Journal of Law and Policy

Volume 7 | Issue 2 Article 4

1999

Proposal For A Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act

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*

*Tatsuya Akamine***

Legislation, both statutory and constitutional, is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions and purposes.[1]

INTRODUCTION

Electronic mail ("e-mail") has become an increasingly popular and important tool of communication in the workplace and at home.[2] Accordingly, people have come to expect the same level

---

* 18 U.S.C. §§ 2232, 2510-2513, 2516-2521, 3117 (1994 & Supp. III 1997). The Federal Wiretap Act is the common name of Title I of the Electronic Communications Privacy Act of 1986 ("ECPA"). *See infra* note 8 and accompanying text (explaining the common use of the term "Federal Wiretap Act" to refer to Title I of the ECPA).

** Brooklyn Law School Class of 2000. The author wishes to thank Jeannie Sha for her editorial advice and encouragement.

[1] Olmstead v. United States, 277 U.S. 438, 472-73 (1928) (Brandeis, J., dissenting) (citing Weems v. United States, 217 U.S. 349, 373 (1909)).

[2] "According to a Gallup poll, 90% of all large companies, 64% of midsize companies and 42% of small businesses use e-mail. Forty million workers correspond via e-mail, and that number is increasing by 20% per year." Edward Hertenstein, *Electronic Monitoring in the Workplace: How Arbitrators Have Ruled*, 52-AUT DISP. RESOL. J. 36, 37 (1997) (citing MARK S. DICHTER & MICHAEL S. BURKHARDT, ELECTRONIC INTERACTION IN THE WORKPLACE: MONITORING, RETRIEVING AND STORING EMPLOYEE COMMUNICATIONS IN THE

of protection for e-mail as a telephone communication.[3] In particular, when a person is given a private password for using an e-mail account, such an expectation of privacy is quite reasonable.[4]

INTERNET AGE § I.A (1996), *available at* <http://www.mlb.com/speech1.-htm>). "As of January, 1996, thirty-seven percent of U.S. households (35.1 million) had a personal computer; of those, fifty-three percent (18.75 million) had at least one modem." Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 414 (1997).

[3] *See* United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (holding that e-mail users generally enjoy a reasonable expectation of privacy); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (holding that e-mail users enjoy a reasonable expectation of privacy for the transmitted message *until retrieved by the recipient*); Stephen P. Heymann, *Legislating Computer Crime*, 34 HARV. J. ON LEGIS. 373, 385-86 (1997) (implying a reasonable expectation of privacy for an e-mail message, as in the case of a voicemail message). Although e-mail may be more vulnerable to an interception than a telephone, such a difference does not necessarily justify a different level of privacy protection. *See* Leib, *supra* note 2, at 412-14.

> E-mail messages, by their very nature, are already less private than many other forms of communication. Typically, an e-mail message, which originates in the computer of the sender, travels through many computers before reaching its final destination. At each computer, the operator of the computer system can access the message. In addition, when the service provider receives the message, the system computer stores a copy of that message and retains it, even after retrieval by the intended recipient. . . .
>
> E-mail is an important technology whose vulnerability to interception makes it that much more important to give it strong legal protection from interception. . . .
>
> . . . .
>
> Electronic communication's vulnerability to interception is not a sound reason for giving it less protection from government interception.

Lieb, *supra* note 2, at 412-13 (footnotes omitted).

[4] *See* Leib, *supra* note 2, at 414 (implying that people have a reasonable expectation of privacy for e-mail when using a private password); Scott A. Sundstrom, Note, *You've Got Mail! (and the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2082-86 (1998). However, due to certain exceptions under the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat.

The most important legislation designed to protect privacy interests for e-mail is the Electronic Communications Privacy Act of 1986 ("ECPA").[5] The ECPA was enacted to amend Title III of

---

1848 (codified in scattered sections of 18 U.S.C.), employers enjoy a broad authority to monitor communications by their employees in the workplace. Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 235 (1994). The first exception is the "ordinary course of business" exception under section 2510(5)(a)(i) of the ECPA. *Id.* at 235-36. It is similar to the use of an extension telephone and permits an employer to monitor employee communication through the device furnished to and used by an employee in the ordinary course of business. *Id.* The second exception is a "system provider" exception under section 2511(2)(a)(i), whereby an employer, as a system provider, is able to monitor employee communication as a means to maintain its e-mail system. *Id.* at 236-37. *See also* 18 U.S.C. § 2701(c)(1) (providing that the prohibition on unauthorized access to stored wire or electronic communications is not applicable to the conduct authorized by the entity providing a wire or electronic communications service). These exceptions in favor of an employer come from the notion that an employer has the right to preserve its property rights. *See* Hertenstein, *supra* note 2, at 41-42 (discussing case law, NLRB rulings and arbitration awards which "point toward the concept that employees have some privacy rights at work, but that those rights are limited by employers' personal property rights"). However, some commentators address the need to strike an appropriate balance between an employer's interest in monitoring employee communication and an employee's privacy concern. *See, e.g.*, Kevin J. Baum, Comment, *E-mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011, 1041 (1997); Greenberg, *supra*, at 249-50; Sundstrom, *supra*, at 2068. It is also recommended that an employer tell its employees of the monitoring policy. *See, e.g.*, Hertenstein, *supra* note 2, at 44; Baum, *supra*, at 1041; Greenberg, *supra*, at 249-50.

[5] Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.). In addition to the ECPA, there are several federal statutes regarding the protection of privacy interests. One such statute is the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-1811 (1994), 18 U.S.C. § 2511 (1994 & Supp. III 1997), and 18 U.S.C. §§ 2518-2519 (1994)). The FISA, however, is confined to national security cases, authorizing electronic surveillance to obtain foreign intelligence information. *Id.* Another legislation designed to address the recent technological developments in the context of an electronic communication is the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010 (1994) and in scattered sections of 18 U.S.C. and 47 U.S.C.). The CALEA requires telephone companies' cooperation with law enforcement and also extends the

the Omnibus Crime Control and Safe Streets Act of 1968[6] (the original Federal Wiretap Act) in order to cover e-mail and other forms of electronic communications.[7] Title I of the ECPA ("Federal Wiretap Act")[8] addresses the issue of an interception of electronic communications (i.e., wiretapping), and Title II of the ECPA ("Stored Communications Act")[9] deals with unauthorized

---

protections under the ECPA to a cordless telephone. In addition, other federal statutes, not specifically directed at electronic surveillance, but potentially relevant under certain circumstances, include: Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. III 1997) (regulating government's handling of individual information); Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994 & Supp. III 1997) (regulating credit reporting agencies to protect the confidentiality of credit reports); Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (1994) (prohibiting video stores from disclosing customers' rental records); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (codified in scattered sections of 47 U.S.C., 15 U.S.C., 46 U.S.C., 18 U.S.C., 50 U.S.C.) (prohibiting cable operators from disclosing customers' viewing records). *See also* Joshua B. Sessler, Note, *Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet*, 5 J.L. & POL'Y 627 (1997) (describing these statutes in detail).

[6] 18 U.S.C. §§ 2510-2513, 2515-2520 (1982); 47 U.S.C. § 605 (1982).

[7] *See infra* notes 8-9 and accompanying text (delineating the ECPA).

[8] 18 U.S.C. §§ 2232, 2510-2513, 2516-2521, 3117 (1994 & Supp. III 1997). Title III of the Omnibus Crime Control and Safe Streets Act of 1968 has been commonly referred to as the "Federal Wiretap Act" or "Title III." *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994); James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 71 (1997). Since Title I of the ECPA is an amendment to the Federal Wiretap Act, in this Note, Title I of the ECPA is often interchangeably referred to as the "Federal Wiretap Act" for ease of reference, Title III being distinguished as the "original Federal Wiretap Act." Title I of the ECPA is captioned as "Interception of Communications and Related Matters," and its main provisions are included in the chapter referred to as "Wire and Electronic Communications Interception and Interception of Oral Communications." Title I of the ECPA expanded the pre-existing Federal Wiretap Act in order to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. REP. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. In contrast, Title II of the ECPA was added to Title 18 as a new chapter. *Id.*

[9] 18 U.S.C. §§ 2701-2710 (1994 & Supp. III 1997). Title II of the ECPA is referred to as "Stored Wire and Electronic Communications and Transactional

access to stored electronic communications.[10] For example, section 2511 prohibits the interception and the use or disclosure of wire, oral, or electronic communications,[11] and sections 2701 and 2702 prohibit the unauthorized access to and disclosure of stored wire and electronic communications.[12] Title I requires a court

---

Records Access," and its main provision, section 2701, is entitled "Unlawful Access to Stored Communications." Thus, in this Note, Title II of the ECPA is often interchangeably referred to as the "Stored Communications Act" for ease of reference. Yet this does not suggest that an e-mail message stored in a service provider computer is solely covered by Title II. It only means that some stored communications are particularly covered by Title II. The court opinions and commentaries often refer to Titles I and II by their numbers only. *See, e.g.*, *Steve Jackson Games*, 36 F.3d at 459. However, for ease of reference, this Note often uses descriptive names for Titles I and II of the ECPA as well as their numbers.

[10] *See supra* notes 8-9 and accompanying text (delineating the ECPA).

[11] Section 2511 provides, in relevant part:

> (1) 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; . . . (c) 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; (d) intentionally uses, or endeavors to use, 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; . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511.

[12] Section 2701 provides, in relevant part:

> (a) Offense.—Except as provided in subsection (c) of this section whoever (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 punished as provided in subsection (b) of this section.

18 U.S.C. § 2701. Section 2702 provides, in relevant part:

order for wiretapping,[13] while Title II only requires a search warrant for accessing stored communications.[14] The criminal sanctions and the civil liabilities for violation of Title I are greater than those for violation of Title II.[15] The ECPA addresses invasion of privacy by private parties as well as by government.[16]

In 1994, the Fifth Circuit held, in *Steve Jackson Games, Inc. v. United States Secret Service*, that Title I of the ECPA (the Federal Wiretap Act) is not applicable to the unauthorized access

---

> (a) Prohibitions.—Except as provided in subsection (b)—(1) 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 (2) 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—(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and (B) 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 for purpose of providing any services other than storage or computer processing.

18 U.S.C. § 2702 (1994).

[13] 18 U.S.C. § 2518 (1994).

[14] 18 U.S.C. § 2703 (1994 & Supp. III 1997).

[15] The violation of Title I is, in most cases, punishable by a fine or imprisonment for not more than five years, or both. 18 U.S.C. § 2511(4)(a) (1994). In contrast, the violation of Title II is punishable by a fine or imprisonment for not more than six months, or both. 18 U.S.C. § 2701(b). *See infra* note 69 and accompanying text (describing the criminal sanctions for violation of Title II). Under section 2520, compensatory damages as well as punitive damages are recoverable, together with a reasonable attorney's fee. 18 U.S.C. § 2520 (1994). The damages are the greater of (I) the sum of the actual damages and any profits made by the violator, or (II) statutory damages of greater of $100 a day or $10,000. *Id.* Under section 2707, compensatory damages as well as the punitive damages are recoverable, together with a reasonable attorney's fee. 18 U.S.C. § 2707 (1994 & Supp. III 1997). The damages include actual damages and any profits made by the violator, and will in no case be less than $1,000. *Id.*

[16] 18 U.S.C. §§ 2511, 2701. *See infra* notes 68-70 and accompanying text (describing the criminal and civil liabilities for violation of the ECPA).

of e-mail stored in a service provider computer, which a subscriber accesses in order to retrieve and read the e-mail message.[17] Unlike a telephone communication, e-mail is stored in a service provider computer until the addressee accesses the computer to retrieve and read the message.[18] The Fifth Circuit, relying upon *United States v. Turk*,[19] stated that the interception of an electronic communication prohibited by Title I must occur contemporaneously with the transmission of e-mail.[20] Thus, the unauthorized access to e-mail stored in a service provider computer does not violate Title I.[21] The court also emphasized that the definition of "electronic communication" does not specifically refer to electronic storage, as contrasted with the definition of "wire communication," which explicitly includes electronic storage.[22] Thus, the court concluded that an interception of electronic communications

---

[17] 36 F.3d 457, 457 (5th Cir. 1994).

[18] A service provider computer is not a personal computer of an addressee, but a computer of an e-mail service provider connected via a telephone line with the subscriber's personal computer. S. REP. No. 99-541, at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562. The Senate Report explains electronic mail as follows:

> Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer 'mail box' until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system.
>
> Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.

Id.

[19] 526 F.2d 654, 658 (5th Cir. 1976).

[20] *Steve Jackson Games*, 36 F.3d at 460. *See infra* Part II.B, discussing the court's reasoning in *Steve Jackson Games*.

[21] *Steve Jackson Games*, 36 F.3d at 460.

[22] *Id.* at 461.

does not cover e-mail stored in a service provider computer, because the term "electronic communication" does not include "electronic storage."[23] Additionally, the Fifth Circuit considered the difference in requirements and procedures between Titles I and II as critical.[24] The court stated that Title I does not apply when accessing e-mail stored in a service provider computer, because Title II addresses such access.[25] After *Steve Jackson Games*, several cases, including *Wesley College v. Pitts*,[26] followed the reasoning of the Fifth Circuit.[27]

However, the consequence of the *Steve Jackson Games* decision is largely criticized by commentators.[28] For example, Commentator Gregory L. Brown, cited in *Wesley College*, states

---

[23] *Id.* at 461-62.

[24] *Id.* at 462. *See infra* Part II.B, discussing the court's reasoning in *Steve Jackson Games*.

[25] *Steve Jackson Games*, 36 F.3d at 462-63.

[26] 974 F. Supp. 375, 381-91 (D. Del. 1997).

[27] *See* United States v. Moriarty, 962 F. Supp. 217, 220-21 (D. Mass. 1997) (holding that listening to a stored voice mail message was not an interception because the defendant did not listen to the voice mail while it was recorded on the answering machine); Bohach v. City of Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (holding that the access to the messages stored in the computer paging system was not an interception); United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (holding that pressing the pager button to gain access to its message was not an interception because such access was not made while the message was being transmitted to the pager); Payne v. Norwest Corp., 911 F. Supp. 1299, 1303 (D. Mont. 1995) (holding that non-simultaneous recording of a voice mail message with a hand-held tape recorder was not an interception), *aff'd in part and rev'd in part*, 113 F.3d 1079 (9th Cir. 1997).

[28] *See, e.g.*, Gregory L. Brown, Recent Development, Steve Jackson Games, Inc. v. United States Secret Service*: Seizure of Stored Electronic Mail Is Not an "Interception" Under the Federal Wiretap Act*, 69 TUL. L. REV. 1381, 1390-91 (1995); Nicole Giallonardo, Casenote, 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, 183-86 (1995); Robert S. Steere, Note, *Keeping "Private E-Mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 232-46 (1998); Jarrod J. White, Commentary, *E-Mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1083 (1997).

that denying application of Title I (the Federal Wiretap Act) to a stored e-mail message allows the government to circumvent Title I by accessing a stored e-mail message rather than one in transmission.[29] In other words, since transmitted e-mail messages are immediately stored in a service provider computer, it is not necessary for the government to intercept e-mail transmission.[30] Moreover, denying the application of Title I (the Federal Wiretap Act) to such unretrieved e-mail messages contradicts the Congressional intent that Title I should generally protect an electronic

---

[29] *See* Brown, *supra* note 28, at 1390. Brown describes the undesirable result of the *Steve Jackson Games* court's construction as follows:

> [T]he privacy interests of an individual sending E-mail change constantly during the course of transmission, depending on whether the message is in a wire, in computer memory, or in a disk when captured. This arbitrary alteration of privacy interests and penalties renders the procedural requirements of [the ECPA] meaningless because an entity could wait until an electronic communication is in electronic storage before gaining access, thereby bypassing the more stringent requirements necessary for intercepting the electronic communication.

Brown, *supra* note 28, at 1390 (citations omitted). *See also* Steere, *supra* note 28, at 263-64. In addition, Brown warns that the ECPA, as interpreted by *Steve Jackson Games*, is likely to raise a constitutional issue under the Fourth Amendment, and that the *Katz* test, for determining a reasonable expecation of privacy, will be used by the courts. *See* Brown, *supra* note 28, at 1391; *infra* Part I.A, discussing the *Katz v. United States* decision. *See also infra* note 65 and accompanying text (discussing the potential constitutional problem).

[30] *See supra* note 18 and accompanying text (describing the e-mail communication process). It is not difficult for the government to access the stored e-mail because Title II provides less stringent requirements for the government access. *See infra* notes 71-72 and accompanying text (describing the different requirements and procedures between Titles I and II of the ECPA). Jarrod J. White also criticizes the court's reading as follows:

> Following the Fifth Circuit's rationale, there is only a narrow window during which an E-mail interception may occur—the seconds or miliseconds before which a newly composed message is saved to any temporary location following a send command. Therefore, . . . interception of E-mail within the prohibition of the ECPA is virtually impossible.

White, *supra* note 28, at 1083.

communication in the same manner as a telephone communication,[31] and also does not conform to the overall structure of the ECPA.[32] Several courts, consistent with these contentions, held that unretrieved e-mail messages enjoy a reasonable expectation of privacy.[33] This emerging judicial recognition threatens the *Steve Jackson Games* court's assumption that the interception of unretrieved e-mail messages—not complying with the stringent procedures under Title I that were established as the necessary safeguards for the protection of a reasonable expectation of privacy—does not violate the Fourth Amendment.[34] Furthermore, recently the Ninth Circuit held, in *United States v. Smith*, that "intercept" under Title I does not have to be contemporaneous with the transmission,[35] thereby rejecting the Fifth Circuit's narrow reading of "intercept" in *Steve Jackson Games*.

In Part I of this Note, the pre-ECPA history and the contents of the ECPA are briefly described, including the differences between Titles I and II. Part II first examines the Fifth Circuit's narrow interpretation of "intercept" in *United States v. Turk*,[36] the Ninth Circuit's recent rejection of such interpretation in *Smith*,[37] and reviews the courts' analysis in *Steve Jackson Games* and *Wesley College*. Part III proposes an alternative statutory interpretation of Titles I and II in support of the position that Title

---

[31] *See infra* notes 57, 64-65 and accompanying text (arguing that Congress generally intended to protect an electronic communication in the same way as wire or oral communications and that there is nothing in the legislative history to indicate the exclusion of unretrieved e-mail messages from the coverage of Title I).

[32] *See* discussion *infra* Part III, arguing that "electronic communication" impliedly includes "electronic storage" and such storage is subject to Title I.

[33] *See* United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (holding that e-mail users generally enjoy a reasonable expectation of privacy); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (holding that e-mail users enjoy a reasonable expectation of privacy for the transmitted message *until retrieved by the recipient*).

[34] *See infra* note 65 and accompanying text (discussing the potential constitutional problem of the *Steve Jackson Games* decision).

[35] 155 F.3d 1051, 1057-58 (9th Cir. 1998), *cert. denied*, 119 S. Ct. 804 (1999).

[36] 526 F.2d 654, 658 (5th Cir. 1976).

[37] 155 F.3d at 1057-58.

I (the Federal Wiretap Act) applies to unretrieved e-mail stored in a service provider computer.[38]

I. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

The Electronic Communications Privacy Act of 1986 ("ECPA") was enacted in 1986 to amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968[39] in an effort "to protect against the unauthorized interception of electronic communications."[40] The ECPA was designed to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[41] In particular, the Senate Report noted, "the law must advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment. . . . [Privacy] will gradually erode as technology advances."[42] At the same time, the ECPA was intended to balance privacy interests against the legitimate needs of law enforcement.[43]

---

[38] The discussion of the statutory language is critical, because the Fifth Circuit in *Steve Jackson Games* criticized the defendants for failure to discuss the relevant provisions of the ECPA:

> For the most part, [defendants] fail to even discuss the pertinent provisions of the [ECPA], much less address their application. Instead, they point simply to Congress' intent in enacting the ECPA and appeal to logic (i.e., to seize something before it is received is to intercept it). But, obviously, the language of the [ECPA] controls.

Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460-61 (5th Cir. 1994).

[39] 18 U.S.C. §§ 2510-2513, 2515-2520 (1982); 47 U.S.C. § 605 (1982).

[40] S. REP. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

[41] *Id.*

[42] S. REP. No. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

[43] *Id.*

A. *The Pre-ECPA Era: Katz v. United States and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (The Original Federal Wiretap Act)*

Before the 1967 decision in *Katz v. United States*,[44] the Supreme Court held that a violation of the right to be free from unreasonable search and seizure under the Fourth Amendment[45] must accompany a physical trespass by government.[46] Thus, a telephone wiretapping without a physical trespass was not covered by the Fourth Amendment.[47] In *Katz*, however, the Supreme Court held that a telephone wiretapping violates the Fourth Amendment right to be free from unreasonable searches and seizures—even if such conduct does not involve a physical trespass.[48] The Court noted, "the Fourth Amendment protects people, not places."[49] However, the Supreme Court indicated that surveillance approved in advance, by a specific court order establishing precise limits, may be acceptable under the Fourth Amendment.[50] In response to the *Katz* decision, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the original Federal Wiretap Act).[51] Title III required the

---

[44] 389 U.S. 347 (1967).

[45] The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

[46] Olmstead v. United States, 277 U.S. 438, 465-66 (1928) (reasoning that the language of the Fourth Amendment only refers to tangible things, such as persons, houses, papers, and effects, not hearing or sight).

[47] *Id.*

[48] *Katz*, 389 U.S. at 353. In *Katz*, FBI agents wiretapped a public telephone booth without physically trespassing the suspect's property. *Id.* at 348-49.

[49] *Id.* at 351.

[50] *Id.* at 356-57.

[51] Pub. L. No. 90-351, §§ 801-804, 82 Stat. 197, 211-25. Congress also took into consideration the Supreme Court's decision of *Berger v. New York*,

government to obtain a court order to tap a telephone and provided for application of the statutory exclusionary rule for unlawfully obtained evidence.[52]

---

388 U.S. 41 (1967), which struck down the New York electronic eavesdropping (bugging) statute as violative of the Fourth Amendment. *Id.* at 64. The *Berger* court delineated the constitutional standards that such a statute should contain. *Id.* at 58-60. Title III was designed to conform to these constitutional criteria as well as to the *Katz* decision. The Senate Report states:

> To assure the privacy of oral and wire communications, title III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers engaged in investigations or prevention of specific types of serious crimes, and only after authorization of a court order obtained after a showing and finding of probable cause.

S. REP. No. 90-1097, at 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153. "Electronic eavesdropping," sometimes called "bugging," is eavesdropping by an electronic device. *Berger*, 388 U.S. at 45-49. Electronic eavesdropping is a broader term than "wiretapping," which concerns only telegraph and telephone communications. *Id.* Neither Title III nor the ECPA uses the terms "electronic eavesdropping" or "wiretap" in their provisions, though Title III is entitled "Wiretapping and Electronic Surveillance." Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801-804, 92 Stat. 197. These statutes instead use the term "intercept." *See* 18 U.S.C. § 2510(4) (1994) (defining "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"). Therefore, these statutes in effect cover "electronic eavesdropping," although the statutes are generally referred to as the wiretap acts. *See supra* note 8 and accompanying text (explaining the common references to these statutes).

[52] 18 U.S.C. § 2518 (1994). James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology, Washington, D.C., and a former assistant counsel for former Rep. Don Edwards (former chairman of the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee), succinctly describes the safeguards established under Title III as follows:

> [C]ontent of wire communications could be seized by the government in criminal cases pursuant to a court order issued upon a finding of probable cause; wiretapping would be otherwise outlawed; wiretapping would be permitted only for specified crimes; it would be authorized only as a last resort, when other investigative techniques would not work; surveillance would be carried out in such a way as to "minimize" the interception of innocent conversations; notice would be

B. *Extension of Protection to Electronic Communication by the ECPA*

Prior to the enactment of the ECPA, only wire and oral communications were protected under the original Federal Wiretap Act.[53] By the mid-1980s, absence of the protection of privacy interests in electronic communications created serious problems, such as electronic espionage and computer hackers.[54] To remedy

---

> provided after the investigation had been concluded; and there would be an opportunity prior to introduction of the evidence at any trial for an adversarial challenge to both the adequacy of the probable cause and the conduct of the wiretap. "Minimization" was deemed essential to satisfy the Fourth Amendment's particularity requirement, compensating for the fact that law enforcement was receiving all of the target's communications, including those that were not evidence of a crime. The showing of a special need, in the form of a lack of other reasonable means to obtain the information, was viewed as justification for the failure to provide advance or contemporaneous notice of the search.

Dempsey, *supra* note 8, at 71-72 (footnotes omitted).

[53] *See* 18 U.S.C. § 2511(1) (1982). The Senate Report discusses the situation before the enactment of the ECPA as follows:

> In 1984, Senator Leahy asked the Attorney General whether he believed interceptions of electronic mail and computer-to-computer communications were covered by the Federal wiretap law. The Criminal Division of the Justice Department responded that Federal law protects electronic communications against unauthorized acquisition only where a reasonable expectation of privacy exists. Underscoring the need for [the ECPA], the Department concluded: 'In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious.'
>
> Senator Leahy's letter and the Justice Department's response mark the beginning of this legislation.

S. REP. No. 99-541, at 3-4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557-58 (second alteration in original).

[54] *See* Leib, *supra* note 2, at 403-04.

> The consequences of this legal omission [of electronic communication from the original Federal Wiretap Act] were great. In the

this situation, the ECPA extended the protection of privacy interests under the original Federal Wiretap Act to electronic communications, such as e-mail.[55] In addition, the ECPA added

---

> business context, a rival corporation could intercept electronic communications, such as e-mail, without repercussion. In fact, by the mid 1980s, companies were losing millions of dollars a year to "electronic espionage." In addition, because e-mail is stored and, therefore, more easily invaded than a telephone call, providers of the new communications became concerned that customers would be discouraged from using the new technology for fear of interception. Law enforcement agencies worried about potential exposure to liability.

Leib, *supra* note 2, at 403-04 (footnotes omitted). Although Leib does not define "electronic espionage," it seems to be a synonym of "electronic eavesdropping." *See supra* note 51 and accompanying text (describing "electronic eavesdropping"). "A 'hacker' is an individual who accesses another's computer system without authority." Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432, 435 n.2 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994).

[55] Leib, *supra* note 2, at 404. The Senate Report recognizes the importance of keeping up with the technological development of electronic communications, but does not indicate in any way the need to treat electronic communications differently from wire or oral communications. *See* S. REP. No. 99-541, at 1-3, 5-8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-57, 3559-62. Moreover, the legislative history of the ECPA supports the position that e-mail stored in a service provider computer is subject to an interception under Title I of the ECPA (the Federal Wiretap Act). That the legislative history does not speak specifically of the present issue is not dispositive. The Congressional intent, as revealed by the Senate Report, is that the term "electronic communication" added to the subject of Title I (the Federal Wiretap Act) be broadly interpreted in order to be able to accommodate new and evolving technology. *See* S. REP. No. 99-541, at 3-5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557-59 (stating "[m]ost importantly, the law must advance with the technology to ensure the continued validity of the [F]ourth [A]mendment"). The ECPA was enacted based on the pressing concern that the original Federal Wiretap Act had become hopelessly obsolete, covering only wire and oral communications. *Id.* The Senate Report evidences that the statute cannot keep up with the ongoing development of technology. *Id.* Thus, the Congressional intent is that Title I of the ECPA, enacted to remedy such situations comprehensively, be liberally interpreted. At a minimum, absent a discernable intent to exclude an e-mail message temporarily stored in a service provider computer from the coverage of Title I, the interception of the unretrieved e-mail message should be subject to Title I (the Federal Wiretap Act). In this connection, it should be noted that

Title II (the Stored Communications Act) to protect stored wire and electronic communications.[56]

Justice Brandeis, in his dissenting opinion in *Olmstead v. United States*, 277 U.S. 438, 472-73 (1928), also cautioned, in the context of technological development and privacy protection, that we should not lose sight as one construes a statute. *See supra* note 1 and accompanying text (referring to Justice Brandeis' dissenting opinion).

[56] Congress added Title II of the ECPA in order to keep up with "the advent of computerized recordkeeping systems," such as computer database and remote data processing services offered by computer service companies for hospitals and businesses. S. REP. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. The rationale was that such off-site computer data in the control of a third party computer service company might be seen as outside the penumbra of privacy protection and may be freely accessed by government and private parties. *Id.* Thus, e-mail messages stored in a service provider computer as a part of a communication process are not primarily intended to be covered by Title II. *Id.* (stating that e-mail messages stored in a service provider computer for *later reference* are subject to the Title II protection, thereby distinguishing such a recordkeeping system from other communication in transit). Commentator Michael S. Leib describes the background for the addition of Title II as follows:

> The ECPA also granted protection to messages held in electronic communication storage, which previously were unprotected. An e-mail message is often retained in the files of the e-mail service provider for administrative purposes. Without a statutory scheme requiring the government to obtain a warrant before reading these stored messages, the government probably would be able to access the stored communications without court approval. In analogous situations, records kept by a third party, such as copies of personal checks held by a bank, have been deemed the property of the third party and, therefore, not protected by the Fourth Amendment. The rationale is that a person who communicates information to a third party takes the risk that the information will be given to government authorities.

Leib, *supra* note 2, at 404-05 (footnotes omitted). The Senate Report explains the remote computer services as follows:

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data in-house on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computer services to subscribers and customers from remote facilities. Today businesses of all sizes—hospitals, banks and many others—use remote computing

Although Congress extended similar protection to an electronic communication as for wire and oral communications, there are several notable differences.[57] For example, there are no limitations on the kind of federal felonies for which the government can access an electronic communication,[58] as contrasted to the case of wire and oral communications.[59] Furthermore, the statutory

---

> services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computer service . . . or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.

S. REP. No. 99-541, at 10-11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564-65.

[57] *See* Leib, *supra* note 2, at 406. "The wide latitude given the government to intercept electronic communication stands in stark contrast to the controls Congress placed on investigations involving wire and oral communication. . . ." Leib, *supra* note 2, at 406. Although these differences indicate that Congress intended somewhat less statutory protection for e-mail than for wire or oral communication, this does not prove that Congress did not recognize a reasonable expectation of privacy for e-mail. To the contrary, the legislative history shows that Congress generally intended to treat an electronic communication in the same manner as wire and oral communications. S. REP. No. 99-541, at 1-3, 5-8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-57, 3559-62. The above noted differences only go to the extent of statutory protection, such as the kind of crimes for which the government can apply to a court for an order authorizing wiretapping. Accordingly, the addition of e-mail to the subject of the Federal Wiretap Act shows the Congressional intent that an electronic communication enjoys the same reasonable expectation of privacy as wire or oral communications. The interpretation of the Fifth Circuit in *Steve Jackson Games* contradicts this Congressional intent because it assumes that unretrieved e-mail messages stored in a service provider computer lack a reasonable expectation of privacy to be protected by Title I of the ECPA (the Federal Wiretap Act). *See infra* note 65 and accompanying text (arguing that Congress recognized a reasonable expectation of privacy for e-mail).

[58] 18 U.S.C. § 2516(3) (1994) (providing that a government attorney, such as a U.S. Attorney or an Assistant U.S. Attorney, may apply to a federal court for an order authorizing the interception of an electronic communication that "may provide or has provided evidence of any Federal felony").

[59] 18 U.S.C. § 2516(1) (1994 & Supp. III 1997) (listing the specific crimes for which the government may apply to a court for an order authorizing the interception of wire or oral communications, such as murder, kidnapping,

exclusionary rule does not apply to wiretapping of an electronic communication.[60] In other words, the less stringent exclusionary rule developed by the courts only applies to an electronic communication.[61] Commentators criticize these differences as baseless and harmful.[62] To the extent that e-mail enjoys a reasonable expectation of privacy as much as a telephone communication does,[63] wiretapping e-mail should meet the same rigorous requirements as those for a telephone communication.[64] Otherwise, in

---

robbery, extortion, bribery, counterfeiting, and drug offenses). Only the specified officials, such as the Attorney General and other attorneys designated by the Attorney General, may authorize such an application for wiretapping wire or oral communications. *Id.*

[60] 18 U.S.C. § 2518(10) (1994).

[61] *See* Leib, *supra* note 2, at 408.

[62] *See, e.g.*, Heymann, *supra* note 3, at 386; Leib, *supra* note 2, at 408-11, 415-16; Greenberg, *supra* note 4, at 247-49. In delineating adverse consequences to these less stringent protections for an electronic communication, Congress has been criticized for "creat[ing] a number of potentially harmful consequences" and "creat[ing] formalistic distinctions between modes of communication that make the availability of the statutory suppression remedy hinge on arbitrary factors." Leib, *supra* note 2, at 411; *see* Steere, *supra* note 28, at 265-66. "[T]he line drawing creates formalistic distinctions that lack a sound policy basis." Leib, *supra* note 2, at 409. Additionally, Leib asserts that such differences are only the result of the compromise, with the Justice Department voicing its law enforcement concern. Leib, *supra* note 2, at 409-11. The Senate Report itself refers to discussions with the Justice Department as a reason for the inapplicability of the statutory exclusionary rule for an electronic communication. *See* S. REP. No. 99-541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

[63] *See supra* notes 3-4 and accompanying text (arguing that a user has a reasonable expectation of privacy for e-mail).

[64] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the original Federal Wiretap Act) was Congress's response to *Katz*, which led to the development of the reasonable expectation of privacy doctrine. *See* Megan Connor Bertron, *Home Is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 166-67 (1996). Thus, even if the government access to a stored e-mail message without a court order is lawful under Title I of the ECPA, there remains a constitutional issue, which is beyond the scope of this Note. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 89 (1994). *See also infra* note 65 and accompanying text (arguing that Congress, by enacting Title I of the ECPA, intended to protect a reasonable expectation of

light of the Supreme Court decision in *Katz*, wiretapping an unretrieved e-mail message raises a constitutional issue under the Fourth Amendment.[65]

---

privacy for e-mail in the same manner as for wire communication). *See also* Steere, *supra* note 28, at 232 (arguing that all forms of communications should be afforded the same level of protection).

[65] *See* Steere, *supra* note 28, at 232-46 (implying that the *Steve Jackson Games* decision might raise this constitutional issue); Sundstrom, *supra* note 4, at 2078-2102 (arguing that the Fourth Amendment puts a limitation on government workplace e-mail monitoring because there is a reasonable expectation of privacy). The constitutional protection of privacy requires a subjective expectation of privacy and a reasonable expectation of privacy. Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967)). The doctrine of a reasonable expectation of privacy is subject to certain limitations developed by case law. *See* Steere, *supra* note 28, at 242-46 (describing such limitations including: the lack of "the power to exclude others by exercising dominion and control;" the open field doctrine; the assumption of the risk of exposure to a third party). In addition to the constitutional claim, private parties may assert a tort cause of action for invasion of privacy. *See* Baum, *supra* note 4, at 1020. Raphael Winick describes the relationship between the constitutional requirement and the statutory requirement as follows:

> Since the protection offered by these statutes exceeds that afforded by the Fourth Amendment, a government action may be constitutionally acceptable, but still prohibited by these statutory requirements. Conversely, an action not expressly prohibited by statute may still be prohibited if it violates the [C]onstitution. Unlike the protection of the Fourth Amendment, these statutory prohibitions also apply to individuals not acting on behalf of the government.

Winick, *supra* note 64, at 89. The original Federal Wiretap Act is clearly based on the doctrine of a reasonable expectation of privacy, as is shown by its legislative history indicating that the Act was enacted in response to the *Katz* decision. *See* Bertron, *supra* note 64, at 166-67. For example, the definition of "oral communication" manifests the relevance of such a doctrine. *See* 18 U.S.C. § 2510(2) (1994) (defining "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*") (emphasis added). Wire and electronic communications are defined without reference to any privacy expectation, but are protected nevertheless. *See* 18 U.S.C. § 2510(1) (1994) (defining "wire communication" as "any aural transfer made . . . through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin

The ECPA includes Title I (the Federal Wiretap Act) and Title

---

and the point of reception . . . for the transmission of interstate or foreign communications"); 18 U.S.C. § 2510(12) (1994 & Supp. III 1997) (defining "electronic communication" as "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"). *See also* Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 354 (1995); Steere, *supra* note 28, at 269 n.246.

The justifications for a greater restriction for wiretapping are that all communications are subjected to the surveillance; the lack of particularity required by the Fourth Amendment (general searches); on-going intrusion (the duration); and the lack of notice to a suspect. *See* Dempsey, *supra* note 8, at 70-72. *See also supra* notes 51-52 and accompanying text (describing the original Federal Wiretap Act). With respect to accessing e-mail stored in a service provider computer, these elements are met even though such access is not contemporaneous with its transmission by a sender. *See* Winick, *supra* note 64, at 89. As between wire and electronic communications, the Senate Report does not make any distinctions about the needs for privacy protection. S. REP. No. 99-541, at 1-5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-59. The possible manners of government intrusion are also similar because the above four elements equally apply to wire and electronic communications. The underlying expectation of privacy does not change even if the e-mail message is temporarily stored in a service provider computer. *See supra* notes 3-4 and accompanying text (arguing that e-mail, even if temporarily stored before retrieved, enjoys a reasonable expectation of privacy). *See also* S. REP. No. 99-541, at 1-5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-59 (generally treating wire and electronic communications in the same manner, without singling out an unretrieved e-mail message stored in a service provider computer).

Because the term "wire communication" explicitly includes its "electronic storage," no one disputes that the stored wire communication enjoys privacy protection. The Senate Report did not make any distinctions between the stored e-mail and stored wire communication. *Id.* There is also nothing in the legislative history that indicates denial of a reasonable expectation of privacy in unretrieved e-mail stored in a service provider computer. Since there exists a reasonable expectation of privacy for unretrieved e-mail stored in a service provider computer, the *Steve Jackson Games* court's interpretation, in light of the *Katz* decision, raises the serious constitutional problem that government access not complying with the Title I requirements violates the Fourth Amendment. Such access deserves the greater protection under Title I (the Federal Wiretap Act). *See supra* note 52 and accompanying text (describing the protection afforded by the original Federal Wiretap Act).

II (the Stored Communications Act), with different restrictions and procedures applicable to each title.[66] Title I regulates the interception of e-mail as "electronic communication," and Title II applies to unauthorized access to a stored e-mail message.[67] The violation of Title I is, in most cases, punishable by a fine or imprisonment for not more than five years, or both.[68] The violation of Title II is punishable by a fine or imprisonment for not more than six months, or both.[69] Furthermore, civil remedies are available under both Titles I and II.[70] However, the government must obtain a court order to wiretap an electronic communication in accordance with the strict requirements under Title I (the Federal

---

[66] Title III of the ECPA prohibits the use of pen register and trap and trade devices without a court order. 18 U.S.C. §§ 3121-3126 (1994); S. REP. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. The Senate Report explains pen registers and trap and trace devices as follows:

> Pen registers are devices that record the telephone numbers to which calls have been placed from a particular telephone. These capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones. The same holds true for trap and trace devices, which record the numbers of telephones from which calls have been placed to a particular telephone.

Id. at 3564. Originally, the ECPA excluded from protection "the radio portion of a cordless telephone communication transmitted between the cordless handset and the base unit" because such a communication can be intercepted easily with an AM radio. *Id.* at 3566. However, that exclusion was deleted in 1994 by the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994).

[67] 18 U.S.C. §§ 2510, 2701 (1994 & Supp. III 1997).

[68] 18 U.S.C. § 2511(4)(a) (1994).

[69] 18 U.S.C. § 2701(b). In the case where there exists the aggravating factors, such as the commercial gain purpose and malicious destruction, the imprisonment term increases up to two years. *Id.*

[70] 18 U.S.C. § 2520 (1994); 18 U.S.C. § 2707 (1994 & Supp. III 1997). Under section 2520, compensatory damages as well as punitive damages are recoverable, together with a reasonable attorney's fee. 18 U.S.C. § 2520. The damages are the greater of (I) the sum of the actual damages and any profits made by the violator, or (II) statutory damages of greater of $100 a day or $10,000. *Id.* Under section 2707, compensatory damages as well as the punitive damages are recoverable, together with a reasonable attorney's fee. 18 U.S.C. § 2707. The damages include actual damages and any profits made by the violator, and will in no case be less than $1,000. *Id.*

Wiretap Act),[71] but may access a stored electronic communication by a search warrant in accordance with the less stringent procedures under Title II (the Stored Communications Act).[72] Accordingly, Title II affords significantly less protection than Title I against government intrusion.[73]

II. CASE LAW: *TURK*, *SMITH*, *STEVE JACKSON GAMES*, AND *WESLEY COLLEGE*

The Fifth Circuit in *Steve Jackson Games* held that access to unretrieved e-mail stored in a service provider computer was not an interception under Title I (the Federal Wiretap Act).[74] In so holding, the Fifth Circuit employed the narrow reading of the term "intercept" as used in *United States v. Turk*.[75] However, the *Turk* court's interpretation lacked sound basis either in the statutory

---

[71] 18 U.S.C. § 2518 (1994). The court order must not be "for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days." *Id.* Furthermore, the authorized interception must be conducted "in such a way as to minimize the interception of communications." *Id.*

[72] 18 U.S.C. § 2703 (1994 & Supp. III 1997) (providing that the government may access a stored electronic communication with a search warrant). *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 n.7 (5th Cir. 1994) (stating that government must obtain a court order under Title I in order to access a stored wire communication).

[73] *See* Leib, *supra* note 2, at 405-06. "[S]tored electronic communication is treated much like regular mail sent via the United States Postal Service." Leib, *supra* note 2, at 405.

[74] Steve Jackson Games, 36 F.3d at 460-64. In the ECPA, the term "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1994).

[75] 526 F.2d 654 (5th Cir. 1976). In *Turk*, "intercept" was construed as "requir[ing] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device." *Id.* at 658. In *Turk*, cassettes tapes containing a previously recorded telephone conversation were seized by police without a warrant. *Id.* at 656. The court required that an interception by definition be contemporaneous with the transmission of a telephone communication. *Id.* at 657. Thus, the seizure of the cassette tapes was held not to be an interception. *Id.* at 658.

language or the legislative history.[76] The Fifth Circuit in *Steve Jackson Games* also considered the absence of the term "electronic storage" in the definition of "electronic communication" as critical.[77] Such absence, the court concluded, implied that an interception of "electronic storage" of "electronic communication" was not covered under Title I (the Federal Wiretap Act).[78] Subsequent courts, including the court in *Wesley College v. Pitts*,[79] relied on *Steve Jackson Games*.[80] However, the Ninth Circuit, in *United States v. Smith*, recently rejected the *Turk* court's narrow interpretation of "intercept."[81] Furthermore, "electronic communication" impliedly covers the entire communication process—including its "electronic storage."[82] The *Steve Jackson Games* court's interpretation is also in contradiction of the

---

[76] *See infra* Part II.A, discussing the court's reasoning in *Turk*.

[77] *Steve Jackson Games*, 36 F.3d at 461-62. *See* 18 U.S.C. § 2510(12) (1994 & Supp. III. 1997) (defining "electronic communication" as "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").

[78] *Steve Jackson Games*, 36 F.3d at 461-62.

[79] 974 F. Supp. 375, 385-87 (D. Del. 1997) (holding that e-mail stored in a service provider computer is not subject to an interception under Title I).

[80] *See, e.g.*, United States v. Moriarty, 962 F. Supp. 217, 220-21 (D. Mass. 1997) (holding that listening to a stored voice mail message was not an interception because the defendant did not listen to the voice mail while it was recorded on the answering machine); Bohach v. City of Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (holding that the access to the messages stored in the computer paging system was not an interception); United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (holding that pressing the pager button to gain access to its message was not an interception because such access was not made while the message was being transmitted to the pager); Payne v. Norwest Corp., 911 F. Supp. 1299, 1303 (D. Mont. 1995) (holding that non-simultaneous recording of a voice mail message with a hand-held tape recorder was not an interception), *aff'd in part and rev'd in part*, 113 F.3d 1079 (9th Cir. 1997).

[81] 155 F.3d 1051, 1057-58 (9th Cir. 1998), *cert. denied*, 119 S. Ct. 804 (1999).

[82] *See infra* Part III.A, arguing that "electronic communication" impliedly includes "electronic storage."

Congressional intent that e-mail generally be protected in the same manner as a telephone communication.[83]

A. *Split Between the Fifth Circuit and the Ninth Circuit: Whether "Interception" Requires Contemporaneity with Transmission*

In *United States v. Turk*, the officers of the Dade County Public Safety Department stopped the suspects' car, based on a tip that they possessed cocaine and firearms.[84] After the officers

---

[83] *See supra* note 65 and accompanying text (arguing that Congress recognized a reasonable expectation of privacy for an electronic communication and intended to afford an electronic communication the same basic protection as a telephone communication under Title I of the ECPA (the Federal Wiretap Act)). One of the fallacies of the *Steve Jackson Games* court's interpretation is that it did not inquire into the issue of whether parties to unretrieved e-mail stored in a service provider computer enjoy a reasonable expectation of privacy. In order to conclude that its interpretation conforms with the purpose of Title I, the court, at a minimum, should have addressed this issue. The *Steve Jackson Games* court's reference to the legislative history of the ECPA mainly goes to the point that the *Turk* court's interpretation of "intercept" did not change by the enactment of the ECPA. 36 F.3d at 462. *See also Wesley College*, 974 F. Supp. at 387 (following the *Steve Jackson Games* court's view of the legislative history of the ECPA). That Congress did not intend to change the meaning of "intercept" does not necessarily mean that the *Turk* court's interpretation in a telephone communication case should be strictly followed in the different circumstance of an e-mail communication. *See supra* note 55 and accompanying text (arguing that the contemporaneity with transmission requirement should be liberally applied in an e-mail interception case). In addition, the *Steve Jackson Games* court, referring to the legislative history, argued that the substantial differences in requirements and procedures between Titles I and II show that Congress intended to apply Title I to an interception of stored e-mail. *Steve Jackson Games*, 36 F.3d at 463 n.8 (noting that section 2511(3) prohibits a service provider from disclosing the contents of an electronic communication while in transmission, while section 2702(a) prohibits a service provider from disclosing the contents of any communication while in electronic storage). However, such an interpretation is inconsistent with the legislative history and the overall structure of the ECPA. *See infra* notes 187-91 and accompanying text (arguing that such interpretation results in the failure to cover the prohibition of the disclosure of an electronic communication by a person other than a service provider).

[84] 526 F.2d 654, 656 (5th Cir. 1976).

discovered cocaine in the car and arrested the suspects, the officers also removed from the car a tape recorder and two cassette tapes.[85] The officers listened to the tapes at the station house.[86] As the court noted, "[t]hey soon realized that they were listening . . . to a recording of a private telephone conversation . . . . [and t]he officers continued to listen out of 'curiosity.'"[87] The issue before the court was whether the seizure and replaying of the cassette tapes was an "interception" under the original Federal Wiretap Act.[88]

The court held that an interception "require[d] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device."[89] The officers, who seized and listened to the tapes, were not involved in the recording of the tapes.[90] The suspect himself had recorded his previous telephone conversation in the tapes.[91] Thus, the seizure of the cassette tapes was not an interception prohibited under the original Federal Wiretap Act.[92] This interpretation, however, was not derived from a close reading of the statutory language. Rather, the *Turk* court looked to the legislative history of the statute to support its interpretation.[93]

---

[85] *Id.*

[86] *Id.*

[87] *Id.* at 656-57.

[88] *Id.* at 657. This case was decided in 1976, before the enactment of the ECPA. *Id.* at 654.

[89] *Id.* at 658. "[A]n 'interception' requires, at the least, involvement in the initial use of the device contemporaneous with the communication to transmit or preserve the communication." *Id.* at 658 n.3. At the time of *Turk* and before the enactment of the ECPA in 1986, "intercept" was defined in the original Federal Wiretap Act as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." *Id.* at 657. The ECPA differs from the original Act by its use of "aural" instead of "aural or other" and its reference to "electronic communication." *See supra* note 51 and accompanying text (delineating the language of the current version of section 2510(4)).

[90] *Turk*, 526 F.2d at 656.

[91] *Id.*

[92] *Turk* was decided before the 1986 enactment of the ECPA. *Id.* at 654.

[93] *See id.* at 658-59 (citing S. REP. No. 90-1097, at 90 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2178).

Primarily, the court noted in evaluating Title I that "[t]he words 'acquisition . . . through the use of any . . . device' suggest that the central concern is with the activity engaged in at the time of the oral communication which causes such communication to be overheard by uninvited listeners."[94] Furthermore, the court pointed to the policies reflected in the legislative history and stated that the specific focus of the statute was wiretapping and electronic surveillance.[95] In other words, the contemporaneity element of an interception was merely based on the court's presumption that the interception meant wiretapping, which is not defined anywhere in the statute.[96] Even if the court presumed that wiretapping a telephone communication required its contemporaneous acquisition with transmission, it does not lead to the conclusion that wiretapping e-mail also requires the contemporaneity with transmission because access to unread e-mail does not require contemporaneity with its transmission.[97] Therefore, the contemporaneity element did not have sound basis either in the statutory language or the

---

[94] *Id.* at 658.

[95] *Id.* at 659 ("[A]ct of surveillance and not the literal 'aural acquisition' (i.e., the hearing), which might be contemporaneous with the surveillance, or might follow therefrom, was at the center of congressional concern."). Although the *Turk* court looked to the reference to a device in the definition of "intercept," the element of the contemporaneity with a communication and the participation by police in the initial acquisition of the contents of a communication are primarily derived from the court's understanding of the statutory purpose that wiretapping is the designed objective of the prohibition. It should be noted that limiting the term "intercept" to a vague concept of the wiretapping activity does not necessarily require the acquisition of a communication strictly contemporaneous with transmission. The court merely attempted to describe wiretapping in the context of a telephone communication, which is different from e-mail in that the acquisition of a telephone communication is possible only while in transmission. Thus, the *Steve Jackson Games* court should not have used the same reading for an e-mail communication.

[96] *See supra* note 51 and accompanying text (stating that the word "wiretapping" is not used in the substantive provisions of the ECPA).

[97] *See supra* note 18 and accompanying text (describing the e-mail communication process). *See also supra* note 30 and accompanying text (arguing that requiring contemporaneity renders an interception of e-mail under Title I virtually impossible).

legislative history.[98] In fact, the court conceded that the defendant's interpretation—that an interception included the seizure and replaying of an audio tape of a prior telephone conversation—was a conceivable reading.[99] Moreover, the court acknowledged that "[n]o explicit limitation of coverage to contemporaneous 'acquisitions' appears in the [the original Federal Wiretap Act]."[100] Accordingly, the *Turk* court should not have created its own narrow interpretation of "intercept." Rather, the court could simply have reasoned that the telephone communication ended when police seized and listened to the tape of the telephone conversation.[101]

---

[98] In essence, the *Turk* court attempted to limit the meaning of "acquisition" to obtaining the contents of a communication using a device. *See supra* notes 94-95 and accompanying text (describing the *Turk* court's interpretation of "intercept"). Acquiring the contents of unretrieved e-mail messages stored in a service provider computer clearly satisfies this limitation. Thus, the contemporaneity with the communication, stated by the *Turk* court, need not be strictly understood as the acquisition while in transmission.

[99] *Turk*, 526 F.2d at 657.

[100] *Id.* at 658.

[101] In *Turk*, police were not involved in the initial recording of the telephone conversation. *Id.* at 656-57. *See id.* at 658 (emphasizing that the "central concern is with the activity"). *See also supra* note 93 and accompanying text (arguing that the *Turk* court's interpretation of "intercept" does not necessarily require the acquisition while in transmission). Furthermore, because the contemporaneity requirement for an interception was developed for a telephone wiretapping in *Turk*, such a requirement should not have been carried over to a situation involving e-mail. *See* Bertron, *supra* note 64, at 183-84. In a telephone wiretapping, an interception must be contemporaneous with the conversation in order to acquire its contents. In contrast, e-mail need not be wiretapped while it is transmitted, because the message is stored in a service provider computer. *See supra* note 3 and accompanying text (describing the e-mail communication process). Megan Connor Bertron, cited in *Wesley College*, compares first class mail, a telephone and e-mail by noting that:

> Unlike telephone transmissions, which involves simultaneous discussion, both e-mail and regular mail generally involve some delay between transmission and reception . . . . [B]oth first class mail and e-mail wait for the recipient if she is not at home and can be read by the recipient on her own time. . . . [U]nlike telephone communications, the content [of an e-mail or first class mail] is not lost as soon as the user hangs up. . . . [E]-mail and telephones are much less comparable.

Recently, the Ninth Circuit, in *United States v. Smith*, rejected the Fifth Circuit's narrow interpretation of "intercept" and held that an interception does not have to be contemporaneous with the transmission.[102] In *Smith*, the defendant, who was an executive at a software design firm, left his colleague a voicemail message indicating that the defendant engaged in insider trading.[103] Another employee of the firm ("Gore"), without authorization, retrieved the message and recorded it with a handheld tape recorder.[104] Gore gave the tape to her co-worker, who then informed government of the contents of the tape.[105] The defendant was convicted of insider trading.[106] One of the issues before the court was whether Gore's conduct amounted to an interception of a wire communication under Title I of the ECPA (the Federal Wiretap Act).[107] The district court answered the question in the affirmative and suppressed the evidence of the voicemail message, though the conviction was also based on other evidence.[108] The Ninth Circuit agreed with the district court that Gore's conduct constituted "interception" under Title I.[109]

The Ninth Circuit rejected the *Turk* court's narrow interpretation of "intercept" requiring contemporaneity with transmission, because the definition of "intercept" does not contain the contemporaneity limitation, but rather is "broad enough to encompass Gore's conduct."[110] The court, rejecting the use of a dictionary meaning of "intercept," noted that "[w]hen, as here, the meaning of a word is clearly explained in a statute, courts are not at liberty to look beyond the statutory definition."[111] Moreover, the court stated that inclusion of the contemporaneity element in the

---

Bertron, *supra* note 64, at 183-84 (footnote omitted).

[102] 155 F.3d 1051, 1057-58 (9th Cir. 1998), *cert. denied*, 119 S. Ct. 804 (1999).

[103] *Id.* at 1053.

[104] *Id.* at 1054.

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.* at 1059.

[110] *Id.* at 1055-58.

[111] *Id.* at 1057 (quoting Calautti v. Franklin, 439 U.S. 379, 393 (1979)).

definition of "intercept" renders the prohibition of an intercept of a wire communication in electronic storage under Title I essentially meaningless, because the stored message cannot be acquired contemporaneously.[112]

B. *"Interception" and "Electronic Communication" in Steve Jackson Games, Inc. v. United States Secret Service*

In *Steve Jackson Games*, the operator and users of an electronic bulletin board system ("BBS") sued the United States Secret Service ("Secret Service") for violation of the ECPA.[113] The plaintiffs alleged that the Secret Service, without authorization, seized and read the e-mail messages stored in a service provider computer in connection with a search of the operator's premises.[114] The search was conducted to seize evidence of unauthorized access to a telephone company's computer files, and the unauthorized distribution of such information on the BBS.[115] However, the BBS also provided an e-mail service to the operator's customers.[116] The hard disk of the BBS computer temporarily stored e-mail messages addressed to the customers, who were to access the BBS computer in order to retrieve their messages.[117] The Secret Service seized the computer operating the

---

[112] *Id.* at 1058.

[113] Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 459 (5th Cir. 1994).

[114] *Id.*

[115] *Id.* at 459. The search warrant authorized:

> [T]he seizure of, *inter alia*, [c]omputer hardware . . . and computer software . . . and . . . documents relating to the use of the computer system . . . , and financial documents and licensing documentation relative to the computer programs and equipment . . . which constitute evidence . . . of federal crimes. . . . This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained in the above described computer and computer data.

Id.

[116] *Id.* at 458.

[117] *Id.*

BBS.[118] This computer contained "162 items of unread, private E-mail . . . stored on the BBS,"[119] which were read by the Secret Service.[120]

The district court held that the Secret Service violated Title II (the Stored Communications Act) and awarded $1,000 to each individual plaintiff, but denied the government's liability under Title I (the Federal Wiretap Act).[121] The Fifth Circuit affirmed the district court's judgment.[122] The Fifth Circuit, relying on *Turk*, reasoned that the acquisition of the contents of an electronic communication was not contemporaneous with their transmission, and thus, was not unlawful under Title I (the Federal Wiretap Act).[123]

However, *Turk* and *Steve Jackson Games* are distinguishable in one critical aspect. In *Turk*, police seized cassette tapes of a suspect found in his car without a warrant.[124] These tapes contained a private telephone conversation made by the defendant that he recorded previously.[125] Thus, the telephone communication had ended and had been recorded in the cassette tapes when police seized and listened to them.[126] On the other hand, in *Steve Jackson Games*, the e-mail messages were not received by their intended addressees.[127] The Fifth Circuit in *Steve Jackson Games*, however, failed to discuss such a difference.[128]

---

[118] *Id.* at 459.

[119] *Id.*

[120] *Id.*

[121] *Id.* at 459-60. The district court reasoned that "the Secret Service did not intercept the communications, because its acquisition of the contents of those communications was not contemporaneous with their transmission." *Id.* at 460.

[122] *Id.* at 464.

[123] *See id.* at 460.

[124] United States v. Turk, 526 F.2d 654, 656 (5th Cir. 1976).

[125] *Id.* at 656-57.

[126] *Id.*

[127] *Steve Jackson Games*, 36 F.3d at 459.

[128] *Id.* at 460-61. The court's real difficulty may be in drawing a line between a more serious invasion to "electronic storage" of "electronic communication" (for example, wiretapping e-mail stored in a service provider computer) and a less serious one (for example, seizure of a floppy disk containing prior e-mail messages recorded by its owner-receiver), because both cases do not involve participation by police in an initial storage of e-mail transmission. In

The term "intercept" is defined in the ECPA 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."[129] This definition may be divided into three parts: (1) an acquisition of the contents; (2) of a wire, electronic, or oral communication; and (3) through the use of a device. Of these three parts, (1) and (2) are relevant to the issue of whether access to e-mail stored in a service provider computer is an interception under Title I (the Federal Wiretap Act). As stated in *United States v. Smith*,[130] an "acquisition of the contents" is the term broad enough to encompass the access to a stored e-mail message,[131] and thus, an "intercept" need not be simultaneous with the transmission.[132]

Thomas R. Greenberg, cited in *Wesley College*, nevertheless argues that an "intercept" means "'interrupt the progress or course of,'" citing a dictionary meaning.[133] Thus, "the acquisition of a

---

fact, the Fifth Circuit in *Wesley College* used the seizure of a computer disk containing "electronic communication" as an example of a troublesome case to apply the stringent requirements under Title I of the ECPA (the Federal Wiretap Act). Wesley College v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997). However, such difficulty is overstated, because in both cases there exists the risk of general searches, which is the very concern under the Federal Wiretap Act. At a minimum, the court could have differentiated the recorded cassette tapes in *Turk* from the unread (unretrieved) e-mail messages stored in a service provider computer. The latter case may easily be analogized to a telephone message in the process of communication (for example, a message recorded in an answering machine). One possible factor to differentiate the requirements under the ECPA is that the unread (unretrieved) e-mail message stored in a service provider computer is part of a communication process, though necessarily is not in "electronic storage."

[129] 18 U.S.C. § 2510(4) (1994).

[130] 155 F.3d 1051, 1055-59 (9th Cir. 1998), *cert. denied*, 199 S. Ct. 804 (1999).

[131] *See infra* note 200 and accompanying text (discussing the term "intercept").

[132] *See supra* note 98 and accompanying text (arguing that the *Turk* court does not require strict contemporaneity with transmission for an interception).

[133] *See* Greenberg, *supra* note 4, at 248 (citing WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1176 (1986)). Greenberg's interpretation was cited in *Wesley College* as an example of the endorsement of the court's interpretation by commentators. *See* 974 F. Supp. at 388 n.12.

wire, oral, or electronic communication will constitute an 'interception,' only while being transmitted."[134] However, another commentator interprets the word "intercept" differently,[135] asserting that an intercept means "'(1) to prevent and hinder; (2) to stop, seize, or interrupt in progress or course or before arrived; or (3) to interrupt communication, or connection with.'"[136] Alternatively, she argues, that "'interception' is the 'taking or seizure by the way or before arrival at destined place.'"[137] Thus, she concludes that the Secret Service intercepted the e-mail, because they seized it "before the intended recipients took control."[138] Accordingly, the search for the common meaning of "intercept" by resorting to a dictionary definition is not conclusive.[139] To say the least, the language of the definition does not compel the interpretation adopted by the *Steve Jackson Games* court.

With respect to the second part of the definition of "intercept" under the ECPA, the Fifth Circuit in *Steve Jackson Games* considered the differences between "wire communication" and "electronic communication" as critical.[140] While the definition of "wire communication"[141] includes "electronic storage," the

---

[134] Greenberg, *supra* note 4, at 248.

[135] *See* Giallonardo, *supra* note 28, at 185, 203-04.

[136] Giallonardo, *supra* note 28, at 185 (citing WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 630 (1988)).

[137] Giallonardo, *supra* note 28, at 185 (citing BLACK'S LAW DICTIONARY 811 (6th ed. 1990)).

[138] Giallonardo, *supra* note 28, at 185.

[139] *See* MCI Telecomm. Corp. v. American Tel. & Tel. Co., 512 U.S. 218, 240 (1994) (Stevens, J., dissenting) ("Dictionaries can be useful aids in statutory interpretation, but they are no substitute for close analysis of what words mean as used in a particular statutory context.").

[140] Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994).

[141] The ECPA defines "wire communication" as:

> [A]ny 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 between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign

definition of "electronic communication" does not include "electronic storage."[142] In essence, the *Steve Jackson Games* court stated that the absence of any reference to "electronic storage" in the definition of "electronic communication" suggested that the interception does not apply to a stored "electronic communication."[143] Thus, the court held that Title I (the Federal Wiretap Act) does not apply to a stored "electronic communication," such as e-mail stored in a service provider computer.[144] However, mere absence of the reference to "electronic storage" does not necessarily mean that it is excluded from the meaning of "electronic communication."[145] In other words, if the meaning of

---

communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.

18 U.S.C. § 2510(1) (1994).

[142] In contrast, the ECPA defines "electronic communication" as:

[A]ny 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—(A) any wire or oral communication; . . . (D) 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 & Supp. III 1997). "Electronic storage" is defined as:

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) 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).

[143] *Steve Jackson Games*, 36 F.3d at 460-62. The court also reasoned that the use of the word "transfer" in "electronic communication" supports its interpretation. *Id.* However, "transfer" is used in the ECPA as covering the entire process of communication from the message's origin to its receipt by an addressee. *See infra* note 208 and accompanying text (arguing that "transfer" as used in the ECPA is broader in meaning to cover the entire communication process, including its incidental storage).

[144] *Steve Jackson Games*, 36 F.3d at 460-62.

[145] *See* discussion *infra* Part III.A.

"electronic communication" is broad enough to encompass "electronic storage," it is not necessary to add the reference to "electronic storage." Similarly, even if the definition of "wire communication" contains a specific reference to "electronic storage," it does not necessarily lead to the conclusion that the absence of the same reference in the definition of "electronic communication" implies the exclusion of "electronic storage" from that definition. The reference in the definition of "wire communication" is instead designed to clarify that "wire communication" includes storage of an *electronic* nature.[146]

Moreover, the court's argument presupposes that an interception occurs only while in transmission. As stated in *United States v. Smith*, contemporaneity is not required for an interception.[147] In fact, the reasoning of the court in *Steve Jackson Games* does not require that the definition of "electronic communication" exclude "electronic storage," because an intercepting activity itself, as the court interpreted, excludes access to "electronic storage."[148] Accordingly, the absence of any reference to "electronic storage" in the definition of "electronic communication" does not compel the court's interpretation that access to e-mail stored in a service provider computer is not subject to the Title I (Federal Wiretap Act). Since the definition of "electronic communication" is applicable to Titles I and II,[149] it is more consistent with the structure of the ECPA to read that "electronic communication" includes its storage.[150] The court's assumption that "electronic communication" excludes "electronic storage," unless the

---

[146] *See* discussion *infra* Part III.B.

[147] 155 F.3d 1051, 1057-58 (9th Cir. 1998), *cert. denied*, 119 S. Ct. 804 (1999).

[148] *See Steve Jackson Games*, 36 F.3d at 460.

[149] Section 2711 of Title II incorporates the definitions in section 2510, and thus, the definitions in section 2510 are used both for Titles I and II. 18 U.S.C. § 2711 (1994). There is no separate definition of "electronic communication" for Title II only.

[150] *See* discussion *infra* Part III.A, arguing that "electronic communication" impliedly covers "electronic storage".

definition expressly includes the storage, contradicts the structure of the ECPA.[151]

The Fifth Circuit in *Steve Jackson Games* cited the differences of requirements and procedures between Titles I and II as an additional reason to deny the application of Title I (the Federal Wiretap Act) to "electronic storage" of "electronic communication."[152] First of all, the court concluded that Title II (the Stored Communications Act) clearly applies to the Secret Service's conduct in the case.[153] The court proceeded to state that the conduct prohibited under Title II is "most unlikely" to be covered by Title I, because there are substantial differences between both titles.[154] However, the court's reasoning cannot explain why Title I should not be applicable to an interception of a stored "electronic communication."[155]

---

[151] *See* discussion *infra* Part III.A, arguing that "electronic communication" impliedly covers "electronic storage." The task of statutory interpretation begins with examination of the language of the statute. *See* Mead Corp. v. Tilley, 490 U.S. 714, 722 (1989). However, the language of the statute should be understood in context, examining the statutory language as a whole and taking into consideration the overall statutory structure. *See* United States Nat'l Bank of Or. v. Independent Ins. Agents of Am., Inc., 508 U.S. 439, 455 (1993) (quoting United States v. Heirs of Boisdore, 49 U.S. (8 How.) 113, 122 (1849)); Offshore Logistics, Inc. v. Tollentire, 477 U.S. 207, 220-21 (1986). The flaw in the *Steve Jackson Games* court's analysis is that it examined only "intercept," "electronic communication" and "wire communication," without taking into consideration other related terms, such as "electronic storage" and "electronic communication system." *Steve Jackson Games*, 36 F.3d at 461-62. *See infra* discussion in Part III.A, arguing that "electronic communication" impliedly includes "electronic storage" in view of the context and structure of the statute as a whole.

[152] *Steve Jackson Games*, 36 F.3d at 464.

[153] *Id.*

[154] *Id.* Those differences cited by the court include: (1) a court order requirement under Title I and a warrant requirement under Title II; and (2) the minimization, duration and types of crimes requirements in the court order under Title I. *Id. See also* 18 U.S.C. §§ 2516, 2518(5) (1994).

[155] Moreover, Title II was not intended to address the issue of the interception of the ongoing electronic communication process. *See supra* note 56 and accompanying text (arguing that Congress intended, by the addendum of Title I, to deal with the interference with the computerized recordkeeping system, such as computer database and remote data processing services).

The Fifth Circuit in *Steve Jackson Games* also suggested that e-mail stored in a service provider computer was less subject to invasion of privacy than a telephone wiretap.[156] The court reasoned that, unlike the case of an interception of "electronic communication" in transmission, law enforcement can avoid accessing unrelated communications in the case of a stored electronic communication by using "key word searches."[157] Thus, noted the court, the risk of access to unrelated communications by law enforcement is minimal in the case of a stored electronic communication.[158] However, the Fifth Circuit pointed to the district court's finding that the Secret Service read all the messages despite its contrary contention that it used "key word searches."[159] Hence, there is no assurance that a stored electronic communication is not subject to the risk of general searches by the government.[160]

---

[156] *Steve Jackson Games*, 36 F.3d at 463.

[157] *Id.* "The key word search might include the names of suspected participants, important dates, places of events surrounding the crime under investigation, and other words likely to be found in the relevant communications." Bertron, *supra* note 64, at 189 n.175.

[158] *Steve Jackson Games*, 36 F.3d at 463.

[159] *Id.*

[160] "Although [listening to all calls] may be a necessary evil when tapping a telephone because the contents otherwise will be lost forever, this rationale does not apply to e-mail transmissions, and monitoring officers should never be allowed to read all messages received on a suspect's e-mail account." Bertron, *supra* note 64, at 188. Bertron, cited in *Wesley College*, also notes that:

> Ideally, to meet the particularity requirement of Fourth Amendment search warrants, officers should have probable cause to believe that a particular e-mail communication contains evidence of crime. When this level of particularity cannot be met, however, officers applying for warrants to search electronic mail should be required to describe a key word search that will be used to sift through the suspect's e-mail. By using key word searches, the common abuse of telephone wiretaps—i.e., listening to every conversation that passes through the phone line—can be avoided.

Bertron, *supra* note 64, at 189 (footnote omitted). However, as the finding of the district court in *Steve Jackson Games* indicates, there is no assurance that the "key word search" is always enough, and thus, there remains the necessity for regulating an interception of e-mail messages. Furthermore, it is easily

In addition, there is no guarantee that the "key word search" is an effective technology to prevent government access to unrelated communications. Even if such technology becomes available in the future, there remains the same level of the risk, unless the use of such technology is mandated by the ECPA.[161] The very necessity of such a restriction shows that access to a stored electronic communication requires stringent protection, as in the case of an interception of an electronic communication in transmission. It should be noted that the Supreme Court in *Katz* stressed that privacy interests are best protected from governmental invasions through an independent judicial process.[162] The Court rejected the government's argument that self-restraint by the government was sufficient.[163]

C. *An Examination of Statutory Language in Wesley College v. Pitts*

In *Wesley College v. Pitts*,[164] the plaintiff college sued a former computer maintenance employee and others for violation of Titles I and II of the ECPA.[165] The defendant allegedly had

---

conceivable that criminals may possibly disguise their messages to avoid the chance of detection by using symbols or encryption technologies. The Senate Report does not discuss the use of the "key word search." S. REP. No. 99-541, at 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585. The Senate Report only notes, "the minimization [of wiretapping] should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete all non-relevant materials and disseminate to other officials only that information which is relevant to the investigation." *Id.*

[161] A court order mandating the use of the "key word search" in accord with the particularity requirement under the Fourth Amendment may also suffice.

[162] Katz v. United States, 389 U.S. 347, 357 (1967).

[163] *Id.* at 356.

[164] 974 F. Supp. 375 (D. Del. 1997).

[165] *Id.* at 377. In the cases of governmental seizure, such as *Steve Jackson Games*, access to the unread (unretrieved) e-mail messages was made incidental to the execution of the search warrant for other items. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 459 (5th Cir. 1994). The e-mail messages were stored in the e-mail service provider's computer, which was covered by the search warrant (although the e-mail messages were not covered

unauthorized access to e-mail messages stored in the college's mainframe computer.[166] The court held that such access did not constitute an interception under Title I (the Federal Wiretap Act) because the access was not contemporaneous with the transmission of the e-mail messages.[167]

---

by the warrant). *Id.* The court in *Steve Jackson Games* applied Title II and found the government liable, but denied the government liability under Title I. *Id.* at 459-60. Thus, in *Steve Jackson Games*, the extent of the invasion of privacy interest was somewhat confined as the court analogized its case to the seizure and listening to the audio tapes not covered by a search warrant. *Id.* at 460. However, in *Wesley College*, there was no such unique situation. The defendant employee, who was responsible for the maintenance of the plaintiff's computer system, was sued for reading e-mail messages in the computer without authorization. *Wesley College*, 974 F. Supp. at 377-80.

[166] *Wesley College*, 974 F. Supp. at 377-80.

[167] *Id.* The court stated that "[such] conclusion has been endorsed, either implicitly or otherwise, by commentators." *Id.* at 388 n.12. For example, the court quoted Thomas R. Greenberg as stating:

> [T]he stored communications provisions of [section] 2701 prohibit the unauthorized accessing of wire or electronic communications once stored. While the distinction between the terms "intercept" and "access" has little significance for forms of communication that only exist as transmissions, and are never stored, the distinction is critical when a transmitted communication is later electronically stored, because it is at the time of storage that a communication becomes subject to different provisions of the ECPA. This is the case with both E-mail and voice-mail messages, both of which have a transmission phase and a storage phase. During the transmission phase, any protection against unlawful interception under [the ECPA] is governed by [section] 2511. On arrival in storage, the same messages are subject to [section] 2701.

Id. (alterations in original) (quoting Greenberg, *supra* note 4, at 248). However, Greenberg bases his conclusion on the assumption that the term "intercept" must be narrowly construed to mean "interrupt the progress or course of," citing an English dictionary. *See* Greenberg, *supra* note 4, at 248. *See also supra* note 133 and accompanying text (citing the dictionaries quoted by Greenberg). However, Greenberg acknowledges that such a construction results in an "irrational result" and "an insupportable result given Congress' emphasis of individual privacy rights during passage of the ECPA." Greenberg, *supra* note 4, at 249. The court in *Wesley College* also cited Gregory L. Brown, who describes *Steve Jackson Games* as "correct in its reasoning and holding." *Wesley College*, 974 F. Supp. at 388. *See also* Brown, *supra* note 28, at 1390.

The plaintiff argued that access to e-mail stored in a service provider computer is an interception.[168] The plaintiff asserted that "electronic communication" and "wire communication" focus on "the manner in which a communication is transmitted," not "the meaning of a 'communication.'"[169] In other words, "a communication does not cease being a communication after it is transmitted," and "[t]here is no temporal limitation on the acquisition of a communication in the definition of intercept."[170] Thus, the plaintiff argued that such language evinced that Congress did not intend to limit "interception" to the access simultaneous with transmission.[171]

Moreover, the plaintiff argued that Titles I and II were overlapping and interconnected.[172] Thus, the difference in requirements and procedures between Titles I and II cannot justify denying the application of Title I to a stored electronic communication.[173] The plaintiff reasoned that Title II is a lesser included offense of Title I for a stored electronic communication; that is, Title I requires acquisition of the contents of "electronic communication," while Title II prohibits mere access, without authorization, to a stored electronic communication.[174] The court, however,

---

However, Brown does not give a reason why the court's reasoning and holding are correct. *See* Brown, *supra* note 28, at 1389-91. Instead, Brown makes the point that the court's reasoning and conclusion result in an undesirable interpretation and warns that a constitutional claim under the Fourth Amendment is likely to arise in the future. *See* Brown, *supra* note 28, at 1390-91.

[168] *Wesley College*, 974 F. Supp. at 386.

[169] *Id.*

[170] *Id.*

[171] *Id.*

[172] *Id.* at 388-89.

[173] *Id.* at 388.

[174] *Id.* at 388-89. The Fifth Circuit in *Wesley College* referred to the same argument made by the government in *United States v. Moriarty*. *Wesley College*, 974 F. Supp. at 389 n.13 (citing Moriarity, 962 F. Supp. 217, 219 (D. Mass. 1997). The government in *Moriarty* gave an example as follows: "[A] person could violate [Title II] by entering the Justice Department's computer system and altering the codes that would allow access to e-mail by authorized users. This would be a violation even though confidential e-mail messages were never intercepted. Such contact would not violate [Title I]." *Id.* (second and third alteration in original). The *Moriarty* court did not resolve this issue. *Id.* The

rejected this argument because the plaintiff lacked support for its reasoning.[175]

Yet, the Ninth Circuit, in *United States v. Smith*, agreed with the plaintiff's position.[176] The court stated that "[t]he word 'intercept' entails *actually* acquiring the contents of a communication, whereas the word 'access' merely involves *being in position* to acquire the contents of a communication."[177] Thus, "'access' is a lesser included offense . . . of 'intercept[ion].'"[178] The court reasoned that "[b]oth textual and structural considerations support our interpretation."[179] First, the court's interpretation "comports with the statutory definition of 'intercept' as entailing actual 'acquisition,' . . . and with the ordinary meaning of 'access[]'

Fifth Circuit in *Wesley College* also left the issue open. *Id.* However, the Ninth Circuit, in *United States v. Smith*, answered the question affirmatively. 155 F.3d 1051, 1058-59 (9th Cir. 1998), *cert. denied*, 119 S. Ct. 804 (1999).

[175] *Wesley College*, 974 F. Supp. at 389 (stating "[the plaintiff] has pointed to no authority or legislative history to indicate Congress intended such a result"). *See also* S. REP. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (stating that the focus of Title II is "the advent of computerized recordkeeping system"). The Senate Report also notes that:

> [T]he providers of electronic mail create electronic copies of private correspondence for *later reference*. . . . [O]ften [the information] is maintained for approximately 3 months to ensure system integrity. For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist unauthorized access to communications.

Id. (emphasis added) (citation omitted). Title II seems to cover the special case of recordkeeping in the control of a third party, supplementing the primary protection under Title I. *See supra* note 56 and accompanying text (discussing the coverage of Title II).

[176] 155 F.3d 1051, 1058-59 (9th Cir. 1998), *cert. denied*, 119 S. Ct. 804 (1999).

[177] *Id.* at 1058 (emphasis in original).

[178] *Id.* (alteration and emphasis in original).

[179] *Id.*

(which is not statutorily defined) as meaning 'to get at' or to 'gain access to.'"[180] Second, "whereas the language of § 2701 refers broadly to accessing a communication's 'facility,' § 2515 refers more pointedly to intercepting the 'wire . . . communication' itself."[181] Third, the court explained that its interpretation was consistent with the stiffer criminal and civil liabilities under Title I.[182] Fourth, the absence of a statutory exclusionary rule for Title II conforms to the interpretation that Title II deals with only access, and thus the mere possibility of acquiring the contents of a communication.[183]

The plaintiff in *Wesley College* also argued that Titles I and II overlapped because the definition of "wire communication" includes "electronic storage."[184] In fact, the court conceded that there may be overlap between the two titles as to "wire communication," but countered that it does not necessarily show that a similar overlap exists for "electronic communication."[185] However, the plaintiff's point, at a minimum, significantly weakens the court's argument that the differences between requirements in Titles I and II require denial of the application of Title I to the "electronic communication" in storage, because the same argument can be made for "wire communication."[186]

Moreover, the plaintiff asserted that if Title I is not applicable to a stored electronic communication, the disclosure of the contents of an electronic communication by a private person, other than a service provider, may not be punished under either Title I or Title II.[187] In other words, Title I prohibits disclosure of the contents of an electronic communication, but does not specifically refer to

---

[180] *Id.* (citing WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 49 (1986)) (alteration in original).

[181] *Id.* at 1059.

[182] *Id.*

[183] *Id.*

[184] 974 F. Supp. 375, 389 (D. Del. 1997).

[185] *Id.*

[186] Despite the differences between the requirements in Titles I and II, both titles apply to "wire communication" while in "electronic storage." 18 U.S.C. §§ 2511, 2701 (1994 & Supp. III 1997).

[187] *Wesley College*, 974 F. Supp. at 388.

such disclosure of a *stored* electronic communication.[188] Further, Title II prohibits the disclosure of a stored electronic communication made only by a service provider.[189] Thus, unless Title I encompasses a stored electronic communication, a person, other than a service provider, who discloses the contents of a stored electronic communication may not be punishable under the ECPA. The court, while acknowledging the gap to be troubling, simply stated that it was a matter to be addressed by Congress.[190] However, a settled canon of statutory interpretation is that the literary interpretation must be avoided when it results in an absurd result.[191] Here, the court bluntly ignores the absurd result without justification.

Furthermore, the contemporaneity requirement of the interception has led other courts, which followed the requirement mechanically, to the undesirable conclusion.[192] For example, in *United States v. Moriarty*, the court held that listening to a stored voice mail message was not an interception because the defendant did not listen to the voice mail while it was recorded on the answering machine.[193] Similarly, in *United States v. Reyes*, the court held that pressing the pager button to gain access to its message was not an interception because such access was not made while the message was being transmitted to the pager.[194] Further, in *Payne v. Norwest Corp.*, the non-simultaneous recording of a voice mail message with a handheld tape recorder was held not to be an

---

[188] 18 U.S.C. § 2511(3) (1994).

[189] 18 U.S.C. § 2702(a) (1994).

[190] *Wesley College*, 974 F. Supp. at 389.

[191] *See* United States v. Ron Pair Enter., Inc., 489 U.S. 235, 242 (1989) (quoting Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 571 (1982)); Hughey v. JMS Dev. Corp., 78 F.3d 1523, 1529 (11th Cir. 1996).

[192] *See supra* note 29 and accompanying text (discussing that a consequence of the *Steve Jackson Games* decision is the tendency of the police to circumvent Title I by accessing stored communications).

[193] 962 F. Supp. 217, 220-21 (D. Mass. 1997) (citing *Steve Jackson Games'* contemporaneity requirement).

[194] 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (citing *Steve Jackson Games'* contemporaneity requirement).

interception.[195] Finally, in *Bohach v. City of Reno*, the access to the messages stored in the computerized paging system was held not an interception, because such an access was not contemporaneous with the transmission.[196]

III. AN ALTERNATIVE STATUTORY INTERPRETATION MORE CONSISTENT WITH THE OVERALL STRUCTURE OF THE ECPA

The courts in *Steve Jackson Games* and *Wesley College* failed to examine in detail the meaning of the critical term "electronic storage," and therefore misunderstood the relationship between "electronic storage" and "electronic communication." "Electronic storage" is a part of the entire 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."[197] The inclusion of the reference to "electronic storage" in the definition of "wire communication" does not mean that the word "communication" excludes "storage." The reason why "wire communication" requires the reference to "electronic storage" is that although "wire communication" might cover its *wire* storage as part of the entire communication process, it is not clear whether "wire communication" includes storage of an *electronic* nature, without the reference to "electronic storage."[198] Accordingly, the absence of the explicit reference to "electronic storage" in "electronic communication" does not support the interpretation of the Fifth Circuit in *Steve Jackson Games* that "electronic communication"

---

[195] 911 F. Supp. 1299, 1303 (D. Mont. 1995) (citing *Steve Jackson Games'* contemporaneity requirement), *aff'd in part and rev'd in part*, 113 F.3d 1079 (9th Cir. 1997).

[196] 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (following the *Steve Jackson Games* court's reasoning).

[197] *See* discussion *infra* Part III.A, arguing that "electronic communication" impliedly covers "electronic storage".

[198] *See infra* Part III.B, discussing the function of the reference to "electronic storage" in the definition of "wire communication" in the overall statutory structure.

does not include "electronic storage."[199] To the contrary, "electronic communication" impliedly includes "electronic storage," and thus, Title I (the Federal Wiretap Act) applies to e-mail stored in a service provider computer.[200]

A. The Term "Electronic Communication" Impliedly Covers "Electronic Storage"

The meaning of "electronic storage" is important because the Fifth Circuit in *Steve Jackson Games* considered the absence of that term in the definition of "electronic communication" as determinative of the nonapplicability of Title I (the Federal Wiretap Act) to an interception of e-mail stored in a service provider computer.[201] The term "electronic storage" is defined in the ECPA basically as "a temporary, intermediate storage of a

---

[199] *See infra* Part III.A, arguing that "electronic communication" impliedly covers "electronic storage".

[200] *See infra* Part III.B (discussing the function of the reference to "electronic storage" in the definition of "wire communication" in overall statutory structure). In the ECPA, the term "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1994). Since the acquisition of the contents of e-mail messages does not necessarily require simultaneous access with the transmission of e-mail, the definition of "intercept" is broad enough to include access to e-mail stored in a service provider computer. *See id.* Such a broadly written definition of "electronic communication" should be given liberal construction to be consistent with Congressional intent. *See supra* note 55 and accompanying text (arguing that Congress intended liberal construction of the term "electronic communication"). When Congress intended to exclude certain electronic communications, Congress added explicit clauses for the exceptions at the end of the broad definition of "electronic communication." 18 U.S.C. § 2510(12) (1994 & Supp. III 1997) (defining "electronic communication," following the substantive descriptive words, as "not includ[ing]—(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device . . . ; or (D) electronic funds transfer information stored by a financial institution in a communication system used for the electronic storage and transfer of funds").

[201] Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994).

wire or electronic communication incidental to the electronic transmission thereof."[202]

By its definition, "electronic storage" is a part of the communication process, because "electronic storage" is the temporary and intermediate storage of communication, either wire or electronic.[203] For example, a message recorded on a telephone answering machine is still in the process of communication. Furthermore, the definition of "electronic communication" excludes a certain kind of stored information,[204] and thus, such exclusion assumes that "electronic communication" generally includes its storage.[205]

---

[202] 18 U.S.C. § 2510(17) (1994). *See supra* note 142 and accompanying text (delineating section 2510(17)). The term "electronic storage" is used in the definition of "wire communication." 18 U.S.C. § 2510(1) (1994). *See supra* note 141 and accompanying text (delineating section 2510(1)). Furthermore, Title II covers "electronic storage" of both "wire communication" and "electronic communication." 18 U.S.C. § 2701 (1994 & Supp. III 1997). *See supra* note 12 and accompanying text (delineating section 2701).

[203] 18 U.S.C. § 2510(17). Moreover, "electronic storage" is defined to be incidental to electronic transmission, and thus, is by concept closely related to the transmission process. *See id.* In other words, "electronic storage" accompanies the transmission, and therefore is not a totally separate and independent process. Hence, "electronic storage" is a part of the entire communication process. *See infra* note 208 and accompanying text (discussing that such a construction conforms to the overall statutory structure). Commentator Nicole Giallonardo, however, argues that stored e-mail is in transit and does not complete its final transmission until the intended recipient retrieves the e-mail from a service provider computer. Giallonardo, *supra* note 28, at 186. Giallonardo concludes that e-mail is acquired contemporaneously with its transmission process, amounting to an interception under Title I, as construed in *Turk*. Giallonardo, *supra* note 28, at 186. However, *Turk*'s contemporaneity requirement was designed to exclude this very stored communication, and therefore her argument fails.

[204] 18 U.S.C. § 2510(12)(D) (1994 & Supp. III 1997). "Electronic communication" does not include "electronic funds transfer information *stored*." *Id.* (emphasis added). *See supra* note 142 and accompanying text (delineating section 2510(12)).

[205] Moreover, section 2510(12)(D) was added in 1996, after the *Steve Jackson Games* decision. Thus, it is more likely that Congress assumed that "electronic communication" generally includes storage of the communication, notwithstanding the *Steve Jackson Games* decision.

Moreover, "electronic communication system"[206] is defined as the facilities for "electronic transmission" and "electronic storage," and thus, implies that communication includes both the "transmission" and "storage" stages. Similarly, "electronic communication" is defined as "transfer," not "transmission,"[207] and thus, such difference indicates that "electronic communication" includes more than mere transmission. In fact, the word "transfer" is used in the ECPA as the entire process of communication from its origin to its receipt by an addressee.[208]

---

[206] 18 U.S.C. § 2510(14) (1994) provides as follows: "'electronic communication system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."

[207] 18 U.S.C. § 2510(12) (1994 & Supp. III 1997). *See supra* note 142 and accompanying text (delineating section 2510(12)).

[208] The term "aural transfer" is defined as "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. § 2510 (18) (1994). "Aural" points to "containing the human voice," and "transfer" points to "at *any* point between and including the point of origin and the point of *reception*." *Id.* (emphasis added). Therefore, transfer covers the entire process of communication from its origin to its receipt by an addressee, including its temporary and intermediate storage, if any. Transfer is broader in meaning than transmission, and includes an incidental process of transmission, i.e., the temporary and intermediate storage. *See* S. REP. No. 99-541, at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 (explaining that "the term 'wire communication' means the transfer of a communication . . . through the use of communication transmission facilities"). The title of "Electronic Communications Privacy Act" indicates that communication covers the entire communication process, including its storage, because the statute consists of Title I (the Federal Wiretap Act) and Title II (the Stored Communications Act). Furthermore, among oral, wire and electronic communications, the meaning of communication, and transfer, should be seen as the same. *See* 18 U.S.C. § 2510(1) (1994); 18 U.S.C. § 2510(12) (describing "electronic communication" as "transfer," as in the case of "wire communication" under section 2510(1)). If different meanings are to be given to communication in "oral communication," "wire communication," and "electronic communication," such would be spelled out. *See* 18 U.S.C. § 2510(1), (2), (12). However, these definitions focus on the means of communication, because the word "communication" itself is not defined. *See id.* In addition, the interpretation that the meaning of communication is basically the same in oral, wire and electronic communications is supported by the phrase in section 2510(12)(A),

Accordingly, "electronic communication" includes "electronic storage," regardless of whether it is specifically mentioned in the definition of "electronic communication." The Fifth Circuit in *Steve Jackson Games*, however, considered the absence of the reference to "electronic storage" dispositive.[209] The court assumed, without explanation, that the definition of "electronic communication" does not include "electronic storage."[210] However, such an assumption is misplaced because "electronic communication" includes its "electronic storage" as part of the entire communication process.[211] Since the definition of "electronic communication" itself already covers "electronic storage," it is not necessary to specifically add that phrase. Therefore, since "electronic communication" includes "electronic storage," the absence of the reference to it in "electronic communication" does not support the court's conclusion that "electronic communication" does not include "electronic storage."

B. The Function of the Reference to "Electronic Storage" in the Definition of "Wire Communication" in the Overall Statutory Structure

"Communication" encompasses the entire process of communication, including its transmission and storage.[212] In addition, the

---

which specifically excludes oral and wire communications from an electronic communication to clarify the relationship between these three communications. 18 U.S.C. § 2510(12)(A). *See supra* note 142 and accompanying text (delineating section 2510(12)). Thus, transfer, and in turn, communication includes the whole process of the communication until received and covers its temporary and intermediate storage. *See* 18 U.S.C. § 2510(1), (2), (12).

[209] Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994).

[210] *Id.* at 461-62.

[211] *See supra* note 208 and accompanying text (arguing that such a construction conforms to the overall statutory structure).

[212] *See* discussion *supra* Part II.A, arguing that "electronic communication" impliedly covers "electronic storage". Moreover, Title II provides in part "whoever . . . obtains, alters, or prevents authorized access to *a wire or electronic communication while it is in electronic storage* in such system shall be punished." 18 U.S.C. § 2701 (1994 & Supp. III 1997) (emphasis added).

definition of "wire communication" specifically states that it encompasses the entire process "between the point of origin and the point of reception."[213] Thus, "wire communication" clearly includes its intermediate storage, even without referring to it. Therefore, the assumption of the Fifth Circuit in *Steve Jackson Games* that the reference to storage in "wire communication" is made in order to include its storage is misplaced.[214]

The phrase "and such term includes any electronic storage of such communication"[215] in the definition of "wire communication" is necessary in order to include storage of an *electronic* nature, which is broader than *wire* storage. Without the specific reference to "electronic storage," it is not clear whether "wire communication" includes storage of an *electronic* nature. "Wire communication" historically meant a telephone and a telegraph.[216] Thus, although the word "wire communication" includes its incidental storage process, such storage will normally be understood as *wire* storage, not "*electronic* storage."[217] Therefore, the phrase "and such term includes any electronic storage of such communication" removes the ambiguity about the relationship between "wire communication" and "*electronic* storage." Such a

---

Thus, the phrase "a wire or electronic communication while it is in electronic storage" implies that both communications include their storage phases. *See supra* note 208 and accompanying text (arguing that such a construction conforms to the overall statutory structure).

[213] 18 U.S.C. § 2510(1). "Wire communication" is defined as "any aural transfer made . . . between the point of origin and the point of reception." *Id.* *See supra* note 141 and accompanying text (delineating section 2510(1)).

[214] In *Steve Jackson Games*, that assumption was the basis of the court's conclusion that the absence of the reference to the storage in "electronic communication" shows that it does not include the storage. *See* 36 F.3d at 461.

[215] 18 U.S.C. § 2510 (1). *See supra* note 141 and accompanying text (delineating section 2510(1)).

[216] *See supra* note 51 and accompanying text (citing Berger v. New York, 388 U.S. 41, 45-49 (1967)).

[217] The term "electronic communication" is important because Title II (the Stored Communications Act) primarily deals with "electronic storage" of wire and electronic communications. *See* 18 U.S.C. § 2701.

phrase expressly shows that "wire communication" covers its "*electronic* storage."[218]

Accordingly, a close examination of the language and structure of the ECPA requires the opposite result of that reached by the Fifth Circuit in *Steve Jackson Games*. The court failed to examine the meaning of the term "electronic storage," and thus, misunderstood the relationship between "electronic storage" and "electronic communication." The term "electronic communication" impliedly covers "electronic storage" as part of its entire communication process.[219] The court's reliance on the absence of the reference to "electronic storage" in "electronic communication" is misplaced. Since "electronic communication" includes its "electronic storage," e-mail stored in a service provider computer is subject to an interception under Title I (the Federal Wiretap Act). This interpretation conforms to the overall structure of the ECPA,[220] and also eliminates the undesirable result created by the interpretation of the Fifth Circuit in *Steve Jackson Games*.[221]

---

[218] Moreover, since "electronic communication" is defined as exclusive of "wire communication," 18 U.S.C. § 2510(12) (1994), and "electronic communication" includes "electronic storage," if "wire communication" does not include "electronic storage" other than wire storage, such "electronic storage" might be construed as part of "electronic communication," which is less protected under certain circumstances under Title I. *See supra* Part II.B, describing the less protection under Title I for an electronic communication. Without the specific addendum of its "electronic storage" to the definition of "wire communication," "wire communication" will not include its "electronic storage," because it may be a part of the larger concept of "electronic communication." *See supra* note 141 and accompanying text (delineating section 2510(12)).

[219] *See* discussion *supra* Part III.A, arguing that "electronic communication" impliedly covers "electronic storage".

[220] Moreover, the legislative history generally supports this interpretation in that electronic communication is not distinguished from wire or oral communications for the needs of privacy protection and Title II is not intended to cover an interception of e-mail temporarily stored in a service provider computer. *See supra* note 56 and accompanying text (referring to the Senate Report for this Congressional intent).

[221] *See supra* note 29 and accompanying text (arguing that police tend to circumvent Title I (the Federal Wiretap Act) by accessing e-mail stored in a service provider computer).

CONCLUSION

Seventy years ago, Justice Brandeis, in his dissenting opinion in *Olmstead v. United States*, predicted that modern technological development would someday enable law enforcement to search people or their properties without physically trespassing a person's property.[222] Today, advancements in telecommunications technology have dramatically changed our life. In particular, Internet technology has increased in popularity and will significantly change the way we handle our affairs.[223]

Justice Brandeis also stated that courts should be alert to the changes of time and the emergence of new conditions and purposes in determining the issue of statutory interpretation.[224] However, the current interpretation of the ECPA by the courts following *Steve Jackson Games* directly contradicts the Congressional intent that e-mail enjoy a reasonable expectation of privacy and be subject to Title I (the Federal Wiretap Act). Such an interpretation has created the undesirable consequence that police can circumvent Title I by accessing e-mail stored in a service provider computer. As in the case of a telephone wiretapping, an interception of e-mail, whether stored or not, leads to a serious invasion of privacy by government without the safeguards of Title I. Moreover, the courts' interpretation contradicts the language and structure of the ECPA. Contrary to a line of cases following *Steve Jackson Games*, Title I applies to the access to e-mail stored in a service provider computer because the statutory language and structure of the ECPA, consistent with the Congressional intent, supports such a fair interpretation.

Given the alternative fair interpretation of Titles I and II of the ECPA proposed by this Note, courts should re-examine the privacy protection of e-mail under the ECPA in light of the *Katz* decision that led to the doctrine of a reasonable expectation of privacy. Uneven protection of "electronic communication" and "wire

---

[222] 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

[223] *See* Dempsey, *supra* note 8, at 67-69.

[224] *See Olmstead*, 277 U.S. at 472-73 (Brandeis, J., dissenting).

communication" as a result of *Steve Jackson Games* underestimates the reasonable privacy expectation of people who use e-mail routinely and discourages their reliance on e-mail as a contemporary method of communication.