NOTES

PRIVACY IN THE INFORMATION AGE: THE NEED FOR CLARITY IN THE ECPA

I. INTRODUCTION

"Private—Keep Out." "Private and Confidential." "Do Not Disturb." Privacy pervades American society, and Americans cherish their privacy rights. The Fourth Amendment of the United States Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects . . .."[1] Numerous other privacy laws have followed the Constitution's lead,[2] and invasion of privacy has long been an established tort action.[3] Given the substantial legacy of privacy rights and the dramatic technological advances during the past few decades, it is no surprise that Congress enacted the Electronic Communications Privacy Act of 1986[4] ("ECPA") to extend privacy law into the electronic communications area.

The ECPA is an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("1968 Act"),[5] which protected wire and oral communications from privacy breaches. The ECPA expanded legal privacy protection to include electronic communications. The ECPA is divided into three titles, each addressing a slightly different area. Title I addresses the interception and disclosure of different types of communications.[6] Title II deals with access to stored electronic communications.[7] Title III regulates the use of pen registers and trap and trace devices, which are used to record the

1. U.S. CONST. amend. IV.

2. *See, e.g.*, Privacy Protection Act, 42 U.S.C. § 2000aa *et seq.* (1996) (outlining First Amendment privacy protection with limits on searches and seizures by government officers and employees in criminal investigations, and giving civil right of action to aggrieved persons); Buckley Amendment, 20 U.S.C. § 1232g (1994) (protecting rights of students and parents to inspect educational records and prohibiting funds for educational institutions that release education records without written consent from the student or parents); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (1993) (insuring consumer reporting agencies respect consumers' rights to privacy by limiting the information they can disclose and by requiring agencies to get permission from consumers before disclosure).

3. *See* RESTATEMENT (SECOND) OF TORTS § 652 (1977).

4. 18 U.S.C. §§ 2510 - 3127 (1994).

5. Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of 18 and 42 U.S.C.).

6. *See* 18 U.S.C. § 2511 (1994).

7. *See* 18 U.S.C. §§ 2701 - 2707 (1994).

telephone numbers dialed from and into a specific telephone line.[8] This Note addesses only Titles I and II. Title III is beyond the scope of this Note.

Title I prohibits the intentional interception of wire, oral or electronic communications, and the use or disclosure of such communications with the knowledge that they were obtained through unlawful interception.[9] The term "intercept" is defined in Title I as the acquisition of the contents of any such communication through the use of a device.[10] Title I is often called the Wiretap Act. Exceptions to the prohibitions in Title I include communication service providers who are acting in a capacity necessary to provide the service, or who are responding to a court order. Consent of one of the parties to the communication and the acquisition of foreign intelligence information by the United States Government are also exceptions.[11]

Title II, the Stored Communications Act, is focused more narrowly, dealing exclusively with electronic communications. Title II forbids intentional, unauthorized access to and disclosure of stored electronic communications,[12] and gives specific requirements for government access to stored electronic communications.[13] An exception to the Title II prohibition of unlawful access to stored electronic communications exists for communication service providers.[14] In addition, several exceptions to the prohibition of disclosure are enumerated. These include disclosure to an addressee or intended recipient, disclosure with the consent of one of the parties, and disclosure to a law enforcement agency if the contents were inadvertently obtained and appear to pertain to the commission of a crime.[15]

While the ECPA represented significant progress for privacy generally when it was passed in 1986, technology has continued to outpace the law. The ECPA was required to update the 1968 Act in order to preserve privacy rights in light of advances in technology. Similarly, the ECPA has been made less relevant and less effective due to subsequent advances in technology

---

8. *See* 18 U.S.C. §§ 3121 - 3127 (1994).

9. *See* 18 U.S.C. § 2511 (1994); *see also infra* note 47 for the text of this statute.

10. *See* 18 U.S.C. § 2510(4) (1994); *see also infra* note 61 for the ECPA's definition of "intercept."

11. *See* 18 U.S.C. § 2511(2) (1994); *see also infra* note 25 for the text of the provision.

12. *See* 18 U.S.C. §§ 2701, 2702 (1994); *see also infra* notes 49 and 82 for the relevant text of the statutes.

13. 18 U.S.C. § 2703(a) states as follows:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic 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 . . . .

18 U.S.C. § 2703(a) (1994).

14. *See* 18 U.S.C. § 2701(c)(1) (1994); *see also infra* note 49 for the text of the statute.

15. *See* 18 U.S.C. § 2702(b) (1994); *see also infra* note 82 for the text of the statute.

which have occurred even more rapidly then between the passage of the 1968 Act and the ECPA.[16] Laws concerning privacy must be clear, easily applicable, and up-to-date so as to safeguard this valuable right. Because the ECPA has proven itself to be unclear and confusing, especially in light of advances in technology, it needs to be amended to promote privacy in an increasingly technological world.

One major problem courts have faced with the ECPA is that it contains no guidelines for determining whether Title I or Title II applies in a given situation, though the two titles provide different standards and different punishments.[17] Title I's "interception" and Title II's "access" may appear easily distinguishable at first glance,[18] but in today's technological realm things are seldom so clear. For example, when an individual reads an e-mail message intended for another who has not yet read it, but who has left the message open on a computer screen, has the individual *intercepted* the electronic communication or *accessed* it in electronic storage?[19] If this preliminary determination cannot be made, judges must either choose randomly between the ECPA provisions or look elsewhere to determine liability.

Another problem with the ECPA is its narrow prohibition on disclosure of stored electronic communications.[20] While virtually all unauthorized access to electronic communications is unlawful,[21] service providers are the only parties prohibited from actually disclosing the contents of stored communications.[22] For example, the online service provider America Online cannot publish your e-mail stored within its system, but a person whom you have authorized to use your account could publish your private e-mail without violating the ECPA.[23] Private, stored electronic communications

16. The most revolutionary technological change since the original ECPA was passed in 1986 is without doubt the advent of the Internet, a global, publicly accessible computer network. Subsequent mainstream acceptance and adoption of Internet technologies have had a profound influence on the United States economy, journalism, the government, and people's everyday lives. For example, electronic mail (e-mail) has become a fundamental element of personal and business communications in this country, and e-mail clearly falls within the purview of the ECPA. The increasing popularity of e-commerce, consumer purchasing via credit cards on the World Wide Web (WWW), is a monumental privacy issue. For a more detailed explanation of the development of the Internet, see *infra* note 115.

17. *Compare* 18 U.S.C. § 2511(1) (1994) *and* 18 U.S.C. § 2511(4) (1994) *with* 18 U.S.C. § 2701 (1994); *see also infra* notes 47 and 49 for the text of the statutes.

18. *See infra* notes 47 and 49 for the text of the relevant ECPA provisions.

19. This question is at the core of *Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997). *See infra* notes 88, 89, 91 and accompanying text for further explanation of this case.

20. *See* 18 U.S.C. § 2702 (1994); *see also infra* note 82 for the text of the statute.

21. *See* 18 U.S.C. § 2701(a) (1994); *see also infra* note 49 for the text of the statute.

22. *See* 18 U.S.C. § 2702(a) (1994); *see also infra* note 82 for the text of the statute.

23. This person would not have violated Title I, because he or she did not intercept the e-mail while it was in transmission as "intercept" is defined in Title I. *See infra* notes 47 and 61 for the

deserve stronger protection from unwarranted disclosure.

A third problem area in the complex ECPA is the lax standards for accessing stored communications that apply to electronic communication service providers.[24] Specifically, service provider employees can freely rummage through subscribers' communications, especially if they claim it is necessary to maintain the system.[25] While legitimate business or system concerns may warrant service provider access upon occasion, the privacy of electronic communications need not be compromised.

The lack of statutory guidelines as to whether Title I or Title II should apply, the law's narrow protection for stored electronic communications, and the law's leniency on service provider access to stored communications comprise the three areas of the ECPA most in need of change. Student[26] and attorney commentators,[27] as well as the courts,[28] all point to the need for

---

relevant Title I provision and the statutory definition of "intercept," respectively. There is no Title II violation because the person had authorization to access the account. *See infra* note 49 for the relevant Title II provision. Also, the disclosure of the e-mail contents by the person is not prohibited by the ECPA, since he or she is not providing the electronic communication service to the public. *See infra* note 82 for another relevant Title II provision.

24. *See* 18 U.S.C. § 2701(c) (1994); *see also infra* note 49 for the text of the statute.

25. *See* 18 U.S.C. § 2701(c) (1994), quoted in *infra* note 49; *see also* 18 U.S.C. § 2511(2), which states:

> (2)(a)(I) It shall not be unlawful under this chapter for an operator of a switchboard, or on [sic] officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

18 U.S.C. § 2511(2)(a)(I) (1994).

26. *See* Michelle Skatoff-Gee, *Comment, Changing Technologies and the Expectation of Privacy: A Modern Dilemma*, 28 LOY. U. CHI. L.J. 189 (Fall 1996). Student commentator Michelle Skatoff-Gee agrees that better privacy protection for changing technology is needed. Specifically, she observes that new technologies make it hard to determine whether or not a reasonable expectation of privacy exists. *See id.* at 202. Skatoff-Gee even goes so far as to say that Title I of the ECPA codifies Fourth Amendment principles, a fact that further supports the need for the privacy law to change with technology. *See id*. *See also* Robert S. Steere, *Keeping "Private E-Mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U.L. REV. 231 (Fall 1998) (proposing that Congress amend the statutory definitions of "electronic communication," "wire communication," "electronic storage," and "electronic communication system" to relieve the confusion surrounding these terms in the ECPA).

27. *See* Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1, 2 (1998). Katrin Schatz Byford recently noted that there is a great need for uniformity in legal privacy theory and privacy law, especially in the electronic communications area. Byford opines that privacy legislation must go beyond the "piecemeal attempts that have traditionally been made to prevent specific privacy intrusions in narrowly delimited areas." *Id.* at 57. Byford also observed that because the ECPA contains an exception for interceptions and disclosures for which the consent of at least one of the

clarification in the ECPA. While much clarification is needed, the task is not insurmountable. A few simple additions to the text of the ECPA would remove much of the confusion that presently surrounds its interpretation.[29]

This Note first examines the legislative history of the ECPA and interpretations of the ECPA by various courts in various jurisdictions. Next, this Note analyzes the legislative history and court decisions and discusses the strong points and shortcomings that emerge therefrom. Finally, this Note offers a solution to the convoluted ECPA in the form of several specific amendments.

---

parties has been given, it is not a strong enough protection against informational privacy violations in contemporary networked environments. *See id*. at 58.

28. *See, e.g.* Davis v. Gracey, 111 F.3d 1472, 1484 (10th Cir. 1997) (admitting confusion as to exactly how the ECPA applies to law enforcement officers); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (commenting on the ECPA's "lack of clarity"); United States v. Moriarty, 962 F. Supp. 217, 219 (D. Mass. 1997) (pointing out the lack of a definition for "access" in either Title I or II of the ECPA).

29. *See infra* notes 146, 149, 151, 154, 159, and accompanying text for proposals to amend and clarify the language of the ECPA. In the years since the ECPA was enacted, several amendments to the ECPA have been proposed and passed as new technology has emerged. The Telephone Privacy Act of 1990 was proposed to clarify the legal status of Caller ID services. *See* H.R. 4340, 101st Cong. (1990). The Motion Picture Anti-Piracy Act was proposed to amend the ECPA to prohibit devices whose primary purpose was to deactivate copy protection technology. *See* S. 1086, 102nd Cong. (1991). Neither of these proposed bills was passed.

The Communications Assistance for Law Enforcement Act of 1994 broadened government agency access to telephone subscriber information. *See* 47 U.S.C. § 1001 *et seq.* (1998). The law amended § 2709 of the ECPA to ensure that advancing technology would not encroach on government surveillance. Specifically, the amendment requires an electronic communications service provider to give the Federal Bureau of Investigation access to identification information of subscribers without a court order or subpoena, when the information is allegedly related to a foreign counterintelligence investigation. *See* 18 U.S.C. § 2709(b) (1994).

One of the more recently proposed amendments to the ECPA is the Children's Online Privacy Protection Act of 1998. *See* S. 2326, 105th Cong. (1998). This act would require the Federal Trade Commission to promulgate rules governing children's World Wide Web sites. The rules would require commercial web sites to get parental consent before requesting personal information from children under the age of 12, and to ensure the confidentiality of any personal information gathered from children. This act is currently under consideration by the Senate Committee on Commerce.

In 1999, several bills to amend various sections of the ECPA were introduced. One bill would amend Title III of the ECPA to allow for the use of clone pagers by law enforcement officials. *See* S. 411, 106th Cong. (1999). Another bill, known as the Telephone Privacy Act of 1999, would allow interception of telephone communications only after the consent of all parties. *See* S. 781, 106th Cong. (1999). The Patients' Telephone Privacy Act of 1999 would require the consent of patients before health insurance companies or physicians could intercept the patients' wire, oral, or electronic communications. *See* S. 782, 106th Cong. (1999). Finally, the Electronic Rights for the 21st Century Act would increase law enforcement access to information concerning the location of computers, and would enhance privacy protection for information on computer networks and on the Internet. *See* S. 854, 106th Cong. (1999).

II. THE ECPA IN LEGISLATIVE HISTORY AND CASE LAW

A. Legislative History

According to legislative history, the purpose of the ECPA was to update the Omnibus Crime Control and Safe Streets Act of 1968[30] to ensure continued privacy protection in the presence of new computer and telecommunications technologies.[31] The legislature's emphasis on privacy in the passage of the ECPA is evident by the inclusion within the Senate Judiciary Committee's Report of Justice Brandeis' powerful dissent in *Olmstead v. United States*[32]. In this dissent, Brandeis vehemently defended privacy and opined that government wiretapping violates the Fourth Amendment.[33] By enacting the ECPA, Congress attempted to strike a balance between privacy interests in personal and proprietary information on the one hand and legitimate law enforcement interests on the other.[34]

In addition to privacy issues, Congress was concerned with updating the law to address the significant changes in communication technology that occurred in the 1970s and 1980s, including electronic mail, or e-mail.[35] The Senate Committee that examined the ECPA wanted to preserve privacy for electronic communications that are subject to control by third party computer operators.[36] Because the information in those communications has virtually no constitutional privacy protection,[37] Congress expressly provided privacy

---

30. Congress stated that the purpose of the 1968 Act was to balance individual privacy interests and law enforcement investigative interests. *See* S. REP. NO. 90-1097, at 87 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112. The 1968 Act prohibits all wiretapping and electronic surveillance by persons other than law enforcement officers investigating certain types of crimes pursuant to a court order, with exceptions for several groups. *See* 18 U.S.C. § 2511 (1970). Congress also said that the 1968 Act was a response to the Supreme Court decisions of *Berger v. New York*, 388 U.S. 41 (1967) (holding that the Fourth Amendment applies to government interception of a telephone conversation), and *Katz v. United States*, 389 U.S. 347 (1967) (extending Fourth Amendment protection to electronic eavesdropping upon oral conversations). *See* S. REP. NO. 90-1097, at 105-108 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112.

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

32. 277 U.S. 438 (1928).

33. *See id.* at 485.

34. This scheme is easily discerned in the structure of the statutes themselves. For example, in Title II, §§ 2701 and 2702 protect privacy concerns of citizens, whereas § 2703 describes the parameters for government and law enforcement access to electronic communications. *See* 18 U.S.C. §§ 2701, 2702, 2703 (1994), quoted in *infra* notes 49, 82 and *supra* note 13, respectively.

35. The Senate Report which recommended passage of the ECPA cited electronic mail, computer-to-computer data transmissions, cellular telephones, cordless telephones, paging devices, and video teleconferencing as some of the technological advances the ECPA was designed to reach. *See* S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

36. *See* S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

37. The Senate Committee cited *United States v. Miller*, 425 U.S. 435, n.3 (1976) (concluding that a bank customer has no standing to contest disclosure of his or her bank records).

protection for those communications in the statutes of the ECPA.[38]

Congress seemed particularly concerned that the law had not kept pace with technology in the communications area. Indeed, Senator Leahy of Vermont stated in his introduction of the bill that the existing law as set forth in the 1968 Act was "hopelessly out of date."[39] Some of the changes to the 1968 Act that Congress enacted were relatively minor,[40] while others were quite drastic.[41] In essence, Congress hoped to update the law and accomplish vast improvements in electronic communication law with the ECPA.

B. Case Law: Should ECPA Title I or Title II apply?

Since the passage of the ECPA in 1986, several courts have considered the necessary choice of whether to apply either Title I or Title II, discussing the "interception" of transmitted communications in Title I as opposed to the "accessing" of stored communications in Title II.[42] *Steve Jackson Games, Inc. v. United States Secret Service*[43] is the most prevalently cited case that examines this issue. In *Steve Jackson Games*, the Secret Service seized a computer from the plaintiff's premises in the course of an investigation.[44] The seized computer housed an electronic bulletin board system[45] that

---

38. *See* S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555; *see also* Title II of the ECPA, 18 U.S.C. § 2701 *et seq*. (1994).

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

40. For example, the ECPA changed the state of mind requirement from "willful" to "intentional." *See id*. at 5. Also, Congress redefined "intercept" to make it clear that it is illegal to intercept the non-voice portion of a wire communication. *See id*. at 12.

41. The best examples of drastic changes are the Title II statutes on unlawful access to stored communications; they are original to the ECPA, and are modeled on the Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq*. *See id*. at 3. Congress also responded to industry interest groups by implementing changes in satellite provisions and cellular phone provisions. *See id*. at 5. The definition of "contents" was amended to exclude information about the identity of parties or the existence of the communication. *See id*. at 12. Finally, Congress added a new government action for injunctive relief that is separate from the criminal penalties specified in the ECPA. *See id*. at 19.

42. *See infra* notes 47 and 49 and accompanying text for the text of the ECPA statutes and for further details on the law.

43. 36 F.3d 457 (5th Cir. 1994).

44. *See id*. at 458. Steve Jackson Games, Inc. produces books, magazines and role-playing games. The company established a bulletin board system (BBS) in the mid-1980s to post information about its games, to encourage interest in the role-playing hobby, and to communicate with customers via e-mail. One of Steve Jackson Games' employees, Loyd Blankenship, operated another BBS which provided access to a computerized text file containing confidential information about the Bell telephone system's emergency calling system. The Secret Service's search and seizure was aimed at recovering this confidential information, and because Blankenship was a co-systems operator of the Steve Jackson Games BBS, that equipment was seized as well. It was the latter seizure that resulted in this lawsuit. *See id*.

45. *See id*. Bulletin board systems (BBS) are computers typically run by individuals in their homes that allow dial-up access to users. A BBS is similar to an online service like America Online, but on a much smaller, often localized scale. A BBS allows users to send and receive e-mail amongst

allowed plaintiff's customers to access private e-mail. At the time of seizure, the computer contained stored e-mail messages that intended recipients had not yet retrieved from the system.[46] Thus, the issue before the Fifth Circuit was whether the actions of the Secret Service constituted an "intercept[ion]" under Title I of the ECPA.[47]

The court held that there was no violation of Title I because the Secret Service agents did not seize the messages while they were being transmitted.[48] However, the court held that the Secret Service violated Title II

---

themselves, and sometimes with other BBS's and their users. The posting of public messages in discussion groups or forums is also a typical service of a BBS, as are file downloads and online games. BBS's were popular among personal computer users in the 1980s and early 1990s before general access to the Internet became common. Their popularity has not died out completely, as is evidenced by the facts in *Steve Jackson Games* and Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997). *See infra* notes 73-74 and accompanying text for an account of the use of a BBS by the parties in *Davis*.

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

47. *See id.* Title I's section 2511 is entitled, "Interception and disclosure of wire, oral, or electronic communications prohibited." It states:

> [A]ny person who --
>
> intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when --
>
> such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in a wire communication . . .
>
> intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing . . . the information was obtained . . . in violation of this subsection . . .
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511(1) (1994).

48. *See Steve Jackson Games*, 36 F.3d at 461. There has been much criticism of this decision, particularly from privacy advocates. They argue that the court interpreted the language of the ECPA, especially the term, "intercept," much too narrowly. *See* 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 (1999) (interpreting the ECPA term "electronic communication" to include "electronic storage," thereby contradicting the Fifth Circuit's analysis by claiming that stored electronic communications can be intercepted within the meaning of Title I); A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and The Constitution*, 143 U. Pa. L. Rev. 709, 897 (1995) (declaring the Fifth Circuit's narrow interpretation of the ECPA a "stunted view"); Nicole Giallonardo, *Steve Jackson Games v. United States Secret Service: The Government's Unauthorized Seizure of Private E-Mail Warrants More Than the Fifth Circuit's Slap on the Wrist*, 14 J. Marshall J. Computer & Info. L. 179, 203-04 (1995) (concluding that the Fifth Circuit should have followed the plain meaning of "intercept," which is broader than the statutory definition); Jarrod J. White, *Commentary: E-Mail @ Work.Com: Employer Monitoring of Employee E-Mail*, 48 Ala. L. Rev. 1079, 1083 (1997) (claiming that the Fifth Circuit's narrow decision means that it is virtually impossible to intercept e-mail within the meaning of the ECPA).

because the seizure was unauthorized "access" that prevented authorized "access."[49] The court reasoned that because Congress used the word "transfer" in its definition of "electronic communication," and because it omitted any reference to electronic storage in that definition,[50] there was no intent for "intercept" to apply to electronic communications in storage.[51] This definition of electronic communication is in contrast to the statutory definition of "wire communication,"[52] which encompasses stored wire communications, and to which "intercept" clearly applies.

The court also observed that Congress apparently did not intend to require that a Title II violation be linked to a Title I violation.[53] This observation is supported by the fact that substantive and procedural requirements for the

---

49. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 458, 462 (5th Cir. 1994). The relevant Title II provision, § 2701, is as follows:

> Except as provided in subsection (c) of this section whoever --
> intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> 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 punished as provided in subsection (b) of this section . . .
> Subsection (a) of this section does not apply with respect to conduct authorized --
> by the person or entity providing a wire or electronic communications service;
> by a user of that service with respect to a communication of or intended for that user; or
> in section 2703, 2704 or 2518 of this title.

18 U.S.C. § 2701 (1994).

50. The ECPA definition states:

> "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--
> any wire or oral communication;
> any communication made through a tone-only paging device;
> any communication from a tracking device (as defined in section 3117 of this title); or
> electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2510(12) (1994).

51. *See Steve Jackson Games*, 36 F.3d at 461-62; *see also infra* note 61 for the statutory definition of "intercept."

52. The definition of "wire communication" is "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) (1994).

53. *See Steve Jackson Games*, 36 F.3d at 463. The determination that Titles I and II of the ECPA are essentially mutually exclusive is a central theme in ECPA jurisprudence. Many courts continue to look to the reasoning by the Fifth Circuit in this case to make similar determinations. *See generally* Davis v. Gracey, 111 F. 3d 1472 (10th Cir. 1997); Wesley v. Pitts, 974 F. Supp. 375 (D. Del. 1997), United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996). For details on each court's reliance on Steve Jackson Games, see *infra* notes 76, 91, and 55 and accompanying text.

government to intercept are much more stringent than the requirements for government access to stored communications.[54] Also, other requirements for government interception, such as minimization, duration, and types of crimes available for investigation do not exist with respect to government access to electronic storage.[55] The Fifth Circuit laid the groundwork for ECPA interpretation in *Steve Jackson Games*, particularly with respect to the mutually exclusive nature of Titles I and II.

The Ninth Circuit has also recently faced the dilemma of whether to apply ECPA Title I, Title II, or both, but in the voicemail rather than e-mail context. In *United States v. Smith*,[56] an employee accessed a co-worker's voicemail box, then listened to and recorded one of the co-worker's stored messages that implicated several employees in an insider trading deal.[57] The court held that the act of obtaining and recording the voicemail message was an "intercept[ion]" and was governed by Title I of the ECPA, not Title II.[58] The message here was a "wire communication" because it was an "aural transfer" made using a wire (the telephone line), and was then in "electronic

54. *See Steve Jackson Games*, 36 F.3d at 463. The difference is essentially that government officials must only obtain a warrant to access stored electronic communications under Title II, but they must obtain a *court order* to intercept electronic communications under Title I. *See* 18 U.S.C. §§ 2703(a), 2518.

55. *See Steve Jackson Games*, 36 F.3d at 463. Government access to electronic storage was at issue in *United States v. Reyes*, 922 F. Supp. 818 (S.D.N.Y. 1996), in conjunction with constitutional issues. Federal agents from the Bureau of Alcohol, Tobacco and Firearms seized three different pagers from the defendant. *See id.* Because the agents violated the Fourth Amendment when they seized the third pager using a warrant without probable cause, the court held that the seizure violated the ECPA. *See id.* at 837. In determining the ECPA violation, the court first examined whether the agents' conduct violated Title I by intercepting electronic communications or whether it violated Title II by accessing stored communications. *See id.* at 836.

While struggling to define "interception" and "electronic storage," the court cited statutory definitions and observed that electronic communications do not include those in electronic storage. *See id.* The court concluded that "intercept" means "acquiring the transfer of data," and the requirement that the acquisition be simultaneous with the original transmission is implied. *See id.* Drawing on *Steve Jackson Games*, the court said that retrieving numbers from the memory of a pager is more like accessing electronic communications in storage than intercepting them. *See id.* at 836-37. Therefore, Title II applied in this case.

56. 155 F.3d 1051 (9th Cir. 1998).

57. *See id.* at 1054. In this case, two fundamental government policies seem to clash. On the one hand, the government clearly has an interest in preventing and punishing insider trading deals, but on the other hand, the most compelling evidence in this case was obtained in such a way as to violate the ECPA. The Ninth Circuit avoided a contradiction in the law by holding that the district court correctly suppressed the tape of the voicemail message itself, but not the other government evidence, because the other evidence was not derived directly from the illegal recording. *See id.* at 1063.

58. *See id.* at 1059. The issue of whether Title I or Title II controls was of particular significance in this case, because the exclusion of evidence was at stake. Title I (Wiretap Act) excludes evidence of any intercepted communication, *see* 18 U.S.C. § 2515, whereas Title II (Stored Communications Act) does not allow exclusion of evidence as a remedy, *see* 18 U.S.C. § 2708.

storage" on the company voicemail system.[59]

The Ninth Circuit strayed far from traditional ECPA analysis in an attempt to harmonize Titles I and II of the ECPA by claiming that "intercept" and "access" are not temporally different and that "access" is a lesser-included offense of "intercept."[60] As support for its interpretation of the law, the court cited the statutory definition of "intercept," which uses the term "acquisition,"[61] and the fact that the ordinary meaning of "access" is adhered to in the ECPA.[62] The court next pointed to the different penalty schemes for Titles I and II of the ECPA,[63] and the absence of an exclusion of evidence remedy in Title II as support for its interpretation.[64] *Smith*'s lesser-included offense interpretation is unique in ECPA jurisprudence.

The view that Titles I and II of the ECPA are mutually exclusive is by far the prevailing sentiment, as evidenced recently in another voicemail decision. The defendant in *United States v. Moriarty*[65] obtained and listened to voicemail messages intended for others.[66] The court held that ECPA Title II § 2701 governs once electronic messages are stored, so the defendant only faced allegations of violating Title II, not Title I as well.[67] After a brief examination of the history of the ECPA and its interpretations, the court concluded that the amended definition of "intercept" in § 2510(4) requires contemporaneous acquisition of the communication, but "access" could apply to both contemporaneous and stored communications.[68]

The court also noted that legislative intent indicates a temporal difference between § 2511 and § 2701; only Title II § 2701 applies once electronic

---

59. *See Smith*, 155 F.3d at 1055. The ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication."
18 U.S.C. § 2510(17)(1994).

60. *See Smith*, 155 F.3d at 1058.

61. The ECPA definition is as follows: "'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1994).

62. *See* United States v. Smith, 155 F.3d 1051, 1058 (9th Cir. 1998).

63. Title I has harsher penalties than Title II. *See* 18 U.S.C. §§ 2701(b), 2707, 2511, 2520 (1994).

64. *See Smith*, 155 F.3d at 1059.

65. 962 F. Supp. 217 (D. Mass. 1997).

66. *See id.* at 219.

67. *See id.* at 221. This case was decided by a United States Magistrate Judge upon a motion by the defendant to dismiss Count II of the indictment and consolidate it with Count III. Count II alleged illegal wiretapping in violation of 18 U.S.C. § 2511(1)(a), and Count III alleged illegal access to voice mail in violation of 18 U.S.C. § 2701. The Magistrate judge granted the defendant's motion. *See id.* at 217-18.

68. *See id.* at 220. See also *infra* notes 149-151 and accompanying text for a proposed statutory definition of "access."

messages are stored.[69] In the context of this case, the court asserted that both accessing a voicemail system without listening to messages and actually listening to stored messages are aspects of "access" instead of "intercept" and are therefore subject to § 2701.[70] To solidify its position, the court noted that listening to a stored voicemail message is not an "intercept[ion]" because it does not occur while the message is in transmission.[71] The court concluded that the government was incorrect to charge the defendant under Title I § 2511 for listening to the stored messages.[72] This reasoning squarely follows the Fifth Circuit's lead in *Steve Jackson Games*.

The uncertainty surrounding interpretation of the ECPA has caused the Tenth Circuit to question when and if the law applies at all. In *Davis v. Gracey*,[73] police officers seized computer equipment that was used to run a bulletin board system from which pornographic material was accessible.[74] The court held that the officers' reliance on a valid warrant established a good faith defense to the ECPA.[75]

The court distinguished this case from *Steve Jackson Games* by pointing to the fact that agents reviewed the contents of the stored electronic communications in *Steve Jackson Games*, but here the officers did not attempt to read the stored e-mail.[76] In addition, whereas the owner of the bulletin board was not a suspect in *Steve Jackson Games*,[77] the computer equipment seized here was an instrumentality of a crime for which the owner of the bulletin board was under investigation.[78]

The court here noted some discrepancies in the ECPA, first pointing out that it is unclear whether Title II § 2701 applies to the law enforcement activities involved in this case, or if it is directed more toward "hackers."[79]

---

69. *See id*. at 221; *see also* S. REP. NO. 99-541, at 3, 32 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 (discussing the new statutes of Title II, which cover stored electronic communications, and identifying their model, the Right to Financial Privacy Act).

70. *See* United States v. Moriarty, 962 F. Supp. 217, 221 (D. Mass. 1997).

71. *See id*.

72. *See id*.

73. 111 F.3d 1472 (10th Cir. 1997).

74. *See id*. at 1475; *see also supra* note 45 for more information on bulletin board systems. After Davis's state court criminal conviction for distributing obscene materials and his civil forfeiture of the computer equipment involved, he, along with his businesses and several users, brought this action under the ECPA against the officers who executed the search. *See Davis*, 111 F.3d at 1475.

75. *See id*. at 1485. The good faith defense in Title II of the statute is as follows: "A good faith reliance on (1) a court warrant or order . . . is a complete defense to any civil or criminal action brought under this chapter or any other law." 18 U.S.C. § 2707(e)(1)(1994).

76. *See Davis*, 111 F.3d at 1483.

77. *See supra* note 44 for details on the facts of *Steve Jackson Games*.

78. *See* Davis v. Gracey, 111 F.3d 1472, 1483 (10th Cir. 1997). Mr. Davis was under investigation for distributing obscene material. *See id*. at 1475.

79. *See id*. at 1484. The court cited *State Wide Photocopy, Corp. v. Tokai Financial Services,*

The court also commented on the confusion surrounding the term "access" in the law.[80] In spite of the considerable confusion surrounding the ECPA, the court affirmed summary judgment for the defendant police officers because of their reliance on the warrant.[81]

C. Case Law: Narrow Prohibition of Disclosure of Stored Electronic Communications in ECPA § 2702

Section 2702 of Title II of the ECPA governs the disclosure of contents of stored electronic communications,[82] and its application has produced results

---

Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (commenting that "it appears that the ECPA was primarily designed to provide a cause of action against computer hackers, (i.e., electronic trespassers)."); *see also infra* note 99 and accompanying text for a discussion of this case. Both courts are likely uncertain about the application of the ECPA to law enforcement officers because of the inclusion of § 2703 and § 2704 in the ECPA. These sections outline the requirements for governmental access to electronic communications and for governmentally requested backup preservation of electronic communications. *See also supra* note 13 for the text of the ECPA provision on government disclosure of stored communications.

80. *See Davis*, 111 F.3d at 1484. The court here was unsure if "access" encompassed the physical dismantling of the computer hardware. Pursuant to a search warrant, the officers had seized Davis's bulletin board equipment, including computers, monitors, keyboards, modems, CD-ROM drives and changers. *See id*. at 1476.

81. *See id*. at 1484-85.

82. Title II's § 2702 states:

> Except as provided in subsection (b) --
>
> a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--
>
> on behalf of, and received by means of electronic transmission from . . . a subscriber or customer of such service; and
>
> solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications . . .
>
> A person or entity may divulge the contents of a communication--
>
> to an addressee or intended recipient of such communication or an agent [thereof];
>
> as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
>
> with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
>
> to a person employed or authorized or whose facilities are used to forward such communication to its destination;
>
> as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
>
> to a law enforcement agency, if such contents--
>
> were inadvertently obtained by the service provider; and
>
> appear to pertain to the commission of a crime.

potentially damaging to electronic privacy in courts around the country. The defendant in *Andersen Consulting LLP v. UOP*[83] gave the plaintiff access to its e-mail system because the plaintiff was a hired contractor. After a dispute arose between the parties, the defendant released sensitive contents of plaintiff's e-mail messages to the Wall Street Journal, which published them.[84] The district court held that the defendant was not liable under the ECPA because the defendant did not provide electronic communication service to the public.[85]

While "public" is not defined by the statute or by case law, the ordinary meaning of the word must be assumed. Therefore, the court concluded that § 2702 encompasses any entity that provides electronic communication service to the community at large.[86] The defendant here had an e-mail system for internal communication for business purposes only.[87] *Andersen Consulting* stands for the narrow concept that in order to be held liable for disclosing stored electronic communications under Title II of the ECPA, the disclosing party must be a *public* electronic communications service provider.

Recipients of contents of stored electronic communications can disclose or use the contents without liability under the ECPA, as long as they are not electronic communication service providers. In *Wesley College v. Pitts*,[88] a former clerical employee at a college inadvertently viewed the college president's e-mail messages and revealed some of them to a current faculty member and a former faculty member, who then further disclosed the messages in a lawsuit.[89] As a result, the college sued the former employees and the faculty member for violating Titles I and II of the ECPA.[90]

---

18 U.S.C. § 2702 (1994).

83. 991 F. Supp. 1041 (N.D. Ill. 1998).

84. *See id*. at 1042. In an article published on June 19, 1997, the Wall Street Journal quoted excerpts from some of Andersen Consulting's e-mail messages sent during its work at UOP. Elizabeth MacDonald, *E-Mail Trail Could Haunt Consultant in Court*, WALL ST. J., June 19, 1997, at B1. For example, the article quotes an e-mail message written by an Andersen consultant concerning the qualifications of one of his fellow consultants: "He should be taking classes at a community college, not charging for this." *Id*. It was partly this Wall Street Journal publication, along with the disclosure of the messages, that prompted Andersen Consulting to counterclaim against UOP. *See Andersen Consulting*, 991 F. Supp. at 1042.

85. *See id* at 1043. According to 18 U.S.C. § 2702(a)(1), to be liable for disclosure of electronic communications in storage, the defendant must provide "electronic communication service to the public." See 18 U.S.C. § 2702(a)(1) (1994); *see also supra* note 82 for the text of the statute.

86. *See Andersen Consulting*, 991 F. Supp. at 1042.

87. *See Andersen Consulting*, 991 F. Supp. at 1043.

88. 974 F. Supp. 375 (D. Del. 1997).

89. *See id*. at 378. The former faculty member was involved in a breach of contract suit against the college, and information concerning the president's e-mail messages was initially discovered in a deposition for the contract case. *See id.*

90. This case is unusual in that the employer is suing the employees for violation of the ECPA.

The court held that the faculty members did not violate Title II by disclosing the contents of the e-mail because the faculty members were not communication service providers.[91] The court also concluded that none of the defendants were liable for violating Title I of the ECPA; the former employee's glimpse of the computer screen did not constitute an "interception" within the meaning of the ECPA, though the act may have constituted unauthorized access.[92]

The court reasoned that Title I of the ECPA, § 2511(1)(a),[93] requires an affirmative attempt to intercept or persuade another to intercept an electronic communication.[94] Upon examining the computer expertise of the defendants and the times that the e-mail messages were sent, the court concluded that none of the defendants were liable for violating Title I of the ECPA, which concerns interception.[95] "Intercept" within the meaning of the ECPA does not apply to electronic communications in "electronic storage,"[96] and the e-

---

In many cases, employees sue their employers under the ECPA for monitoring e-mail and other communications sent over the employer's system. *See infra* note 104 and accompanying text for an example of a case illustrating that situation. In the cases where employees sue employers under the ECPA, courts around the country have repeatedly held that employees do not have a reasonable expectation of privacy in communications sent on their employer's electronic communications systems. *See* Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (holding that employee fired for negative comments in company e-mail messages had no expectation of privacy in his e-mail); Bourke v. Nissan Motor Corp., No. YC-003979, slip op. (Cal. Ct. App. June 1993) (holding no reasonable expectation of privacy for employees who were terminated for inappropriate excessive personal e-mail messages at work).

91. *See Wesley College v. Pitts*, 974 F. Supp. 375, 389 (D. Del. 1997); *see also supra* note 82 for the text of the relevant ECPA statute.

92. *See Wesley College*, 974 F. Supp. at 384; *see also supra* note 61 for the statutory definition of "intercept." The court commented, "Congress had in mind more surreptitious threats to privacy than simply looking over one's shoulder at a computer screen when it passed the ECPA." *Wesley College*, 974 F. Supp. at 384, 390.

93. The Title I prohibition on interception and disclosure begins as follows: "Except as otherwise specifically provided in this chapter any person who - (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . .."
18 U.S.C. § 2511(1)(a) (1994).

94. *See Wesley College*, 974 F. Supp. at 381. Title I, 18 U.S.C. § 2511(1)(c) & (d), also prohibits disclosure of and use of the contents of any electronic communication while having reason to know the information was obtained through an illegal interception. *See supra* note 47 for the text of the statute.

95. *See* Wesley College v. Pitts, 974 F. Supp. 375, 384, 390 (D. Del. 1997). The defendants' computer expertise and the times that the e-mails were sent were very important here because they tended to show that the defendants did not intercept any message that was in transit, which is required for liability under the statute. *See id*. at 385.

96. *See id*. at 387. The statutory definition of "electronic communication" does not include electronic storage of the communications. *See id*. at 385; *see also supra* note 50 for the statutory definition. A majority of courts that have looked at this area of the ECPA agree that there is no interception within Title I unless the acquisition of the communications is contemporaneous with their transmissions. *See Wesley College*, 974 F. Supp. at 385. The substantial differences between Titles I and II of the ECPA indicate that it was Congress's intent that "intercept" not apply to electronically

mail messages at issue in this case were in electronic storage at the time of retrieval and disclosure by the defendants.[97] Finally, the court agreed with the college's complaint about the gap in ECPA coverage. If "intercept" does not include the viewing of stored electronic communications, then a person who does not provide an electronic communication service to the public (*e.g.* the defendants here) can freely disclose or use the contents of a communication that was unlawfully obtained from storage by a third party.[98] Although disconcerting, this interpretation appears to accurately reflect the current language of the ECPA.

In addition to its gap in coverage, the ECPA may cause damage to businesses and offer no recourse when the offender is not an electronic communication service provider. The defendant in *State Wide Photocopy, Corp. v. Tokai Financial Services, Inc.*[99] gave confidential customer information to plaintiff's competitor after receiving the information through electronic communications.[100] The district court held that the defendant was not liable for a disclosure violation of Title II of the ECPA because Tokai was a private financing business, not a public electronic communications service provider, and because the plaintiff was not clearly an aggrieved party within the meaning of the ECPA.[101] The court here was not persuaded that § 2702 was intended to protect against the "mundane conduct alleged in almost any wire fraud case—namely use of the wires . . . to perpetrate a scheme to defraud."[102] The current ECPA offers no assistance to those in State Wide's position.

---

stored communications. *See id.* at 387.

97. *See id.* at 378. The messages were in storage in the president's e-mail account.

98. *See id.* at 389; for an example of how this gap in the ECPA works, see *supra* note 23 and accompanying text.

99. 909 F. Supp. 137 (S.D.N.Y. 1995).

100. *See id.* at 139. Defendant Tokai was a financing business that State Wide used to evaluate the creditworthiness of applicants who were in the process of buying or leasing office equipment from State Wide. Tokai agreed that its only use of the information faxed from State Wide would be to evaluate financing for the customers. However, State Wide discovered Tokai was supplying the confidential information to Atlantic, one of State Wide's competitors, who would then offer the customer a lower price. *See id.*

101. *See id.* at 145-46. The plaintiff did not allege that it was a provider, subscriber, or customer within the meaning of § 2707, the section outlining civil actions under the ECPA. Further, 18 U.S.C. § 2707(a) states:

> (a)[A]ny provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2707(a) (1994).

102. *See State Wide*, 909 F. Supp. at 146.

D. Case Law: Liability Exception for Service Providers in ECPA § 2701

The ECPA includes several provisions concerning electronic communications service providers, but the Title II liability exception in § 2701(c)(1)[103] is among the more controversial. This section contains a blanket exception to the prohibition of unauthorized access to stored electronic communications for service providers. The court addressed this section of the statute in *Bohach v. City of Reno*,[104] where the Reno police department retrieved stored pager messages from officers involved in an internal affairs investigation.[105] The court concluded that there was no "interception" in violation of Title I of the ECPA,[106] and because the city was the system provider, it was free to retrieve the stored messages under Title II of the ECPA.[107]

While analyzing the ECPA, the court first distinguished between interception and electronic storage in Titles I and II, respectively.[108] Next the court concluded that there was no interception by the police department, because there was no direct interference with the transmission, such as tapping computer or phone lines, recording with hidden microphones, or cloning duplicate pagers to receive the same messages as the intended recipient.[109] In dictum, the court noted that even if there was an "interception," it was likely that consent was implied[110] because the sender of

---

103. 18 U.S.C. § 2701 (c) gives exceptions to the unlawful access of stored communications provisions in subsection (a). *See supra* note 49 for the text of the statute.

104. 932 F. Supp. 1232 (D. Nev. 1996).

105. *See id*. at 1233. The pagers involved were alphanumeric pagers, which allow users to send brief alphanumeric or voice messages. The Reno Police Department installed software on its local area network computers from which users could send messages. The messages sent on the system were first stored in files on a server at the police department, then transferred to a commercial paging company, who then sent them to the recipient via radio broadcast. *See id*. at 1234.

106. *See id*. at 1237. *But see* Anne L. Lehman, Comment, *E-Mail in the Workplace: Question of Privacy, Property or Principle?*, 5 CommLaw Conspectus 99, 109 (1997) (claiming that the court's reliance on a common understanding of "intercept" is contrary to legislation that adapts to advancing technology).

107. *See Bohach*, 932 F. Supp. at 1237.

108. *See id*. at 1235-36. The court reasoned that "[a]n electronic communication may be put into electronic storage, but the storage is not itself a part of the communication." *Id.* at 1235. Therefore, the "interception" of an electronic communication (governed by Title I of ECPA) is distinguished from access to such communication after it has been put into electronic storage (governed by Title II). *See id*. at 1235-36; *see also* Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 247-48 (1994) (distinguishing between the transmission phase and the storage phase of both e-mail and voice mail messages, and concluding that § 2511 of the ECPA controls the transmission phase, while § 2701 controls the storage phase).

109. *See Bohach*, 932 F. Supp. at 1236.

110. Under Title I's consent provision, it is not unlawful for "a person acting under color of law to intercept a[n] . . . electronic communication, where . . . one of the parties to the communication has given prior consent." 18 U.S.C. § 2511(2)(c) (1994).

a message through a computer must necessarily understand and not object to the fact that the message will pass through that computer.[111]

The court went on to examine Title II of the ECPA, since the access of stored communications was obviously the source of the plaintiff's complaint. The Title II issue was quickly resolved, however, because the city was the electronic communication service provider, and § 2701(c)(1) lets service providers "do as they wish when it comes to accessing communications in electronic storage."[112] Therefore, the court ordered that the city of Reno was free to proceed with its internal affairs investigation.[113]

III. ANALYSIS

Since the passage of the ECPA in 1986, courts have had difficulty applying its provisions. The original intent of Congress in passing the law has been frustrated as technology has continued to advance. Ironically, Senator Leahy's 1986 statement that the then current law was "hopelessly out of date"[114] is equally applicable to the ECPA today, in light of the extraordinary technological developments that have occurred in the last fourteen years.[115] The ECPA is particularly ineffective in articulating the

111. *See* Bohach v. City of Reno, 932 F. Supp. 1232, 1237 (D. Nev. 1996). On a similar note, the court in *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996), held that the defendant had a reasonable, though limited, expectation of privacy in e-mail messages on a commercial subscription service. The defendant's e-mail messages in storage with America Online were obtained pursuant to a warrant in an investigation of child pornography and obscenity. *See id.* at 412-14. The court stated that a network user has a reasonable expectation that e-mail will not be revealed to police, but there is always the risk that an employee of the service provider will obtain access; there is also a risk that the recipient of the e-mail will redistribute it. *See id.* at 418.

The *Maxwell* court analogized the relationship between a computer network subscriber and a network as similar to that of a bank customer and a bank, stating that neither the network subscriber nor the bank customer has a reasonable expectation that the records are completely private. *See id.* Also, in each situation, the customer has no control over which employees see their records. *See id.* While the court agreed with the government that privacy in e-mail messages varies with respect to the type of e-mail involved and the intended recipients, it nevertheless retained its holding that there is a reasonable expectation of privacy for e-mail sent from one individual to another individual. *See id.* at 418-19. This case makes it evident that a clear statutory statement on the reasonable expectation of privacy in electronic communications is needed.

112. *Bohach*, 932 F. Supp. at 1236; *see also supra* note 49 for the text of 18 U.S.C. § 2701(c)(1).

113. *See Bohach*, 932 F. Supp. at 1237. This decision is actually best known for its holding regarding privacy in employee e-mail. The court held the police officers had no reasonable expectation of privacy in the messages sent over the police department's pager system. *See id.* at 1236; *see also supra* note 90 for further discussion of e-mail privacy.

114. *See supra* note 39 and accompanying text for an account of the Senator's remark.

115. The most powerful example is the development and increasing popularity of the Internet. In 1969, academic researchers and developers established the "ARPAnet," a national computer network. By the time the ECPA was passed in 1986, ARPAnet had grown into a global Internet, but still only a relatively small number of academics and scientists had access to the network. The late 1980s saw both academic and corporate connectivity to the Internet gain in popularity, and by the mid-1990s,

appropriate application of Title I as opposed to Title II and in dealing with electronic communications service providers.

Much confusion has surrounded the application of ECPA Title I versus Title II. Indeed, "the intersection of the Wiretap Act (18 U.S.C. §§ 2510-2520) and the Stored Communications Act (18 U.S.C. §§ 2701-2710) is a complex, often convoluted, area of the law."[116] The initial attempt to decipher this aspect of the ECPA by the Fifth Circuit in *Steve Jackson Games*[117] remains the most plausible approach under the current wording of the statute. The Fifth Circuit astutely concluded that Congress did not intend for a violation of Title II to include a violation of Title I as well; the titles operate independently of one another.[118] A communication is either intercepted while in transmission, thereby falling under Title I, or it is accessed while in storage, thereby falling under Title II. While the Fifth Circuit's analysis makes this interpretation seem simple, it is far from obvious from the text of the ECPA. Uncertainty and conjecture are hallmarks of court decisions regarding Titles I and II of the ECPA, an act that is "famous (if not infamous) for its lack of clarity."[119]

One reason the statutes of the ECPA are unclear as to the application of Title I or Title II lies in the omission of a definition for the important term "access." Because of this critical omission, courts have struck out on their own in search of the proper meaning for the term. For example, the court in *United States v. Smith* incorrectly concluded that "access" was a lesser-included offense of "intercept."[120] However, it is possible to intercept communications without accessing them within the meaning of the statute, thereby negating the court's logic.[121] The Tenth Circuit in *Davis v. Gracey*

---

personal computers all over the world were connecting to the Internet. For a more general discussion of the advances technology has made since the ECPA was passed, see *supra* note 16.

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

117. 36 F.3d 457 (5th Cir. 1994).

118. *See Steve Jackson Games*, 36 F.3d at 463; *see also supra* note 53 and accompanying text for a discussion of the court's reasoning.

119. *Id.* at 462.

120. *See Smith*, 155 F.3d at 1058. The court may have reached this conclusion partly because the questionable activity involved the interception of *wire communications*, not electronic communications. The court attempted to distinguish between the two to support its broader interpretation of "intercept," *see id.* at 1057-58, but the narrower interpretation is preferable to ensure uniformity of results.

121. For example, a process colloquially referred to as "packet sniffing" allows a user to intercept raw computer network traffic without necessarily viewing the contents of those communications. The data sent within computer networks are often broken into subparts called "packets." These packets are sent across network connections with identification codes as to which computer should receive the information. The packets are routed to the destination computer, then processed by that computer to make a complete communication, which, for example, might include an e-mail message. However, the other computers in the "network segment," or local portion of the network, also have access to these

was not sure whether the term "access" applied to the physical dismantling of computer hardware or to the activities of law enforcement officers.[122] In *United States v. Moriarty*, the court interpreted "access" as applying to both contemporaneous transmissions and stored communications.[123] This broad interpretation of "access" is slightly flawed in that Congress apparently intended "access" to apply only to stored transmissions in the language of the ECPA.[124]

The courts' quest for the meaning of critical ECPA terms does not stop there. The *Smith* court misunderstood the meaning of "intercept" to be "actually acquiring the contents of a communication,"[125] rather than simply gathering the signals of a communication simultaneously with transmission.[126] "Access" was defined by the court as "being in position to acquire the contents of a communication,"[127] but Congress seemed to intend that access encompass actual acquisition.[128] Though the interpretive tools all point to this definition of access, the statute is nevertheless unclear because of Congress's failure to include "access" in its definition section of the ECPA.[129] When an integral ECPA term like "access" remains undefined by

---

packets. In normal operation, these computers simply disregard packets on the network that are not intended for them. Packet sniffing involves setting up a computer to receive and store *all* packets on the network segment, regardless of their intended recipient. This interception does not, however, block the recipient's access to the communications. In other words, a packet sniffer can, without the recipient's knowledge, intercept that recipient's electronic communications. The party using the packet sniffer may either actively look at the data or simply store it on his computer for later use. Thus, it is possible to "intercept" electronic communications without "accessing" them within the meaning of the ECPA. For an example of the mechanics of packet sniffing, *see* ÆLEEN FRISCH, ESSENTIAL SYSTEM ADMINISTRATION 595-97 (2d ed. 1995).

122. 111 F.3d 1472, 1484, n.13 (10th Cir. 1997). Considering Congress's emphasis on law enforcement interests in passing the ECPA, the discrepancies made apparent in *Davis* should be clarified as soon as possible to remove any hindrance to effective law enforcement. *See* S. REP. NO. 99-541, *supra* note 31, at 4. (commenting that "[t]he lack of clear standards may expose law enforcement officers to liability and may endanger the admissibility of evidence.")

123. 962 F. Supp. 217, 220 (D. Mass. 1997).

124. *See* 18 U.S.C. §§ 2511, 2701 (1994). Congress was careful not to mention the word "access" in Title I, which deals with interception of electronic communications. In addition, Congress did not mention "intercept" in Title II, which deals with access to stored electronic communications. There is an obvious intention to keep the two terms separate in the statutes.

125. *Smith*, 155 F.3d at 1058; *but see* United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (reasoning that Congress intended "intercept" to apply only to acquisition of data simultaneous with transmission of data, not to communications in electronic storage).

126. For courts who follow the latter definition, see Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994) and United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976).

127. United States v. Smith, 155 F.3d 1051, 1058 (9th Cir. 1998).

128. *See Steve Jackson Games*, 36 F.3d at 463 (explaining that when law enforcement officers *intercept* communications, they will often have to gain *access* to the contents of the communications to carry out their investigation)(emphasis added).

129. *See* 18 U.S.C. § 2510 (1994).

Congress, courts can be expected to adopt a wide range of interpretations,[130] thereby endangering uniformity of the law.

Beyond the Title I versus Title II debate and the confusion over "access," the statutes of the ECPA pose even more serious threats to the privacy of electronic communications. Specifically, Title II of the ECPA does not prohibit individuals other than public electronic communication service providers from disclosing stored electronic communications.[131] While courts have had little difficulty applying this statute, it often produces anomalous results.

The most recent example of this Title II provision in action is *Andersen Consulting LLP v. UOP*,[132] where the defendant disclosed to the Wall Street Journal plaintiff's e-mail messages, which were sent on the defendant's computer system.[133] In *Wesley College v. Pitts*,[134] the defendants did not provide an electronic communication service to the public, and so were free to disclose and use the contents of a communication that was unlawfully obtained from storage by a third party.[135] The defendant in *State Wide Photocopy, Corp. v. Tokai Financial Services, Inc.*[136] disclosed the plaintiff's electronic communications to a competitor of the plaintiff, but was not held liable because of the "public" provider prohibition in Title II of the ECPA.[137]

The defendants in these cases escaped unpunished, despite the detrimental effect on plaintiffs' reputations, because of the narrow Title II prohibition of the disclosure of stored electronic communications.[138] These cases illustrate the harsh consequences of invasions of electronic privacy where no statutory protection exists. When drafted by Congress in 1986,[139] the narrow scope of the ECPA was adequate to protect electronic privacy in the much smaller

---

130. For examples of various court interpretations, see *supra* notes 120, 122, and 123 and accompanying text.

131. *See supra* note 82 for the text of 18 U.S.C. § 2702(a)(1). In addition, subsection (2) states, "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . .." 18 U.S.C. § 2702(a)(2) (1994).

132. 991 F. Supp. 1041 (N.D. Ill. 1998).

133. *See id.* at 1042.

134. 974 F. Supp. 375 (D. Del. 1997).

135. *See id.* at 389.

136. 909 F. Supp. 137 (S.D.N.Y. 1995).

137. *See supra* notes 99 and 101 for a discussion of the *State Wide* case.

138. *See Andersen Consulting*, 991 F. Supp. at 1043; *Wesley College*, 974 F. Supp. at 389.

139. The comments in the Senate Committee Report of 1986 reveal that Congress considered the situation where a wire or electronic communications service provider also provides other services to the public. They stated that in such instances, the provider should be treated as if the communication services and the other services were provided by separate sources. *See* S. REP. NO. 99-541, *supra* note 31, at 34. However, Congress did not seem to consider private entities that provide electronic communication services to their employees and contractors, but not to the outside public.

electronic communications market at the time. In contrast, the increased use of high technology and the pervasive use of electronic communication such as e-mail in today's business world makes the ECPA positively harmful to current electronic privacy rights.

Although not quite as serious as its narrow prohibition of disclosure, Title II of the ECPA threatens electronic privacy in another way through lax regulation of service providers. The ECPA liability exception for electronic communication service providers in Title II's § 2701(c)(1)[140] is confusing and has been misconstrued by courts.[141] In *Bohach v. City of Reno*,[142] the court rashly interpreted § 2701(c)(1) as allowing providers to do as they pleased in accessing their employees' stored electronic communications.[143] While Congress clearly intended that service providers be allowed to access stored communications in order to conduct their business, it is not clear that Congress intended them to have free reign with their customers' stored communications.[144] Congress must answer the call of the courts to settle the intended meaning of the service provider liability exception in § 2701(c)(1).

IV. PROPOSAL

Because of the difficulty courts have with interpreting the ECPA as it is written, Congress should make a few simple changes to clarify the law in this

---

140. *See supra* note 49 for the text of the statute.

141. In contrast, § 2703(c)(1)(A) is clear and relatively easy to apply. In this subsection, the ECPA specifically allows electronic communication service providers to reveal the identities of their subscribers. 18 U.S.C. § 2703(c)(1)(A) states:

> Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

18 U.S.C. § 2703(c)(1)(A) (1994).

The plaintiff in *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1106-7 (E.D. Mich. 1998), posted a message that was harassing to her lover's ex-wife, and she sued America Online under the ECPA after the company released her identity to the ex-wife pursuant to a subpoena. The district court held that the prohibitions of the ECPA do not apply in this situation. *See id.* at 1108.

The court reasoned that the ECPA prohibits disclosure of the contents of an electronic communication to any person, *see* 18 U.S.C. § 2702, or to the government, *see* 18 U.S.C. § 2703, without meeting certain restrictions. However, contents were not at issue. The issue, revealing the identity of an America Online customer, is specifically allowed by the statute. *See* 18 U.S.C. § 2703 (c)(1)(A) (1994). Therefore, the plaintiff's claim for violation of the ECPA failed. *See Jessup-Morgan*, 20 F. Supp. 2d at 1108.

142. 932 F. Supp. 1232 (D. Nev. 1996).

143. *See id.* at 1236.

144. This is evident from Congress' statement in the Senate Committee Report regarding their goal of ensuring Fourth Amendment privacy protection to Americans in the wake of advanced technology. *See* S. REP. NO. 99-541, *supra* note 31, at 4.

important area.[145] For example, the application of Title I as opposed to Title II should be explained in detail. To achieve this goal, Congress could add a simple provision in one or both titles stating that

> Title I applies only to interception; that is, acquisition of communications that is contemporaneous with their transmission, and Title II applies when the communications at issue were in electronic storage at the time of the incident in question. A given electronic communication must fall under either Title I or Title II, but not both simultaneously.[146]

This amendment would clarify the scope of each title of the ECPA, thereby circumventing much discussion and debate by the courts.[147] It would also assist the electronic communications industry from a planning perspective, because consequences for violations of the ECPA would be more certain.

Clarification of the scope of Titles I and II also demands a statutory definition of the term "access." Several appellate courts as well as district courts have noted this omission from the ECPA,[148] and were therefore forced to use contextual hints and legislative history to determine Congress's intended meaning. To remedy the current confusion, "access" should be defined as "acquisition of or entry to."[149] Congress should also consider the inclusion of a statement explaining that "access" is completely separate from "interception"[150] and it only applies to stored communications within the

---

145. At present, the simple changes proposed here would eliminate much of the confusion surrounding the ECPA as it is written. However, because of the nature of technology, and consequently the law that deals with technology, future changes will also need to be implemented. Indeed, the framework of the original ECPA will likely have to be abandoned at some point in the future to contend with as yet unfathomable advances in technology. The underlying goal of the ECPA - protecting electronic privacy and Fourth Amendment rights - should remain at the heart of any new legislation.

The author notes that since the drafting of this Note, a bill has been introduced in the House of Representatives called the "Electronic Communications Privacy Act of 2000." *See* H.R. 5018, 106th Cong. (2000). While the bill attempts to expand the current law by adding "electronic communications" to the coverage of many provisions, it does not address the specific changes proposed here, and Congress should consider further changes to the law.

146. Congress could insert this proposed amendment in 18 U.S.C. § 2511 (Title I), the interception provision, and in 18 U.S.C. § 2701 (Title II), the stored communications provision. Another option would be to add a section describing the scope of each title to 18 U.S.C. § 2510, the definitions provision.

147. *See, e.g.*, United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994).

148. *See, e.g.*, Davis v. Gracey, 111 F.3d 1472, n.13, (10th Cir. 1997); United States v. Moriarty, 962 F. Supp. 217, 219 (D. Mass. 1997).

149. Congress could add this definition to the definition section of the ECPA, 18 U.S.C. § 2510.

150. *See* 18 U.S.C. §§ 2510(4), 2511 (1994); *see also supra* notes 61 and 47 for the text of the

ECPA.[151] By establishing a definition for "access," Congress can better express its original intent in passing the ECPA. Courts will no longer struggle with defining this term, and they will be able to forge on to interpretation and application.[152] The differences in Titles I and II and their respective punishments will be made even clearer by defining the term "access."

Title II's lack of prohibition for the disclosure of stored electronic communications by individuals other than electronic communications service providers[153] also deserves Congress's attention. Section 2702 of the ECPA should be extended to prohibit disclosure of unlawfully obtained stored electronic communications by anyone, not just service providers. Congress could accomplish this by adding a third subsection to § 2702(a) which could read, "A person or entity shall not knowingly divulge to any person or entity the contents of any communication in electronic storage that was obtained through unlawful access as described in section 2701."[154]

By broadening the scope of the prohibition on disclosure of stored electronic communications, Congress can deter the further breach of privacy that occurs with disclosure of unlawfully obtained communications, which is unpunished under the current law.[155] This amendment will better serve Congress's purpose of strengthening electronic privacy rights by preventing the wily use of stored communications by non-providers like UOP.[156] As technology and its accessibility within the business and private realms have advanced, opportunities to take advantage of the narrow scope of Title II of the ECPA have increased.[157] Courts have struggled with this problem, sometimes concluding that defendants are not technically liable under Title I or Title II, although their conduct seems inherently wrongful. This increased

---

statutes.

151. *See* 18 U.S.C. § 2701 (1994); *see also supra* note 49 for the text of the statute.

152. This is very important to effect Congress's intentions in the ECPA; often a court's interpretation of the meaning of the key term "access" determines the outcome of the case. For examples of decisions that turn at least in part on the court's interpretation of "access," see *supra* notes 68 and 120 and accompanying text.

153. *See* 18 U.S.C. § 2702(a) (1994); *see also supra* note 82 for the text of the statute.

154. Even after this change, it would remain proper to apply all the current exceptions listed in 18 U.S.C. § 2702(b). It should be noted that the proposed amendment encompasses only stored electronic communications obtained *unlawfully*. Therefore, non-public service providers such as businesses, universities, and bulletin board operators would not face unduly harsh legislative restraints under the amended § 2702.

155. *See supra* note 82 for the text of the relevant statute in the ECPA.

156. For a description of UOP's conduct, see *supra* notes 83-84 and accompanying text; *see also* State Wide Photocopy, Corp. v. Tokai Fin. Serv., Inc., 909 F. Supp. 137, 139 (S.D.N.Y. 1995).

157. *See supra* note 115 for a description of technological advances since the passage of the ECPA.

circumvention of the policy against divulgence of private electronic communications makes a strong case for amendment by Congress.

The liability exception for service providers in § 2701(c)(1)[158] is overly broad and should be restricted. Specifically, this section should be clarified as applying only when access by a service provider is authorized for a legitimate business purpose. Congress could accomplish this by adding the phrase, "when authorized for a legitimate business purpose" to § 2701(c)(1).[159] An amendment of this type would prevent misunderstandings by courts in opinions such as *Bohach v. City of Reno*,[160] where the judge concluded that providers can "do as they wish when it comes to accessing communications in electronic storage."[161] Although a business purpose standard may have shortcomings,[162] still it would deter blatant disregard for the spirit of the law by service providers, which greatly improves the current situation.

V. CONCLUSION

The Electronic Communications Privacy Act of 1986 is quickly becoming outdated. Courts, commentators, and the technology community all demand updated legislation.[163] By adopting the above-proposed amendments to the ECPA, Congress can alleviate the current interpretation

158. *See supra* note 49 for the text of the statute.

159. *See supra* note 47 for the text of the statute.

160. 932 F. Supp. 1232 (D. Nev. 1996).

161. *See id* at 1236.

162. A "legitimate business purpose" standard may invite deference to service providers by courts akin to the deference found in the Business Judgment Rule in corporate law. *See, e.g.*, Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984). In fact, the temptation to defer to service providers is potentially even greater in the electronic communications industry than in corporate law because of the specialized expertise involved. Courts may be likely to blindly trust the assertions of service providers without too much investigation into the technology involved.

163. *See supra* notes 116-119, 122, 26, and 27 for examples of subtle and direct desires for change in the law. A demand for updated legislation in the electronic privacy area can also be attributed to the European Union (EU). The EU's Directive on Data Protection protects personal information about individual customers from being exploited by businesses. *See* Council Directive 95/46/EC, art. 1, 1995 O.J. (L 281) 31. The directive went into effect on October 25, 1998, three years after it was adopted. *See id.* at art. 32. Article 25 of the directive is of utmost concern to the United States, because it prohibits the transfer of personal information from the EU to countries without "an adequate level of protection," which includes the United States by EU standards. *See id.* at art. 25. This prohibition has the potential to devastate electronic commerce between the United States and Europe. A temporary solution has been crafted in a bilateral agreement between the EU and United States companies that choose to voluntarily adhere to certain Safe Harbor Principles. *See* International Trade Administration Electronic Commerce Task Force, *International Safe Harbor Privacy Principles* (last modified Dec. 8, 2000) <http://www.export.gov/safeharbor>. However, a permanent solution to the clashing privacy philosophies of the United States and the EU is still desperately needed to preserve the global economy.

controversies in the courts.[164] More importantly, however, these amendments have the effect of raising electronic privacy to a level commensurate with technology.[165] Allowing the ECPA to continue in its current state deprives electronic communications users of the precious right of privacy in many ways.[166] In order to preserve age-old privacy rights in the information age, the law simply must be changed.

Julie J. McMurry

---

164. *See supra* note 145 for further details on the effects of the amendments proposed here.
165. *See supra* note 145 for further details on the effects of the amendments proposed here.
166. For one example of the ECPA's harsh affect on electronic privacy, see *supra* note 98 and accompanying text.