may allow monetary damages of $100 a day for each day of violation, up to $10,000 for certain violations.\(^8\)

In short, whether the “interception-unauthorized access” issue is resolved under the Fifth Circuit’s analysis in Steve Jackson Games or the Ninth Circuit’s analysis in Konop has serious practical implications for the way businesses and private individuals conduct themselves professionally and personally in respect to the use of electronic communication. Resolution of the “interception-unauthorized access” dilemma, moreover, has implications for the degree of privacy protection that will attach to electronic communications.

B. Privacy Implications of the “Interception-Unauthorized Access” Dilemma

In Steve Jackson Games, the Fifth Circuit held that that the statutory scheme created by the Wiretap Act and Stored Communication Act evidenced Congressional intent to provide reduced protection for stored electronic communications.\(^8\) Courts that adopt the Fifth Circuit’s rationale accordingly would rank electronic communications below oral and wire communications in the communications hierarchy, notwithstanding that unchecked interception of electronic communications may prove to

\(^7\) Konop, 236 F.3d at 1042 (discussing the differing civil damages consequences under the Wiretap Act and Stored Communication Act).
\(^8\) See 18 U.S.C. § 2520(c)(2) (2000) (establishing statutory penalties for acts violating statute other than the private viewing of a private satellite video communication that is not scrambled or encrypted, or certain radio communications that are not scrambled or encrypted).

\(^8\) See Steve Jackson Games, 36 F.3d at 461–63.
have a more deleterious effect upon genuine privacy interests than interception of more traditional communications. The question raised by the Steve Jackson Games holding may be framed thus: Does the Fifth Circuit's construction of the "Wiretap Act" comport with the ideal of privacy protection for electronic communications that Congress sought to preserve and enlarge through ECPA?

The characteristics of electronic communications make such communications ideal for enhancing private relationships and transactions while simultaneously making them more susceptible to unauthorized disclosure, thus compromising the very privacy interests they promote. As discussed in this section, these characteristics suggest that electronic communications should be afforded the maximum protection the law offers that is, at least the protection from unauthorized disclosure enjoyed by other forms of communication, like oral and wire communications and that courts should consider a number of privacy concerns when addressing ways in which the Wiretap Act and Stored Communications Act regulate the acquisition of electronic communications. Such privacy concerns, properly addressed, were inappropriately discounted in Steve Jackson Games.

1. Privacy and the Characteristics of Electronic Communications.

As noted above, privacy is essential to the conduct of human affairs.82 The condition or circumstance of privacy creates a context in which personal and commercial relationships may be forged.83 Developments in communications technology have enhanced the ability to create those personal and commercial relationships. Traditional communications technologies, like the telephone, have allowed those relationships to thrive across geographic distance; now, the reality of electronic communication has added an ability to interact across temporal distances with the ease of wire communication, through such asynchronous communicative modes as ordinary e-mail and the World Wide Web.84

Not surprisingly, electronic communication has become instrumental in promoting personal and commercial relationships, by serving as a new means through which individuals can explore and develop such relationships.85 In the realm of the personal,

[cyberspace ... facilitates relationships that originally form in cyberspace. Typically, these relationships form in virtual communities of common interests, experiences, and fates. Such communities can be

---

82. See supra n. 9 and accompanying text.
83. See supra nn. 9-11 and accompanying text.
85. See Diffie, supra n. 1, at 1 (noting that "we now conduct more and more of our communications, whether personal, business, or civic, via electronic channels").
large, and often their members have not met face-to-face. Examples include academic e-mail distribution lists, Usenet newsgroups, chat rooms, and instant messaging.\textsuperscript{86} And, in the realm of the commercial, “[t]he Internet provides rapid communication capabilities at reduced costs and [has expanded] access to a global market. Business can be conducted almost anywhere by using the Internet.”\textsuperscript{87} The future holds still greater promise for the development of relationships through the use of new and innovative electronic communicative modes; what was once the stuff of science fiction may soon be reality.\textsuperscript{88}

If individuals are to continue to pursue the kinds of relationships and transactions that electronic communication enables, they must have some assurance that their electronic communications will, at least in certain defined circumstances, remain private, just as they do with traditional communications.\textsuperscript{89} Though it addresses a communications technology that differs from more traditional technologies, like telephony, this concern for privacy is little different than that which motivated Congress to enact the Wiretap Act in the 1960s – that is, a concern to ensure, by legal means, that individuals may be able to retreat from prying eyes and ears to conduct their affairs without fear that their communications will be “intercepted by an unseen auditor and turned against the speaker to the auditor’s advantage.”\textsuperscript{90} Today, that concern includes “auditors” equipped with the technological capacity to intercept and disclose electronic communications.

The danger to privacy posed by the threat of unauthorized disclosure of electronic communications indeed may be more significant than the disclosure threat vis-à-vis traditional communications, due to the unique blending of elements present only in electronic communications like e-mail and Web-based chat or information exchanges. Typically, electronic communication combines the casual and un-thoughtful nature of live communication with the reciprocal nature of electronic communications.

\textsuperscript{86} Jerry Kang, Cyber-race, 113 Harv. L. Rev. 1130, 1150 (2000).
\textsuperscript{88} See Kang, supra n. 86, at 1151 (observing that “in the next fifteen years, multimedia exchange will grow rapidly in cyberspace,” including widespread adoption of voice and video transmission).
\textsuperscript{89} See Kurt A. Wimmer, Encryption, the Internet and Bernstein v. Dept. of Justice: The First Amendment Rescues Electronic Commerce and Internet Privacy, BLAST (newsletter of the ABA Sec. Sci. & Tech.) 5–6 (Dec. 1999) (discussing the need “to carry over to the electronic realm the privacy in our communications and transactions that we have historically enjoyed in the non-electronic realm”); see also Diffie, supra n. 1, at viii–ix (observing that “[i]f people are to enjoy the same effortless privacy in the future that they enjoyed in the past, the means to protect privacy must be built into their communications systems”).
oral and wire communications, with the storage and reproduction qualities historically associated with public records or print publications. Due to their digital composition, electronic communications can be captured in ways that analog communications, such as oral communications, cannot. Electronic communication, in other words, possess the combined qualities of those communications formats that receive the full protection of the Wiretap Act and in a form more conducive to unauthorized disclosure. The unique and differentiating characteristics of electronic communications relate primarily to the context in which they occur, the ease of their duplication, and the indicia of legitimacy.

Context. Commentators have noted various ways in which individuals use e-mail and other forms of electronic communication.91 Whereas historically an individual may have picked up a telephone and casually conversed with an acquaintance or co-worker, today the same communication likely flows through e-mail or communication via the World Wide Web.92 These communications, by their very nature, capture an individual's thought process in a far less refined way than a piece of traditional correspondence. As anyone who has ever reviewed large quantities of a stranger's e-mail knows, it often takes several iterations of communications between parties to an electronic conversation to flesh out the context necessary to determine the true meaning of a particular electronic communication. While this aspect of electronic communication conveys potentially greater content than traditional communication formats like old-fashioned pen-and-ink correspondence, it also makes such communications more likely to be misinterpreted when viewed by individuals who are neither intended recipients nor privy to the context in which the communication occurred.93

This is not to say that every particular electronic communication lacks forethought. Rather because information can be digitally compressed, it is possible for electronic communications potentially to carry a broad, almost infinite range of carefully considered content that nonetheless may be inscrutable without a proper context. From the hastily dashed-off note to the carefully considered settlement offer (with accompanying documentation), or from the twelve-year-old's movie Web site to


92. Rosen, Unwanted Gaze, supra n. 91, at 75–76.

93. Jeffrey Rosen offers this illustration: "Even if you had full access to my DoubleClick logs, containing granular details of everything that I had read or downloaded over the past year, you shouldn't, wouldn't, understand me in context." Rosen, Out of Context, supra n. 10, at 214.
the movie studio's official Web site costing thousands of dollars, communication at all levels of formality and containing all depths of information can be conducted through and across electronic media. This diversity alone is not unique, of course; traditional media support an equally diverse range of subject matters. The difference with electronic communications is simply that the relative informality and greater transmission capacity of electronic communication can enhance the risk that a third-party recipient or observer may not be able to discern the difference between the casual and the thoughtful communication.

**Duplication.** The ubiquitous and clandestine duplication and storage abilities inherent in modern electronic networked communications also differentiate electronic communications from traditional communications formats. When communication is conducted over the Internet, for example, whether it consists of Web page postings or e-mail, copies of the communications are generated in several locations in the normal course of transferring that communication. E-mail messages may be stored for considerable lengths of time on: (1) the originator's computer; (2) the mail server of the originator's Internet Service Provider; (3) the mail server of each recipient's Internet Service Provider; or (4) each recipient's computer. This list grows even longer in instances in which either the originators or recipient's mail account is part of an intranet, as is the case with most corporate networks.

Similarly, distributing or accessing information through the World Wide Web "HTML" pages creates copies of the Web pages on: (1) the publisher's computer; (2) the server that hosts the Web site; and (3) the computer of each individual who views the Web site. In all of these cases, the digital nature of the transmission makes each copy the equal of the original in terms of quality and ease of replication. Technology thus makes electronic communication such as e-mail more susceptible

---

94. See Rosen, *Unwanted Gaze*, supra n. 91, at 76 (discussing problem of context with respect to e-mail communication); see also Fried, *supra* n. 9, at 490–91 (discussing the problems created by the unauthorized monitoring of communications).


96. Id.


98. In the case of some other forms of electronic communications, such as UseNet news group postings, the number of copies on automatically updating servers (not to mention end user's computers) can run to the thousands.
than oral or wire communications to the problems associated to unauthorized disclosure and compromised privacy.

Legitimacy. Finally, the nature of electronic communication creates circumstances in which the legitimacy of electronic communications cannot readily be determined. Where electronic communications are concerned, it may be difficult to utilize the indicia of legitimacy which individuals typically use to evaluate other forms of communication, either because those indicia do not exist, or, more subtly, because they are so easily duplicated in digital formats. For example, it may be difficult for a stranger to an electronic communication to authenticate the identity of the communication's purported author; unlike a telephone call, third parties likely will be unable to rely on voice recognition to identify the author. This sort of legitimacy-confusion can lead, ultimately, to misinterpretation of the communication and the potential abuse of its contents. At the least, this aspect of electronic communication may contribute to misunderstandings and misrepresentations large and small, by and about the participants to the communication at issue.


Because of the particular characteristics of electronic communications relating to context, duplication and legitimacy, unauthorized disclosure of such communications may expose individual authors and recipients to the danger that their thought processes and statements will be construed without proper contextual guidance by those who were not privy to the entire communication stream, such as the intended recipients. Such unmediated disclosure entails the most dangerous kind of privacy violation: the potentially damaging distribution and dissemination of misinformation about the parties to the communication, their relationship, or their thought processes.

Consider the facts underlying *Konop v. Hawaiian Airlines*. In that case, an individual, the plaintiff, established and maintained a page on the World Wide Web containing a great deal of information about his employer and the conditions of employment which was intended to be shared only with certain other, authorized individuals. This electronic communication possessed the features that differentiate such communication from traditional communication formats. It represented the views and thoughts of its author in a such a way that context and legiti-

---

99. See Introna, *supra* n. 9, at 197 (noting that in cyberspace, "all the normal social cues such as physical setting, dress, titles, body language, and so on are missing").
100. See Rosen, *Unwanted Gaze, supra* n. 91, at 8.
101. 236 F.3d 1035.
102. *Id.* at 1041.
macy would have been uncertain to a stranger viewing the communication. Any determination of the weight to be given certain parts of the communication, or of the legitimacy of certain parts, may have been equally difficult for a third-party visitor to the plaintiff's Web site. Further, the plaintiff's Web page, as it existed in electronic form, was subject to unauthorized duplication in a variety of ways, such as forwarding via e-mail or hard-copy printing.1

Notably, the plaintiff in Konop created his Web page in furtherance of relationships he sought to establish with those persons he deemed to be authorized recipients; he did not intend for the information in the communication to be disclosed to third parties or strangers.104 And that communication likely would not have been accessible to third parties or strangers had it been transmitted via a traditional communication format, say, by a voice mail message.106 Yet, on the Steve Jackson Games understanding of the Wiretap Act, which effectively limits its reach to those microseconds in which an electronic communication is in pre-storage transmission,106 this communication and its author's subsequent revisions, would not receive the same protection as a wire communication containing far less information than the plaintiff's Web page conveyed to his intended recipients.

The factual circumstances in Konop illustrate how adoption of the Steve Jackson Games construction of the Wiretap Act could lead more readily to the acquisition and disclosure of private electronic communications than to the acquisition and disclosure of comparably or even less substantive private wire or oral communications, and, therefore, to precisely the sort of misunderstandings, misinterpretations and information-confusion that would tend to undermine the use of electronic communications to build personal and commercial relationships. As discussed above, the ability to control how one may be perceived and understood by individuals outside the relationships into which one enters is a central benefit of privacy.107 In respect to electronic communications, this ability is compromised by a regulatory regime, as judicially construed, that fails to consider the relevance of such communications to the conduct of human relationships, the contextual issues raised by such communications, the potentially greater content contained in such communications and, not least, the fact that electronic communications necessarily exist in a retrievable form through digital storage, in ways that traditional communication formats do not.

103. Id. at 1046.
104. See id.
105. See supra nn. 96–99 and accompanying text.
106. See Steve Jackson Games, 36 F.3d at 461.
107. See Rosen, Unwanted Gaze, supra n. 91, at 75–76; Fried, supra n. 9, at 482.
A legal basis to challenge the unauthorized disclosure of information is essential to the maintenance of effective privacy protections. In resolving the “interception-unauthorized access” dilemma to avoid diminishing the statutory privacy protection for electronic communications, the Ninth Circuit’s opinion in Konop, in contrast to the Fifth Circuit opinion Steve Jackson Games, reflects an appreciation for the particular characteristics of such communications and their privacy implications. Recognizing that stored electronic communications, like their traditional wire and oral counterparts, can be intercepted within the meaning of the Wiretap Act, Konop supports a legal regime that treats old and new communication formats consistently. Indeed, as the court observed, it makes no sense to protect an individual’s messages from interception “had he recorded them and delivered them through a secure voice bulletin board accessible by telephone, but not when he set them down in electronic text and delivered them through a secure Web server accessible by a personal computer.” By affording electronic communications equivalent protection under the Wiretap Act, the privacy in the underlying relationships those communications represent is naturally enhanced.

It follows that, given the characteristics of electronic communications and the risks and problems that may flow from their unauthorized disclosure, as well as the intent of Congress as reflected in the structure of the Wiretap Act and Stored Communications Act, the Konop court has the better of the argument regarding the interplay between “interception” and “unauthorized access” under the Wiretap Act and Stored Communications Act. By acknowledging that electronic communications should be afforded at least the same level of privacy protection as oral and wire communications, the Ninth Circuit’s reading of the Wiretap Act

108. See id. at 493. “In most developed societies the only way to give a person the full measure of both the sense and the fact of control is to give him a legal title to control.” Id. See also Nesson, supra n. 1, at 111–12 (arguing that privacy must be protected through legislation).
109. 236 F.3d at 1046.
110. Id.
111. As a matter of mechanical statutory construction, moreover, the Ninth Circuit came closer to the mark in Konop, to the extent the court recognized that the statutory definition of “intercept” contains no temporal acquisition requirement, and that the provisions of the Stored Communications Act only apply to the acquisition of electronic communications stored by electronic communications services providers. Indeed, the Stored Communications Act says nothing whatsoever about the acquisition of stored electronic communications that reside in systems other than those operated by such providers. Id.; see 18 U.S.C. § 2701(a)(1) (2000) (addressing unauthorized access to “a facility through which an electronic communication service is provided”); 18 U.S.C. § 2702 (2000) (limiting disclosure by “a person or entity providing electronic communication service to the public”); 18 U.S.C. § 2703 (2000) (regulating government-mandated “disclosure by a provider of electronic communications services of the contents of an electronic communication”).
and Stored Communications Act serves to promote the importance of privacy considerations in respect to all communication formats.\textsuperscript{112} If widely adopted, the Konop court's construction of the law could provide modest comfort to the growing number of individuals who rely upon electronic communication for personal and commercial purposes and who seek some assurance that their communications, even when digitally stored somewhere deep within the Internet, generally will be regarded as protected from prying eyes and ears.\textsuperscript{113}

V. CONCLUSION

Questions regarding the nature of privacy protections for electronic communications will continue to arise from within and without the legal community as more individuals and businesses turn to electronic communication as a means to connect with their respective families, friends, neighbors, colleagues and customers. An examination of the decisions in Steve Jackson Games and Konop, in which two courts of appeals differed in their understanding of the same statutory scheme, provides some perspective on the considerations to be borne in mind when determining how ECPA should be understood and construed, and the extent to which courts should look to privacy as a guidepost in attempting to make sense of a statutory scheme "famous (if not infamous) for its lack of clarity."\textsuperscript{114} The significant privacy concerns associated with the particular characteristics of electronic communications should at a minimum inform judicial consideration of issues surrounding eavesdropping in the digital age as well as future debates about the importance of legal protection for the privacy of electronic communications.

\textsuperscript{112} Konop, 236 F.3d at 1046 (reasoning that "[i]t makes no more sense that a private message expressed in a digitized voice recording stored in a voice mailbox should be protected from interception, but the same words expressed in an e-mail stored in an electronic post office pending delivery should not").

\textsuperscript{113} Of course, issues remain with the statutory scheme itself. For example, while ECPA arguably protects the privacy of electronic communications to the same extent as wire and oral communications, the suppression of electronic communications wrongfully seized by the government is not statutorily mandated, as with wire and oral communications. See 18 U.S.C. § 2518(10) (2000). Thus, so far as government interception in criminal matters is concerned, electronic communications are, in this sense, still regarded as inferior to wire and oral communications as a matter of law.

\textsuperscript{114} Steve Jackson Games, 36 F.3d at 462.