UIC John Marshall Journal of Information Technology & Privacy Law

Volume 14
Issue 1 *Journal of Computer & Information Law - Fall 1995*

Article 6

Fall 1995

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 (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

I. INTRODUCTION

On March 1, 1990 the United States Secret Service invaded Steve Jackson Games, Inc. ("SJG"),[1] and seized three of its computers, 300 computer disks, and other computer equipment essential to SJG's business operations.[2] The Secret Service believed that one of SJG's employees, a co-sysop,[3] had illegally accessed a sensitive 911 document[4] by

1. Steve Jackson started Steve Jackson Games in 1980. Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432, 437 (W.D. Tex. 1993). The company is located in Austin, Texas and is a major competitor in the market of role playing games. Brief for Appellants at 3-4, Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (hereinafter Appellants' Brief). Role playing games are dice-based games in which every player becomes a character designated with certain skills, traits, and qualities such as Strength, Dexterity, IQ, and Health. James Duncan, Sean Barrett, and Kevin Wong, The GURPS FAQ ("Frequently Asked Questions List") Document URL: http://io.comm./sjgames/gurps/faq.html (September 1994). Events in the role playing games are dictated by dice and games exist in numerous fantasy and futuristic genres. *Id. See infra* note 86 for a description of the GURPS gaming system.

2. *Jackson Games*, 816 F. Supp. at 437.

3. Steve Jackson Games v. United States Secret Service, 36 F.3d 457, 459 (5th Cir. 1994). A sysop is a systems operator. *Id.* A Bulletin Board System ("BBS") sysop is the person with authorization to review or delete any information on a bulletin board. *Id. See also infra* note 6 (defining bulletin board system).

4. *Jackson Games*, 816 F. Supp. at 435. The 911 program was actually a document entitled, "A BellSouth Standard Practice . . . Control Office Administration of Enhanced 911 Services for Specialty Services and Major Account Centers, March 1988." Terri A. Cutrera, Note, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139, 153 (Fall 1991). The authorities feared that a hacker group called "Legion of Doom" was going to utilize the document to shut down the 911 emergency system in nine different states. *Id. See also* Richard P. Klau & Erik J. Heels, *Online: The*

breaking into a BellSouth computer[5] and downloading it onto SJG's electronic Bulletin Board System ("BBS"),[6] Illuminati.[7] Because Illuminati was accessible to the public, the Secret Service thought that the exposure of the 911 document threatened nine cities' emergency call systems.[8] Hence, the Secret Service executed a warrant against SJG to locate and retrieve the document.[9]

One of the computers seized operated SJG's BBS from which Steve Jackson and his employees utilized an electronic mail ("e-mail") system[10]

Electronic Frontier Foundation is Exploring and Charting the Legal Boundaries of Cyberspace, STUDENT LAWYER, Oct. 1994, at 14-15; *see infra* note 70 (defining hacker).

5. *Jackson Games*, 36 F.3d at 458-59. Bell Company is the AT & T parent company which operates phone lines and telecommunications systems nationwide. Cutrera, *supra* note 4, at 153.

6. A Bulletin Board System is a medium of exchange on computer systems between computer users. Jim Suliski, *The Rise of Bulletin Board Systems*, CHI. TRIB., Nov. 18, 1990, § 19, at 17-18. The features of the boards often include the capability to exchange electronic mail ("e-mail"), access software programs, and post personal information. *Id. See infra* note 10 (defining e-mail). Often a BBS is used to facilitate discussion among special interest groups. Suliski at 18. An electronic BBS is the modern, electronic version of the traditional bulletin boards commonly located at grocery stores, universities, and other public places. Jonathan Gilbert, Note, *Computer Bulletin Board Operator Liability for User Misuse*, 54 FORDHAM L. REV. 439, 439 n.1 (1985). Electronic BBSs enable computer users to post and receive messages via computer. Eric C. Jensen, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 FED. COMM. L.J. 217, 217-219 (1987). The sysop of a BBS has the ability to add or delete information existing on the BBS. *Id.* at 219. However, the sysop usually is not able to preview information that other users intend to post on the BBS. *Id.*

Any person with a computer and modem has the capacity to access various BBSs. Jensen at 217. A modem is an electronic device that connects a computer to a telephone to allow communication by computers via the telephone. Robert J. Sciglimpaglia, Jr., *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199, 204 n.19 (1991).

7. Illuminati was SJG's BBS from which it operated e-mail and stored drafts of its publishable materials and business records. *Jackson Games*, 36 F.3d at 458. Illuminati informed BBS users about the products, interests, and ventures of the company. *Id.* In addition, Illuminati functioned as a medium of exchange through which employees, writers, and customers of SJG could send and receive information regarding the company. *Id.*

8. *Jackson Games*, 816 F. Supp. at 435.

9. *Jackson Games*, 36 F.3d at 459; *see infra* note 90 (listing the property enumerated in the warrant).

10. E-mail is a form of electronic communication transmitted by computer and telephone. S. REP. No. 541, 99th Cong., 2d Sess. 8 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3562 (1986). E-mail is sender-specific; it is sent and accessed by specially assigned passwords. *Id.* The sender types a message into a computer and assigns it an appropriate address. Appellants' Brief at 5. Using the computer and telephone lines that are connected by a modem, the sender transmits the message over the telephone lines to an e-mail service. S. REP. No. 541, 99th Cong., 2d Sess. at 8. The e-mail service receives and stores the e-mail in a computer "mail box." *Id.* When the intended recipient calls the service to retrieve e-mail, the e-mail is transmitted over the telephone lines again to the recipient's computer enabling the user to read it. *Id.* The reader may then choose to store the message in a personal computer file or delete it. Appellants' Brief, *supra* note 1, at 5.

for public and private communication.[11] At the time of the seizure, the BBS contained 162 pieces of private unread e-mail.[12] Although the Secret Service obtained a search warrant, it exceeded the scope of the warrant when it seized publishable documents, including a draft manual to the Generic Universal Role Playing Games ("GURPS") Cyberpunk game system and drafts of magazine articles, which were completely unrelated to the investigation.[13] In addition, the Secret Service opened, read, and deleted the e-mail before the intended recipients retrieved or read their mail.[14] Thus, the Secret Service illegally prevented private individuals from receiving personal mail and communications.[15]

Consequently, Steve Jackson and three of his employees[16] initiated a lawsuit against the Secret Service under three federal privacy statutes: the Privacy Protection Act,[17] the Wire and Electronic Communications Interception and Interception of Oral Communications Act ("Federal Wiretap Act"),[18] and the Stored Wire and Electronic Communications

---

11. *Jackson Games*, 36 F.3d at 458.

12. *Id.*

13. *Jackson Games*, 816 F. Supp. at 437-38, 439-40.

14. *Id.*

15. Brief for Amicus Curiae, Electronic Frontier Foundation, Inc., The Society for Electronic Access, and Intercon Systems Corporation, at 9, Steve Jackson Games v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (hereinafter Amicus Curiae Brief).

16. *Jackson Games* 36 F.3d at 458. The employees of SJG who sued the government in this case for seizing, reading, and destroying their private e-mail communications were: (1) Elizabeth McCoy, who used Illuminati as a game player to critique the games and publications of the company and for personal communication with associates and friends; (2) William Miliken, who used Illuminati only to communicate privately with associates and friends; and (3) Steffan O'Sullivan, who used Illuminati to write publishable articles for the company, for inter-office business uses, and to communicate both publicly and privately with associates and friends. *Jackson Games*, 816 F. Supp. at 439.

17. The Privacy Protection Act, 42 U.S.C. § 2000aa(b)(3) (1988) states:

> [I]t shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize documentary materials, other than work product materials, possessed by a person in connection with a purpose to disseminate to the public a newspaper, book . . . or other similar form of public communication . . . . [T]his provision shall not impair or affect the ability of any government officer or employee, pursuant to other applicable law, to search for or seize such materials, if . . . there is reason to believe that the giving of notice pursuant to a subpena duces tecum would result in the destruction, alteration, or concealment of such materials . . . .

Id.

18. Electronic Communications Privacy Act 18 U.S.C. §§ 2510-2521 (1988). This Act states, generally:

> Except as otherwise specifically provided in this chapter [18 U.S.C. §§ 2510 et seq.] any person who . . . intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . .

18 U.S.C. § 2511(1)(a).

and Transactional Records Access Act ("Stored Wire Act").[19] The Western District Court of Texas awarded Steve Jackson and his employees damages under the Privacy Protection Act because the Secret Service illegally seized and retained publishable documents.[20] In addition, the trial court determined that the plaintiffs could recover damages under the Stored Wire Act for the illegal seizure of e-mail; however, the court held that the Federal Wiretap Act did not apply.[21] The District Court held that the Secret Service did not "intercept" the e-mail within the statutory definition of the Federal Wiretap Act.[22]

The significance of the trial court's decision partially lies in the damage award. A violation of the Stored Wire Act subjects the offending party to a minimum $1,000 fine.[23] A violation of the Federal Wiretap Act punishes the party with a $10,000 fine.[24] Imposing $1,000 fines against the government for seizing, reading, and destroying private unread e-mail does not serve to punish the government nor deter it from

---

Section 2520 states, generally:

> Any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation actual damages, or statutory damages of $10,000 per violation or $100 per day of the violation, whichever is greater.

18 U.S.C. §§ 2520(a), (c)(2)(A)-(B).

This Act is Title I under the Electronic Communications Privacy Act ("ECPA"). *See* 18 U.S.C. §§ 2510-2521. Although it is one of two titles under the ECPA, Congress stated that its short title is "ECPA." *Id.* For purposes of this article, to ensure that the reader will distinguish Title I of the ECPA from Title II (also relevant to this article), this note will hereinafter refer to the ECPA using its former name, the "Federal Wiretap Act" and to Title II as the "Stored Wire Act."

19. The Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. §§ 2701-2711. The general nature of the Stored Wire and Electronic Communications and Transactional Records Access Act makes it a crime to:

> (1) intentionally acces[s] 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 . . . .

18 U.S.C. § 2701.

Section 2707(c), regarding damages, reads, "The court may assess . . . damages . . . under this section the sum of the actual damages suffered by the plaintiff . . . but in no case shall a person entitled to recover receive less than the sum of $1,000." 18 U.S.C. § 2707(c).

20. *Jackson Games*, 816 F. Supp. at 441. The District Court awarded SJG $8,781 for expenses and $42,259 for economic damages under the Privacy Protection Act, 42 U.S.C. § 2000aa (6). *Id.*

21. *Jackson Games*, 816 F. Supp. 432; *see supra* notes 18 and 19 (detailing relevant portions of the Federal Wiretap Act and the Stored Wire Act).

22. *Jackson Games*, 816 F. Supp. at 442.

23. *See supra* note 19 (listing statutory damages available under the Stored Wire Act).

24. *See supra* note 18 (listing statutory damages available under the Federal Wiretap Act).

future imprudent behavior. The lower court indicated its insensitivity to computer users' privacy rights in its decision and, consequently, Steve Jackson and his employees appealed the decision to The United States Court of Appeals for the Fifth Circuit.[25]

In *Steve Jackson Games, Inc. v. United States Secret Service*, the Fifth Circuit reviewed and examined whether the Secret Service's illegal seizure of a BBS containing private unread e-mail was an interception under the 1986 amended version of the Federal Wiretap Act.[26] The Fifth Circuit determined that the e-mail existed in electronic storage at the time the Secret Service seized the BBS.[27] After analyzing the Wiretap Act, the court determined that e-mail is only subject to interception under the Act when it is actually in transmission[28] and that the Federal Wiretap Act does not apply to e-mail that is idle in electronic storage.[29] Therefore, the court held that e-mail in electronic storage is not subject to interception under the Federal Wiretap Act.[30] Ultimately, the court found that the Secret Service did not intercept the 162 pieces of unread private e-mail when it seized the BBS containing the unread e-mail.[31]

This casenote asserts that the Fifth Circuit erred by ruling that the Secret Service did not violate the Federal Wiretap Act when it seized the Illuminati BBS and opened, read, and destroyed 162 pieces of private unread e-mail. The court overlooked an important exception[32] contained within the Electronic Communications Privacy Act ("ECPA")[33] which en-

25. *Jackson Games*, 36 F.3d at 457.

26. *Id.* at 460.

27. *Id.* at 461.

28. *Id.* at 462.

29. *Jackson Games*, 36 F.3d at 462.

30. *Id.* at 458, 461-62.

31. *Id.*

32. 18 U.S.C. § 2701(a)-(c). Under this section of the Stored Wire Act, entitled "Unlawful access to stored communications," the relevant text indicates that a person who illegally accesses a stored communication is subject to the punishment under § 2703(b), *unless* the person secured a valid court order under 18 U.S.C. § 2518 to "intercept" the stored electronic communication. 18 U.S.C. § 2701(c)(3).

33. Electronic Communications Privacy Act of 1986, Pub.L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2711 (1986)). The ECPA contains both the Federal Wiretap Act and the Stored Wire Act. S. REP. No. 541, 99th Cong., 2d Sess. 1-5 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555-3559. Sections 2510-2520 existed as the Federal Wiretap Act prior to the enactment of the ECPA in 1986. *Jackson Games*, 36 F.3d at 460. When Congress passed the ECPA, it amended the Federal Wiretap Act to protect electronic communications from illegal interception in addition to oral and wire communications and added the Stored Wire Act to protect against illegal access to wire and electronic communications. *See generally* H.R. REP. No. 647, 99th Cong., 2d Sess., at 17-18; S. REP. No. 541, 99th Cong., 2d Sess. at 1-5. Congress labeled sections 2510-2521 with the short title "ECPA" and remained silent regarding a short title for sections 2701-2711. *Id.* However, so that the reader can easily distinguish between the two statutes, this note uses

compasses both the Federal Wiretap Act[34] and the Stored Wire Act.[35] The exception indicates that when a stored communication is vulnerable to interception, the Federal Wiretap Act preempts the Stored Wire Act.[36] Unread private e-mail which exists on a BBS but has not been retrieved or read by the intended recipient is subject to interception because it has not reached its final destination. Thus, when unread e-mail exists as a stored electronic communication, it remains susceptible to interception.[37] If the Fifth Circuit had studied this important exception to the Stored Wire Act in conjunction with the Federal Wiretap Act and the relevant definitions contained within the ECPA, it would have determined that the Secret Service violated the Federal Wiretap Act when it seized the unread e-mail. Private e-mail that has been sent to a BBS, but remains unread by the intended recipient, is subject to interception.[38]

Second, this casenote argues that the Fifth Circuit failed to adequately consider the legislative history of the ECPA; the court's decision is contrary to specific Congressional intent. When Congress amended the Federal Wiretap Act and enacted the ECPA in 1986,[39] it intended to provide greater privacy protection to electronic communications.[40] Congress aimed to provide the same privacy protection to e-mail and other electronic forms of communication as federal law recognizes for United States Postal Mail and Telecommunications Systems.[41] Regardless, the

---

"ECPA" to refer to both statutes simultaneously, and "Federal Wiretap Act" and "Stored Wiretap Act" to refer individually to §§ 2510-2521 and §§ 2701-2711 respectively.

34. 18 U.S.C. §§ 2510-2521; *see supra* note 18 (citing relevant text of the amended version of the Federal Wire Act).

35. 18 U.S.C. §§ 2701-2711; *see supra* note 19 (citing relevant text of the Stored Wire Act).

36. *See* 18 U.S.C. § 2701(c)(3).

37. *Id.*

38. *See generally* 18 U.S.C. §§ 2701(c)(3) (creating an exception providing for enhanced penalties under Federal Wiretap Act for seizures of communications which have not completed the transmission process).

39. *See generally* H.R. REP. No. 647, 99th Cong., 2d Sess., at 17-18; S. REP. No. 541, 99th Cong., 2d Sess., 1-5 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555-3559; Amicus Curiae Brief, *supra* note 15, at 11-12 *citing* 131 CONG. REC. 11,795 (1985) (statement of Sen. Leahy).

40. S. REP. No. 541, 99th Cong., 2d Sess. at 5 states:

> Most importantly, the law must advance with technology to ensure the continued vitality of the Fourth Amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

Id.

41. *Id.* The Senate Report states:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. Voice communications transmitted via

Fifth Circuit indicated that e-mail is only subject to interception when it is actually in transit from one computer terminal to another.[42] However, e-mail is transmitted virtually instantaneously;[43] thus, the Fifth Circuit's decision in *Jackson Games* makes it highly unlikely that the interception laws could ever apply to e-mail. Because the court failed to consider the Congressional intent to protect e-mail communications in *Jackson Games*, the Federal Wiretap Act is virtually inapplicable with regard to e-mail.

Third, this note demonstrates that the Fifth Circuit disregarded the plain meaning of the word "intercept" when it interpreted the definition under the Federal Wiretap Act. "Intercept" is defined in several ways. It means: "(1) to prevent or hinder; (2) to stop, seize, or interrupt in progress or course or before arrival; or (3) to interrupt communication, or connection with."[44] In addition, "interception" is the "taking or seizure by the way or before arrival at a destined place."[45] The Secret Service intercepted the private unread e-mail when it seized the BBS before the intended recipients took control of their private mail. The Secret Service interrupted the communication, intercepting it within the most basic meaning of the word.

Finally, this note challenges the Fifth Circuit's failure to consider prior case law interpretations of the word intercept as defined by the Federal Wiretap Act.[46] The District Court, citing *United States v.*

---

common carrier are protected by [T]itle III of the Omnibus Crime Control and Safe Streets Act of 1968. But there are no comparable Federal statutory standards to protect the privacy and security of communications services or new forms of telecommunications and computer technology. This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.

Id.

42. *Jackson Games*, 36 F.3d at 461-62.

43. H.R. REP. No. 647, 99th Cong., 2d Sess., at 22 (stating that "e-mail is interactive in nature and can involve virtually instantaneous conversations more like a telephone call than like mail"); *see also* Sebastian J. Leonardi, *Road Map to the Internet*, BARRISTER, Spring 1995, 16, 18 (stating that, "[u]nlike the U.S. Postal Service and other commercial carriers, e-mail delivery is not next day or next week, but practically instantaneous"); Steven Winters, Comment, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197, 198 n.4 (1993) (stating that "e-mail reaches its intended recipient almost instantaneously").

44. WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 630 (1988).

45. BLACK'S LAW DICTIONARY 811 (6th ed. 1990).

46. United States v. Turk, 526 F.2d 654 (5th Cir. 1976) (holding that acquisition of communication must be contemporaneous with the actual conversation to constitute an "intercept" under the Federal Wiretap Act); United States v. Nelson, 837 F.2d 1519 (11th Cir. 1988) (holding that interception refers to the initial acquisition of a communication, regardless of where the communication is actually heard); Amati v. City of Woodstock, Ill., 829 F. Supp. 998 (N.D. Ill. 1993) (stating that interception occurs upon the mere recording; whether anyone subsequently hears the recording is immaterial); Reynolds v. Sears, 857 F.

Turk,[47] concluded that an interception occurs only when the communication is acquired contemporaneously with its initial dispatch.[48] Because the unread e-mail in *Jackson Games* sat idly in electronic storage on the BBS, the district court found that the Secret Service did not intercept the e-mail contemporaneously with its transmission.[49] However, the e-mail was in-transit at the time of the seizure because it had not completed its final transmission, which occurs once the intended recipient retrieves the e-mail from the BBS mailbox and reads it.[50] Thus, the Secret Service acquired the unread e-mail contemporaneously with the e-mail transmission process qualifying the seizure as an interception under *Turk*.[51]

II. BACKGROUND AND SUMMARY OF FACTS

Steve Jackson Games[52] publishes books, magazines, and role playing adventure games[53] from its office in Austin, Texas.[54] Through one of its personal computers, SJG operated an electronic BBS[55] named Illuminati.[56] Illuminati informed interested customers about the products, interests, and ventures of the company.[57] In addition, Illuminati functioned as a medium of exchange through which employees, writers, and customers of SJG could send and receive information regarding the company.[58] Finally, the Illuminati BBS operated an e-mail system.[59] BBS users sent and received private and public messages through the use of special e-mail access code numbers or passwords.[60]

Supp. 1341 (W.D. Ark. 1994) (maintaining that only the initial acquisition of the communication is necessary to constitute an "interception").

47. *Turk*, 526 F.2d at 654.

48. *Id.* at 658.

49. *Jackson Games*, 816 F. Supp. at 441-42.

50. Appellants' Brief, *supra* note 1, at 6 (arguing that e-mail is still in-transit if it was sent to a BBS but remains unread by the intended recipient).

51. *Turk*, 526 F.2d at 654.

52. Steve Jackson started SJG in 1980 and is currently still in business. *Jackson Games*, 816 F. Supp. at 434. "Steve Jackson Games is an award-winning publisher of imaginative role-playing games." Appellants' Brief, *supra* note 1, at 4. *See supra* note 1 (explaining SJG and role playing games generally).

53. *Jackson Games*, 36 F.3d at 458; *see supra* note 1 (defining and explaining role playing games).

54. *Jackson Games*, 816 F. Supp. at 434.

55. *Jackson Games*, 36 F.3d at 458.

56. *Id. See supra* note 7 and accompanying text (describing the Illuminati BBS).

57. *Jackson Games*, 36 F.3d at 458.

58. *Id.*

59. *Id.*

60. *Jackson Games*, 816 F. Supp. at 434. An electronic "password" is the secret alphanumeric code that allows a user access to a particular computer system. WEBSTER'S NEW

In 1986, in an attempt to crack down on computer crime[61] and to provide greater privacy protection for users of e-mail and other modern telecommunications technology,[62] Congress passed the Electronic Communications Privacy Act.[63] The ECPA contains an amended version of the Federal Wiretap Act[64] and a newly created Act called the Stored Wire and Electronic Communications and Transactional Records Access Act ("Stored Wire Act").[65] Congress amended the Wiretap Act to provide the same privacy protection to electronic communications from unlawful interception as it originally provided for wire and oral communications.[66] Congress renamed the Wiretap Act to reflect the 1986 Amendment and called it the Wire and Electronic Communications Interception and Interception of Oral Communications Act.[67] The Stored Wire Act protects stored communications from unlawful access.[68]

WORLD DICTIONARY OF COMPUTER TERMS 276 (4th ed. 1993). The codes are assigned to protect the security of systems containing confidential or private information. *Id.*

61. *See* Michael C. Gemignani, Comment, *What is Computer Crime, and Why Should We Care?*, 10 U. ARK. LITTLE ROCK L.J. 55 (1987/1988) (stating that although companies have conducted research to determine the extent of computer crime, the studies are not conclusive); William F. Flanagan & Brigit McMenamin, *The Playground Bullies are Learning How to Type*, FORBES, Dec. 21, 1992, at 186 (stating that the FBI estimates the gross cost per year to victims of computer crime will grow from $500 million to $5 billion); Glenn D. Baker, Note, *Trespassers Will Be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER L.J. 61, 62-63 (1993) (describing computer crime as "a top priority of the Justice Department"); Michael Alexander, *Computer Crime: Ugly Secret for Business*, COMPUTERWORLD, Mar. 12, 1990, at 1; *see also* H.R. REP. No. 647, 99th Cong., 2d Sess., at 17-18.

62. H.R. REP. No. 647, 99th Cong., 2d Sess. at 18; S. REP. No. 541, 99th Cong., 2d Sess. at 1-5.

63. Electronic Communications Privacy Act of 1986, P. L. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2711 (1986)).

64. Federal Wiretap Act, P. L. 90-351, Title III, Stat. 212 (1968), *amended by* Electronic Communications Privacy Act, P.L. 99-508, Title I, Stat. 1851, 1859 (1986) (which appears as 18 U.S.C. §§ 2510-2521). Congress enacted the original version of the Federal Wiretap Act in 1968. *Id.* The Congressional findings of the original Wiretap Act state:

> In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

CONGRESSIONAL FINDINGS, June 19, 1968, P.L. 90-351, Title III, § 801, 82 Stat. 211 (d). Congress wanted to assure individuals that the government would only intercept communications necessary to fight crime and that it would not misuse the information obtained. *Id.*

65. 18 U.S.C. §§ 2701-2711; *see supra* note 19 (quoting relevant text of the Stored Wire Act).

66. *See* S. REP. No. 541, 99th Cong., 2nd Sess. *supra* note 39.

67. Electronic Communications Privacy Act of 1986, P. L. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2521).

68. 18 U.S.C. §§ 2701-2711; *see supra* note 19 (citing relevant text of Stored Wire Act).

The Executive Branch also responded to the computer crime problem in the late 1980's when it created special computer crime task forces within the Secret Service, Federal Bureau of Investigation, and the United States Attorney's Office.[69] The task forces investigate allegations of large companies and government departments claiming hackers[70] illegally accessed and tampered with their computerized records and documents.[71]

In 1989, Henry Kluepfel, the Director of Network Security Technology, an affiliate of Bell Company,[72] informed the Secret Service that a

---

69. Anne W. Branscomb, *Common Law for the Electronic Frontier*, SCIENTIFIC AMERICAN, Sept. 1991, at 157; Cutrera, *supra* note 4, at 142 (1991); Baker, *supra* note 61, at 62, 87 n.27.

70. Originally, "hacker" was a complimentary term that referred to computer users who possessed a mastery of computer programming. Baker, *supra* note 61, at 70 n.79; *see also* Cutrera, *supra* note 4, at 140-42. The term "hacker" commonly conjures up the stereotype of the harmless computer user staring into a monitor and punching away at his keyboard. *Id.* Currently, the term more commonly refers to those skilled computer users who access computer systems without authorization. *See* Sciglimpaglia, *supra* note 6, at 200-1 n.1 (1991) (explaining the magnitude of hackers' unauthorized activity and characterizing illegal hacking as white collar crime); *see generally* Flanagan, *supra* note 61, at 184 (describing the various unauthorized activities in which hackers participate). Some of these experienced computer users hack into programs for the challenge or to show off their skills to their friends. Philip Elmer-Dewitt, *Cyberpunks and the Constitution: The Fast Changing Technologies of the Late 20th Century Pose a Challenge to American Laws and Principles of Ages Past*, TIME MAGAZINE, Apr. 8, 1991, at 81; *see also* Joshua Quittner, *Computer Rights Advocates Worry About Overzealousness in the Crackdown on Hackers*, NEWSDAY, Sept. 4, 1990, Discovery Section, at 1; (discussing several recent cases in which the Secret Service conducted raids to seize computer equipment and arrest potential abusers); United States v. Morris, 928 F.2d 504 (2nd Cir. 1991) (upholding conviction of Cornell University graduate student who violated Computer Fraud and Abuse Act by electronically sending a "worm" through university, government, and military computers causing loss of millions of dollars of information). The most significant and threatening hackers are those who illegally access computer networks with intent to steal, embezzle, or destroy information. Baker, *supra* note 61, at 70 (explaining that the term currently has various meanings, but that originally it referred to computer professionals).

71. Baker, *supra* note 61, at 87 n.252; Cutrera, *supra* note 4, at 142. A company or government department usually will not learn that a hacker has stolen information from its computers until the hacker publishes it on another existing information system. *See* Cutrera, *supra* note 4, at 142-43. For example, in 1989, the FBI confirmed that a computer at the University of Southern California contained a copy of Digital Equipment Corporation's, ("DEC") Security Software System. J.A. Savage, *Hacker Prosecution*, COMPUTERWORLD, Jan. 9, 1989, at 2. DEC's affidavit submitted to the FBI also noted three other unauthorized intrusions into its system. *Id.* The affidavit alleged that the four invasions amounted to losses of four million dollars for DEC. *Id.* Once reported, the task forces conduct government investigations to attempt to trace the illegal activity to the hacker for prosecution purposes. *Id.*

72. *Jackson Games*, 36 F.3d at 458-59. BellCompany is an AT&T affiliate company, operating phone lines and systems nationwide. Cutrera, *supra* note 4, at 153.

computer hacker[73] had illegally accessed BellSouth's[74] 911 program[75] and published it on a BBS operated in Illinois[76] and on at least one other BBS operated elsewhere.[77] Director Kluepfel and the Secret Service feared that publication of the document threatened a 911 system failure in nine states.[78]

By February of 1990, the Secret Service believed that it had collected sufficient information to link the alleged criminal activity to the operations of SJG.[79] The Secret Service learned that the 911 program, stolen from BellSouth, illegally existed on a BBS called the Phoenix Project, operated in Austin, Texas, by Lloyd Blankenship.[80] The Secret Service determined that the Phoenix Project published hacker information[81] and requested specific information from hackers with regard to the formulation of a decryption scheme.[82] The Secret Service believed that this particular decryption scheme had the potential to invade numerous computer systems, including access to information within the Defense Department.[83] In addition, the Secret Service discovered that Blankenship worked for SJG and had special access to SJG's Illuminati BBS as a cosysop.[84] This meant that Blankenship had the authority to review and delete any material on Illuminati.[85]

After a limited investigation, the Secret Service erroneously concluded that Illuminati also published criminal hacker materials.[86] To

---

73. *Jackson Games*, 816 F. Supp. at 435.

74. *Jackson Games*, 36 F.3d at 459. BellSouth operates in the southeastern United States and is an affiliate of Bell Phone Company. *See* Cutrera, *supra* note 4, at 153; Klau, *supra* note 4, at 15.

75. *Jackson Games*, 816 F. Supp. at 435; *see supra* note 4 (detailing information regarding the 911 program).

76. *Jackson Games*, 816 F. Supp. at 435. The cases fail to specify the name, location, or operator of the Illinois bulletin board where Kluepfel first discovered the 911 program.

77. *Id.*

78. *Id.*

79. *Jackson Games*, 36 F.3d at 459; *see also* Klau, *supra* note 4, at 15.

80. *Id.*

81. *Jackson Games*, 816 F. Supp. at 436.

82. *Id.* Decryption schemes manipulate various passwords to invade computer systems and enable the hacker to steal information. *Id.* at 435-36; *see also* Flanagan, *supra* note 61, at 184 (describing different decryption schemes); Sciglimpaglia, *supra* note 6, at 206-08 (describing the hacking process).

83. *Jackson Games*, 816 F. Supp. at 436.

84. *Jackson Games*, 36 F.3d at 459.

85. *Id.*

86. *Jackson Games*, 816 F. Supp. at 436. During the investigation of SJG, the Secret Service learned of a document stored in SJG's computer files that it believed to be "a manual for computer crime." Suzanne Stefanac, *Dangerous Games*, CAL. LAW., October 14, 1994 at 56. After the Secret Service raided SJG, it discovered the document was actually a rule book to one of a series of Generic Universal Role Playing Games, ("GURPS"), that the company intended to release at the time of the seizure. *Id. See also*, Anne Meredith

prevent further distribution of the 911 document and to prosecute Blankenship,[87] the Secret Service requested a search warrant for SJG's corporate office.[88]

On March 1, 1990, the Secret Service and government experts[89] executed the search warrant.[90] The search warrant authorized the Secret Service to seize all of SJG's computer equipment, materials, and data that related to the alleged illegal hacker activity.[91] At trial, the district court determined that the Secret Service intended to read and review all the information and materials to which Blankenship had access despite the probability that the Secret Service would seize other files unrelated to its investigation.[92] The personal computer that operated the entire Illuminati BBS was among the items seized by the Secret Service.[93]

On the following day, the Secret Service inquired further into the nature of SJG's business and learned of the extent of its publications and the existence of private e-mail messages among the seized information.[94]

Fulton, *Cyberspace and the Internet: Who will be the Privacy Police*, 3 COMMLAW CONSPECTUS 63, 64 (Winter 1995). Although SJG's game was based on computer hacking, it was a fantasy game. *Jackson Games*, 86 F.3d at 459 n.1. The District Court determined that the Secret Service performed a poor investigation prior to obtaining the search warrant. *Jackson Games*, 816 F. Supp. at 436 n.4. The District Court stated, "[t]he affidavit and warrant preparation was simply sloppy and not carefully done." *Id.* at 437.

87. *See Jackson Games*, 816 F. Supp. at 437. The government never filed any criminal charges against Blankenship. *Id.*

88. *Jackson Games*, 36 F.3d at 459.

89. *Jackson Games*, 816 F. Supp. at 437. The Secret Service brought in computer experts to assist with technical matters of the search and seizure. *Id.* The case does not reveal the identity of the experts who assisted the Secret Service in the seizure of computer equipment at SJG. *Id.*

90. *Jackson Games*, 36 F.3d at 459. The search warrant lists the property the Secret Service could search and seize:

> Computer hardware . . . including . . . central processing unit(s), monitors, memory devices, modem(s), programming equipment, communication equipment, disks, and prints . . . and computer software . . . including . . . memory disks, floppy disks, storage media . . . and written material and documents relating to the use of the computer system including networking access files, documentation relating to the attacking of computers and advertising the results of computer attacks (including telephone numbers and location information) . . . and documentation relative to the computer programs and equipment at the business known as Steve Jackson Games which constitute evidence, instrumentalities and fruits of federal crimes, including interstate transportation of stolen property . . . and interstate transportation of computer access information . . . . This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained on the above described computer and computer data.

Appellants' Brief, *supra* note 1, at Appellants' Record Excerpts, Attachment B.

91. *Jackson Games*, 36 F.3d 459; *see also supra* note 90 (quoting text of issued search warrant).

92. *Jackson Games*, 816 F. Supp. at 436.

93. *Jackson Games*, 36 F.3d 459.

94. *Jackson Games*, 816 F. Supp. at 437.

Notwithstanding SJG's status as a legitimate, profit-making company, dependant upon its technology and ability to publish,[95] and the company's pleas to return the material immediately,[96] the Secret Service withheld all seized equipment, publishable materials, and information for over three months.[97] SJG claimed that the Secret Service drove the company into economic turmoil.[98]

When the Secret Service returned the equipment in June 1990,[99] SJG discovered that the Secret Service accessed and removed information and materials that did not involve Blankenship's alleged illegal activity.[100] Furthermore, the Secret Service read and deleted private e-mail messages that Illuminati users had sent to other users.[101]

In response, SJG, Steve Jackson, and three SJG employees who had sent e-mail messages to Illuminati users at the time of the seizure[102] sued the United States Secret Service and the United States Government.[103] The plaintiffs alleged that the Secret Service and the government violated three federal privacy statutes:[104] (1) the Privacy Protection Act;[105] (2) The Wiretap Act;[106] and (3) the Stored Wire Act.[107] The District Court found for the plaintiffs under the Privacy Protection Act and the Stored Wire Act.[108] However, the court stated that the Federal Wiretap Act did not apply to the facts of the *Jackson Games* case.[109]

---

95. *Id.* On March 2, 1990, the Secret Service learned that SJG published legitimate materials that did not promote criminal hacking crimes. *Id.*

96. *Id.*

97. *Jackson Games*, 816 F. Supp. at 437

98. *Id.* at 438. The company lost $8,781.00 in out-of-pocket expenses, $100,617.00 in lost sales, and $42,259.00 for lost profits. *Id.* Additionally, the company was forced to lay off eight employees. *Id.*

99. *Jackson Games*, 816 F. Supp. at 437.

100. *Id.* at 438.

101. *Id.* Originally, the Secret Service denied that it had read the seized private e-mail. *Id.* at 438. However, the District Court stated in its factual findings:

> The preponderance of the evidence, including common sense, establishes that the Secret Service . . . did read all electronic communications seized and did delete certain information and communications in addition to the two documents admitted deleted. The deletions by the Secret Service, other than the two documents consented to by Steve Jackson, were done without consent and cannot be justified.

Jackson Games, 816 F. Supp. at 438.

102. *See supra* note 16 (listing SJG employees involved in the suit).

103. *Jackson Games*, 816 F. Supp. at 434.

104. *Id.* at 434. *See supra* notes 17-19 (quoting relevant text of the federal statutes involved in the original *Jackson Games* case).

105. *See supra* note 17 (quoting text of The Privacy Protection Act, 42 U.S.C. § 2000aa).

106. *See supra* note 18 (quoting relevant text of the Federal Wiretap Act, 18 U.S.C. §§ 2510-2521).

107. *See supra* note 19 (quoting relevant text of the Stored Wire Act, 18 U.S.C. §§ 2701-2711).

108. *Jackson Games*, 816 F. Supp. at 441, 443.

109. *Id.* at 442.

Steve Jackson and his employees filed an appeal in the United States Court of Appeals for the Fifth Circuit.[110] They asked the court to review the district court's decision that found that the Secret Service did not violate the Federal Wiretap Act when it illegally seized, read, and destroyed 162 pieces of unread private e-mail.[111]

III. ISSUES & CONCLUSIONS

The *Jackson Games* court reviewed whether the Secret Service "intercepted" private unread e-mail in violation of the Federal Wiretap Act when it seized a BBS containing 162 e-mail messages sent to the BBS but not yet retrieved or read.[112]

The Fifth Circuit affirmed the district court,[113] holding that the Secret Service's seizure of SJG's computer, which operated the Illuminati BBS and contained unread e-mail,[114] did not amount to an "interception" within the definition of the Federal Wiretap Act.[115] The court stated that the e-mail existed on the BBS in "electronic storage"[116] and referred to e-mail as "stored communications"[117] subject only to the provisions of the Stored Wire Act.[118] The court concluded that Congress did not intend the statutory term "intercept," contained in the Federal Wiretap Act, to apply to idle electronic communications existing in electronic storage.[119] Thus, the *Jackson Games* court held that the Secret Service did not violate the Federal Wiretap Act when it seized, opened, read, and deleted private unread e-mail.[120]

---

110. *Jackson Games*, 36 F.3d at 457.

111. *Id.*

112. *Id.* at 458, 460.

113. *Id.* at 458.

114. *Jackson Games*, 36 F.2d at 459. When the Secret Service seized the BBS, 162 pieces of unread private e-mail existed on the system. *Id.*

115. *Jackson Games*, 36 F.3d at 458. The ECPA defines intercept, for purposes of the Federal Wiretap Act, as "the aural or other acquisitions of the contents of any wire, electronic, or oral communication through the use of any electronic . . . or other device." 18 U.S.C. § 2510(4).

116. *Jackson Games*, 36 F.3d at 461. Electronic storage is "any temporary, intermediate storage of [any] wire or electronic communication [which is] incidental to the electronic transmission thereof . . . ." 18 U.S.C. § 2510(17)(A).

117. *Jackson Games*, 36 F.3d at 463. After the Fifth Circuit determined that unread e-mail exists in electronic storage under the ECPA, it referred to unread e-mail as stored communications throughout its opinion. *Id.*

118. Id. at 462-63.

119. *Jackson Games*, 36 F.3d at 461-62; *but see* 18 U.S.C. § 2701(c)(3) (providing an exception authorizing the greater penalty of the Federal Wiretap Act for illegal seizures of stored electronic communications which are vulnerable to "interception").

120. *Jackson Games*, 36 F.3d at 458.

IV. COURT'S ANALYSIS

The Fifth Circuit began its analysis with a study of the statutory terms defined within section 2510 of the ECPA[121] which are applicable to both the Federal Wiretap Act and the Stored Wire Act.[122] The *Jackson Games* court analyzed the statutory definition of "intercept" and compared the language contained within the two statutes.[123] Based on the statutory analysis, the court determined that the Secret Service did not "intercept"[124] the private unread e-mail[125] in violation of the Federal Wiretap Act[126] when it seized the Illuminati BBS.

The Fifth Circuit noted that "intercept" is defined, under section 2510 of the Federal Wiretap Act, 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."[127] The court next examined each of the terms contained within the definition of intercept.[128] The Fifth Circuit acknowledged that the statute defines "electronic communication" as "any transfer of signs, signals, writing, . . . of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system . . . but does not include . . . any wire or oral communication."[129] The court then recognized that a "wire communication" is similar to an electronic communication, but it is "any aural transfer made in whole or in part for the transmission of communications by the aid of wire [or] cable . . . and such term includes any electronic storage of such communication."[130] Next, the court observed that the statute defined an aural transfer as a "transfer containing the human voice at any point between and including the point of origin and the point of reception."[131]

Comparing the statutory terms, the court noted that, while the defi-

121. Electronic Communications Privacy Act of 1986, P. L. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2521, 18 U.S.C. §§ 2701-2711 (1986)); *see supra* note 33 (detailing the structure of the ECPA).

122. *Jackson Games*, 36 F.3d at 460-62.

123. *Id.*

124. *See supra* note 115 (defining intercept, 18 U.S.C. § 2510(4)).

125. At the time of the seizure, 162 pieces of private unread e-mail existed on the BBS. *Jackson Games*, 36 F.3d at 459; Appellants' Brief, *supra* note 1, at 6.

126. *See generally supra* note 18 for relevant text of the Federal Wiretap Act.

127. *Jackson Games*, 36 F.3d at 460 (citing the statutory definition of intercept at 18 U.S.C. § 2510(4)).

128. *Jackson Games*, 36 F.3d at 461-62.

129. 18 U.S.C. § 2510(12); *see* S. REP. No. 541, 99th Cong., 2d Sess. at 14 (stating the general rule of the ECPA is that "a communication is an electronic communication protected by the federal wiretap law").

130. 18 U.S.C. § 2510(1).

131. *Jackson Games*, 36 F.3d at 461 (describing the statutory definition of "intercept" prior to the enactment of the ECPA in 1986).

nition of "wire communication"[132] includes the electronic storage of such communication,[133] the definition of "electronic communication"[134] does not.[135] The court recognized that the statute defined electronic storage as "any temporary, intermediate storage of a[n] . . . electronic communication incidental to the electronic transmission thereof."[136] Based on this definition, the Fifth Circuit concluded that e-mail exists in electronic storage when it is sent to, and received by, a BBS.[137] The court stated that the use of the word "transfer" and the omission of the term "electronic storage"[138] in the definition of "electronic communication"[139] indicates that "Congress did not intend for the term "intercept" to apply to electronic mail communications when those communications remain idle in electronic storage."[140]

Determining that e-mail exists on a BBS as stored communications, the court concluded that the Secret Service violated the Stored Wire Act when it seized the Illuminati BBS.[141] In addition, the court stated that neither the language nor the legislative history of the Federal Wiretap Act indicated that Congress intended to allow recovery under both the Stored Wire Act and the Federal Wiretap Act for the same conduct.[142] The court reasoned that substantial differences exist that distinguish the two statutes and preclude any overlap between the statutes.[143] Thus, the court awarded SJG damages only under the Stored Wire Act.[144]

In support of its theory, the court reasoned that the "substantive and procedural requirements for authorization to intercept electronic communications . . . are more stringent [and] complicated" than those re-

---

132. *See Jackson Games*, 36 F.3d at 461 (citing statutory definition of "wire communication"). A wire communication is

> Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by aid of wire, cable, or other like connection between the point of origin and the point of reception . . . and such term includes any electronic storage of such communication . . . .

18 U.S.C. § 2510(1).

133. *Jackson Games*, 36 F.3d at 461.

134. *Id.* Section 2510(12) states that "electronic communication means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . ." 18 U.S.C. § 2510(12).

135. *Jackson Games*, 36 F.3d at 461.

136. *Id.* (citing the statutory definition of "electronic storage" at 18 U.S.C. § 2510(17)).

137. *Jackson Games*, 36 F.3d at 461-62.

138. *See supra* note 116 (citing statutory definition of electronic storage. 18 U.S.C. § 2510(17)).

139. *See supra* notes 129 and 134 (defining electronic communication).

140. *Jackson Games*, 36 F.3d at 461-62.

141. *Id.* at 462.

142. *Id.*

143. *Id.* at 462-63.

144. *Jackson Games*, 36 F.3d at 461-62.

quired to access stored electronic communications.[145] In addition, the court noted that the Federal Wiretap Act contains certain provisions that the Stored Wire Act does not contain which minimize the interception and the duration of the interception when communication is "in the process of transmission at the moment of seizure."[146] The court stated that it is necessary to have more stringent requirements to obtain access to communications in transmission because it is nearly impossible to know in advance if the communication is relevant to a criminal investigation.[147] The court acknowledged that a higher risk exists that the government may invade privacy rights when interception is an issue.[148]

Furthermore, the court reasoned that the requirements to access stored communications are less stringent because it is much easier to locate the relevant communications in a stored capacity using key word searches[149] without accessing the contents of the entire communication. The court stated that the Secret Service could have easily utilized key word searches to survey the contents of the unread e-mail stored on Illuminati.[150] Thus, the court concluded that the Secret Service violated only the Stored Wire Act when it failed to obtain a warrant sufficient to access stored communications.[151] The Fifth Circuit found that the e-mail existed in Illuminati's electronic storage, not in the transmission process at the time of the seizure and determined that the Secret Service did not intercept the private e-mail under the Federal Wiretap Act.[152] Additionally, the court concluded that the government was not required to meet to the strict requirements of the Wiretap Act to access electronic communications existing in stored capacity.[153] Thus, the Fifth Circuit concluded that the Secret Service did not intercept the private e-mail, and that the Federal Wiretap Act was inapplicable to the facts of the *Jackson Games* case.[154]

V. AUTHOR'S ANALYSIS

The Fifth Circuit erred when it held that the Secret Service's seizure of the BBS that contained 162 pieces of private unread e-mail did not

145. *Id.* at 463.

146. *Id.*

147. *Id.*

148. *Jackson Games*, 36 F.3d at 463.

149. *Id.* A key word search is a method of locating relevant communications, which exist in a stored capacity without accessing the entire contents of the communication. *Id.*

150. *Jackson Games*, 36 F.3d at 463.

151. *Id.*

152. *Id.*

153. *Id.*

154. *See Jackson Games*, 36 F.3d at 463.

amount to an interception under the Federal Wiretap Act.[155] The Secret Service unlawfully seized, read, and deleted private e-mail unrelated to its investigation before the intended recipients retrieved or read the mail.[156] Consequently, the Secret Service prevented the e-mail from reaching its final destination.

As a result of the Secret Service's overzealous conduct, the court imposed $1,000 fines against the government for each violation of the Stored Wire Act.[157] However, the court's finding does not acknowledge Congress' express intent to protect electronic communications from illegal governmental seizure[158] and it will not serve to deter the government from interfering with private communications in the future. Moreover, in reaching its conclusion, the Fifth Circuit failed to recognize the important exception within the ECPA, failed to study the plain meaning of the word "intercept," and erred in ignoring relevant case law. The Fifth Circuit should have imposed a higher standard against the government for illegally seizing private e-mail and the court should have fined the Secret Service $10,000 for each occurrence for intercepting private unread e-mail in violation of the Federal Wiretap Act.[159]

A. The Critical Exception

The Fifth Circuit overlooked a critical exception contained within the Stored Wire Act[160] when it analyzed the issue of whether the Federal Wiretap Act prohibited the unlawful seizure of unread private e-mail. The court properly determined that, under the statutory definitions of the ECPA, e-mail that is sent to a BBS exists in electronic storage.[161] However, the court erroneously concluded that stored electronic communications are not subject to interception under the Federal Wiretap Act. If the court had properly applied the exception in the Stored Wire Act under section 2701(c)(3), in conjunction with the language of the Federal Wiretap Act's section 2518,[162] the court would likely have concluded that the Secret Service intercepted the private unread e-mail when it seized the Illuminati BBS.

Section 2701(a) of the Stored Wire Act states:

---

155. *Jackson Games*, 36 F.3d at 457.

156. *Id.* at 459.

157. *Jackson Games*, 816 F. Supp. at 443.

158. *See generally* H.R. Rep. No. 647, 99th Cong., 2d Sess. at 7; *See also* S. Rep. No. 541, 99th Cong., 2d Sess. at 1 (explaining that the House and Senate Reports both indicate that Congress intended the Federal Wiretap to provide privacy protection for e-mail).

159. *See* 18 U.S.C. § 2520; *see also supra* note 18 (quoting relevant text of statute).

160. *See* 18 U.S.C. § 2701(c)(3).

161. *Jackson Games*, 36 F.3d at 461-62.

162. 18 U.S.C. § 2518. Section 2518 provides the proper and required "[p]rocedures for interception of wire, oral, or electronic communications." *Id.*

> [e]xcept as provided in subsection (c) of this section whoever . . . intentionally exceeds an authorization to access [a] facility . . . [through which an electronic communication service is provided] 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.[163]

Subsection (c) of the exception states: "[s]ubsection (a) of this section does not apply with respect to conduct authorized . . . in [other unrelated sections] or 2518[164] of this title."[165] Section 2518 is a provision under the Federal Wiretap Act entitled "Procedure for Interception of . . . Electronic Communications."[166] This section specifically proscribes standards to which an investigative or law enforcement officer must adhere when the officer wishes to intercept[167] a wire, oral, or electronic communication.[168] Congress included section 2518 of the Federal Wiretap Act as an exception to illegal access of a Stored Communication. This indicates that, if the proper warrant is obtained, the government may legally intercept an electronic communication in electronic storage.[169] Therefore, as the language of section 2518 clearly states, stored electronic communications are subject to interception under the Federal Wiretap Act.[170]

Contrary to the Fifth Circuit's reading, this exception indicates that the Federal Wiretap Act is applicable, rather than the Stored Wire Act, when an electronic communication located in electronic storage is susceptible to interception.[171] The court found that electronic communications in electronic storage remain idle and are not subject to interception.[172] However, the court should have distinguished between read and unread e-mail. Unread e-mail is technically *still in transmission* because it has not reached the intended recipient; it is vulnerable to interception until the intended recipient retrieves and reads it.[173] The exception indicates that under some circumstances, courts must read and apply the Federal Wiretap Act and the Stored Wire Act concur-

---

163. 18 U.S.C. § 2701(a)-(b).

164. 18 U.S.C. § 2701(c)(3). Section 2518 lists the "Procedure for interception of wire, oral, or electronic communications." 18 U.S.C. § 2518.

165. 18 U.S.C. § 2701(c).

166. 18 U.S.C. § 2518.

167. *See supra* note 115 (defining "intercept," 18 U.S.C. § 2510(4)).

168. 18 U.S.C. § 2518.

169. *See supra* note 116 (defining "electronic storage," 18 U.S.C. § 2510(17)(A)).

170. Supplemental Letter Brief at 3, Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (hereinafter Letter Brief).

171. *See* 18 U.S.C. § 2701(c)(3).

172. *Jackson Games*, 36 F.3d at 461-62.

173. Appellants' Brief, *supra* note 1, at 6; Reply Brief for Appellants at 4, Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (hereinafter Reply Brief); *see also* Klau, *supra* note 4, at 16.

rently; the two statutes are not mutually exclusive.[174] Thus, if the Fifth Circuit had applied the exception, it would have found that the Secret Service intercepted the 162 pieces of private unread e-mail that existed in electronic storage on the BBS in violation of section 2518 of the Federal Wiretap Act.[175]

B. THE ECPA: CONGRESSIONAL INTENT AND LEGISLATIVE HISTORY

The Fifth Circuit failed to thoroughly examine Congressional intent and the legislative history behind the implementation of the ECPA when it decided the *Jackson Games* case. The court indicated that e-mail is only subject to interception when it is actually in transmission from the sender to the address of the intended recipient.[176] Yet e-mail is sent and received almost instantaneously.[177] The court's narrow interpretation intimates that the Federal Wiretap Act will not protect e-mail at all. However, the House and Senate Reports preceding the enactment of the ECPA indicate that Congress intended to provide the same "high level of protection" to e-mail as the law provides for U.S. Postal Mail and telephone communications.[178] If the court had considered Congressional intent in conjunction with its examination of the ECPA, the Fifth Circuit would have likely held that the Federal Wiretap Act protects unread e-mail existing on a BBS from illegal interception.

The expressed purpose of the ECPA is "to protect against the unauthorized interception of electronic communications."[179] Congress acknowledged the need "to update and clarify the Federal privacy protections and standards in light of the dramatic changes in new computer and telecommunications technologies."[180] When Senator Leahy[181]

---

174. Reply Brief, *supra* note 173, at 3; Letter Brief, *supra* note 170, at 1-2.

175. *See generally*, Amicus Curiae Brief, *supra* note 15, at 8, 11-12; Reply Brief, *supra* note 173, at 4; Letter Brief, *supra* note 170, at 3.

176. *Jackson Games*, 36 F.3d at 461-62.

177. H.R. REP. No. 647, 99th Cong., 2d Sess. at 22; Winters, *supra* note 43, at 198 n.4; Leonardi, *supra* note 43, at 18.

178. S. REP. No. 541, 99th Cong., 2d Sess. at 5.

179. S. REP. No. 541, 99th Cong., 2d Sess. at 1. The general rule of the ECPA is that "a communication is an electronic communication protected by the federal wiretap law." *Id.* at 14.

180. *Id.*

181. *See generally* H.R. REP. No. 647, 99th Cong., 2d Sess. at 28; S. REP. No. 541, 99th Cong., 2d Sess. at 2, 4; Amicus Curiae Brief, *supra* note 15, at 11-12. Senator Patrick J. Leahy of Vermont generated Congressional interest in amending the law in 1984 when he wrote to the Attorney General asking if the Federal Wiretap Act protected e-mail from illegal interception. *See generally* H.R. REP. No. 647, 99th Cong., 2d Sess. at 28; S. REP. No. 541, 99th Cong., 2d Sess. at 3-4. Senator Leahy and some of his colleagues participated in numerous hearings and issued reports between 1984 and 1986, emphasizing "electronic mail remains legally as well as technically vulnerable to unauthorized surveillance." S.

introduced the bill in 1985 he indicated that the ECPA should provide Americans confidence and assurance that their electronic communications would be private.[182] In the Statement to the Senate Report, Congress stressed:

> [t]he law must advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.[183]

Congress feared that failing to protect privacy interests on the new technology would discourage potential customers from utilizing it.[184] The emphasis Congress placed on providing privacy protection for electronic communications is clear and unequivocal.[185] However, the *Jackson Games* decision limits this protection against Congress' express intentions. The Fifth Circuit failed to provide the Illuminati e-mail system the protection from interception which Congress intended and advocated.

In addition, Congress noted that e-mail combines the features of postal mail and telephone communications[186] and asserted the need for comparable protection.[187] Congress stated, "American citizens and

---

REP. NO. 541, 99th Cong., 2d Sess. at 4. Senator Leahy and Senator Charles Mathias introduced the ECPA on June 19, 1986 calling the existing law "hopelessly out of date." S. REP. NO. 541, 99th Cong., 2d Sess. at 2.

182. Amicus Curiae Brief, *supra* note 15, at 11, *citing* 131 CONG. REC. 11,795 (1985) (statement of Sen. Leahy); *see also* S. REP. NO. 541, 99th Cong., 2d Sess. at 18 (professing concern for U.S. citizens' privacy rights).

183. S. REP. NO. 541, 99th Cong., 2d Sess. at 5.

184. H.R. REP. NO. 647, 99th Cong., 2d Sess. at 19.

185. *See generally* H.R. REP. NO. 647, 99th Cong., 2d Sess. at 7; *see also* S. REP. NO. 541, 99th Cong., 2d Sess. at 1. The House and Senate Reports both indicate that Congress intended the Federal Wiretap Act to provide privacy protection for e-mail. *See* H.R. REP. NO. 647, 99th Cong., 2d Sess. at 16, 21-22; *see also* S. REP. NO. 541, 99th Cong., 2d Sess. at 1, 3, 11.

186. H.R. REP. NO. 647, 99th Cong., 2d Sess. at 22 (stating that many e-mail users have substituted the new technology for telephone calls, while others utilize e-mail instead of the postal service). *Id.*

187. *See* H.R. REP. NO. 647, 99th Cong., 2d Sess. at 22 (asserting that, although e-mail is similar to U.S. Postal Mail, it is more highly comparable to telephone communications). Congress indicated that e-mail is not under governmental control because it is provided by private companies. *Id.* Second, it stated that e-mail is more similar to telephone communications because of the speed at which the communication travels. *Id.* Congress found that e-mail is "interactive in nature and can involve virtually instantaneous conversations." *Id.* at 22. Last, e-mail differs from postal mail because the e-mail service provider may have access to the communication and actually retain copies of individual correspondence. *Id.* Despite this last distinction, Congress speculated that private parties to an e-mail transmission would likely have a reasonable expectation of privacy in the communication to adequately afford them Fourth Amendment privacy protection. *Id. See generally*, Katz v. United States, 389 U.S. 347, 351 (1967) (stating: "[w]hat a person knowingly exposes to the

American businesses are using the new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services."[188] Moreover, Congress stated, "[i]t does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute."[189] As a result, Congress amended the Federal Wiretap Act, that formally protected oral and wire communications, to include privacy protection for electronic communications.[190] Thus, the *Steve Jackson Games* court should have afforded e-mail the same protection afforded to wire and oral communications.

Furthermore, Congress compared e-mail to U.S. postal mail[191] which also enjoys a high standard of privacy protection.[192] When Senator Leahy originally introduced the bill for the ECPA, he stated:

> From the beginning of our history, first-class mail has had the reputation for preserving privacy, while at the same time promoting commerce. Both of these important interests must continue into our new information age. We cannot let any American feel less confident in putting information into an electronic mail network than he or she would in putting it into an envelope and dropping it off at the Post Office.[193]

Thus, if the Fifth Circuit had analyzed the legislative history of the ECPA more closely when it decided the *Jackson Games* case, it would have determined that Congress intended to afford e-mail the same high

---

public . . . is not a subject of Fourth Amendment protection"). *Katz* also states that what a person "seeks to preserve as private, may be constitutionally protected . . . [T]he Fourth Amendment protects people, not places." *Id.*

188. S. REP. No. 541, 99th Cong., 2d Sess. at 5.

189. *Id.* at 3 (referring to "large scale electronic mail operations" and many other telephone and communications services).

190. *See* Electronic Communications Privacy Act of 1986, P. L. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2711 (1986)).

191. *See supra* note 10 (explaining how e-mail operates); *see also* Branscomb, *supra* note 69, at 157 (stating that BBS's are "analogous to mail, conversations, chitchat or meetings"); Appellants' Brief, *supra* note 1, at 13-14 (analogizing the Secret Service's act of taking the BBS containing private unread e-mail to the Secret Service taking a blue mailbox off the street); Amicus Curiae Brief, *supra* note 15, at 10 (stating that sending e-mail is analogous to the act of addressing a letter and dropping it into a mailbox for delivery by the U.S Postal Service).

192. *See* United States Postal Service Act, 18 U.S.C. § 1702-1708 (1948) (*as amended by* Act of Sept. 13, 1994, P. L. 103-322, § 330016 (1)(I), which substituted "under this title" for "not more than $2,000," wherever appearing). Congress amended the U.S. Postal Service Act to impose higher damages upon individuals in violation of the statute. *See* P. L. 103-322, § 330016 (1)(I) (1994). Congress increased the damages amount to comport with inflationary and cost of living changes. *Id.*

193. Amicus Curiae Brief, *supra* note 15, at 11-12, *citing* 131 CONG. REC. 11,795 (1985) (statement of Sen. Leahy).

level of privacy protection granted to U.S. Postal Mail. Moreover, if the court considered the postal laws, it would have broadened the scope of the Federal Wiretap Act to protect private unread e-mail stored on a BBS from unlawful interception.

For example, section 1702 of the U.S. Postal Service Laws punishes any person who obstructs correspondence.[194] Under the Act, a person obstructs correspondence if he "takes any letter . . . out of any post office or any authorized depository for mail matter . . . before it has been delivered to the person to whom it was directed."[195]

Case law clarifying the U.S. Postal laws indicates that a letter is subject to obstruction until the addressee actually holds the correspondence in his hand. The postal laws protect correspondence between sender and addressee from theft or taking until the correspondence is manually delivered to the addressee;[196] the letter must reach the person to whom it is addressed.[197] Moreover, it is illegal to take any letter from an authorized depository or mailbox before the post office has delivered it to the person to whom it is addressed.[198] The postal laws protect a letter from illegal taking even if the Post Office has delivered it to the address of the intended recipient.[199]

If the Fifth Circuit had applied the postal laws to the *Jackson Games* case, it would have determined that private unread e-mail stored on a BBS is subject to interception until the intended recipient personally retrieves the mail from the BBS mailbox. The Secret Service's act of taking the Illuminati BBS that contained unread e-mail is comparable to an act of illegally taking 162 private mailboxes from citizens' homes that contain delivered, unread postal mail.[200] E-mail delivery to a BBS should not free the government from the provisions of the Federal Wiretap Act. The Fifth Circuit should have found that the Federal Wiretap Act protected the private unread e-mail from unlawful interception until the intended recipients retrieved and read their mail.

Finally, the Fifth Circuit correctly determined that the requirements for intercepting electronic communications differ significantly

194. 18 U.S.C. § 1702 (1994).

195. *Id.* The punishment for violating the Postal Service Act is five years in prison or a monetary amount determined by the court, but not less than $2,000. *Id.* Punishment under the Postal laws is significantly higher than the punishment under the Stored Wire Act. *See supra* note 19 for relevant text of Stored Wire Act.

196. United States v. Wade, 364 F.2d 931 (6th Cir. 1966).

197. Devine v. United States, 278 F.2d 552 (9th Cir. 1960).

198. United States v. Ashford, 530 F.2d 792 (8th Cir. 1976).

199. United States v. Murray, 306 F. Supp. 833 (D. Md. 1964).

200. Reply Brief, *supra* note 173, at 1; Amicus Curiae Brief, *supra* note 15, at 10-11.

from the requirements for accessing stored communications;[201] Congress implemented tougher requirements to intercept a communication under the Federal Wiretap Act than it imposed to access a stored communication under the Stored Wire Act.[202] For example, the Wiretap Act requires the government to obtain a court order before it may intercept an electronic communication.[203] The Wiretap Act also contains a list of six comprehensive elements that the government must address in its application for the court order.[204] For example, the government must prove that it exercised other investigative means prior to its application for the court order.[205] Alternatively, the provisions of the Stored Wire Act only require the government to obtain a warrant to access communications in storage for less than 180 days.[206]

In addition, the damages are much greater for a governmental violation of the Wiretap Act than the damages for a violation of the Stored Wire Act.[207] The Wiretap Act states: "[t]he court may assess . . . statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000."[208] The Stored Wire Act only awards damages for "the actual damages suffered by the plaintiff . . . but in no case shall a person entitled to recover receive less than the sum of $1,000."[209]

The *Jackson Games* court inaccurately concluded that the differences between the two statutes indicate that Congress did not intend law enforcement officials to abide by the higher restrictions of the Federal Wiretap Act to access electronic communications located in electronic storage.[210] Congress amended the Wiretap Act to protect the contents of any transfer of electronic data from illegal interception.[211] Furthermore, Congress implemented higher standards under the Wiretap Act to assure computer users that information they wished to transfer would reach the intended recipient.[212] The Federal Wiretap Act protects an individual's right to receive information, not the location of the commu-

201. *Jackson Games*, 36 F.3d at 463. *See* 18 U.S.C. §§ 2703, 2704, 2518; *see also* Amicus Curiae Brief, *supra* note at 12; Reply Brief, *supra* note 173, at 3; Letter Brief, *supra* note 170, at 2-3.

202. *See generally* 18 U.S.C. §§ 2701-2711, 2510-2521.

203. 18 U.S.C. § 2518(1).

204. 18 U.S.C. § 2518(1)(a)-(f).

205. 18 U.S.C. § 2518(1)(c).

206. 18 U.S.C. § 2703(a); *See also* Reply Brief, *supra* note 173, at 3-4.

207. 18 U.S.C. § 2707(c); *see also* Appellants' Brief, *supra* note 1, at 16 n.4; Letter Brief, *supra* note 170, at 2-3.

208. 18 U.S.C. § 2520(c)(2)(B).

209. 18 U.S.C. § 2707(c).

210. *Jackson Games*, 36 F.3d at 463.

211. 18 U.S.C. §§ 2518-2521.

212. *See* H.R. REP. No. 647, 99th Cong., 2d Sess. at 7; S. REP. No. 541, 99th Cong., 2d Sess. at 1; *see also* 18 U.S.C. §§ 2510-2521.

nication or the form in which the communication exists.[213] Since the Secret Service prevented the intended recipients from receiving the e-mail sent to them, the court should have held that the Secret Service violated the Federal Wiretap Act. Regardless of whether the unread e-mail existed in storage on the BBS or was actually transmitting from one computer to another at the time of the seizure, the Secret Service intercepted the communication.

The existence of higher standards for governmental interception of electronic communications, and substantially greater damages awards under the Wiretap Act, indicates the importance Congress placed on protecting computer users' privacy.[214] Moreover, the House and Senate reports reflect Congress' intent to afford e-mail privacy protection comparable to that of first class mail and telephone communications.[215] Hence, the Fifth Circuit's decision fails to protect individuals' privacy interests contrary to Congressional intent. If the Fifth Circuit had closely examined the legislative history and intent of the ECPA, the court would not have limited the applicability of the Federal Wiretap Act. Instead, the *Jackson Games* court would have determined that the Secret Service intercepted the 162 pieces of private unread e-mail that existed on the BBS at the time of the seizure pursuant to the Wiretap Act.

C. The Plain Meaning of "Intercept"

When the Fifth Circuit decided the *Jackson Games* case, it disregarded the plain meaning of the word "intercept," and focused on the statutory language of the ECPA.[216] However, if the court had considered the plain meaning of the word intercept in conjunction with the statutory definitions of the ECPA, it would have determined that the Secret Service intercepted the unread e-mail when it prevented the intended recipients from receiving their private mail.[217]

"Intercept" is commonly defined in several ways: (1) to prevent or hinder; (2) to stop, seize, or interrupt in progress or course or before arrival; or, (3) to interrupt communication, or connection with.[218] In addition, "intercept" means the "taking or seizure by the way or before

213. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (stating that "the Fourth Amendment protects people, not places").

214. H.R. Rep. No. 647, 99th Cong., 2d Sess. at 17-19, 30; S. Rep. No. 541, 99th Cong., 2d Sess. at 3-6; Amicus Curiae Brief, *supra* note 15, at 7-8, 11-13; Reply Brief, *supra* note 173, at 3-4; Letter Brief, *supra* note 170, at 1-3.

215. H.R. Rep. No. 647, 99th Cong., 2d Sess. at 17-19, 30; S. Rep. No. 541, 99th Cong., 2d Sess. at 3-6.

216. *Jackson Games*, 36 F.3d at 461.

217. *See* Amicus Curiae Brief, *supra* note 15, at 13 (arguing that seizure of messages prior to arrival at their destination is an interception).

218. Webster's Ninth New Collegiate Dictionary 630 (1988).

arrival at destined place."[219] For example, in the American game of football, a player who prevents an opponent from receiving or catching the football by catching the football himself makes an interception.[220]

When the plain meaning of the word intercept is applied to the facts of the *Jackson Games* case, it is clear that the Secret Service intercepted the 162 pieces of unread private e-mail. The Secret Service prevented the intended recipients from receiving and reading their private e-mail.[221] Furthermore, the Secret Service seized or interrupted the electronic process of the e-mail before it completed its final transmission and before the e-mail reached its intended destination.[222] Thus, the Fifth Circuit should have concluded that the Secret Service violated the Federal Wiretap Act.

Each of the plain language definitions of intercept apply to the conduct of the Secret Service. However, the Fifth Circuit overlooked the application of the plain meaning of intercept when it decided the *Jackson Games* case. Instead, the Fifth Circuit erroneously relied on the statutory definitions of the ECPA.[223] Consequently, the *Jackson Games* court mistakenly concluded that the term "intercept" does not apply to the seizure of private unread e-mail messages sent to a BBS but not yet accessed, read, stored, or deleted by the intended recipients.[224]

D. Prior Case Law

Jackson Games was the first case to test the meaning and applicability of the ECPA with regard to e-mail and BBSs. Even so, when the district court decided the interception issue in *Jackson Games*, it relied substantially upon *United States v. Turk*, which provides an interpretation of the term intercept as applied to oral communication.[225] Although *Turk*, decided in 1976, predates the ECPA and interprets "intercept" in accordance with the older version of the Federal Wiretap Act,[226] the case remains useful to courts interpreting the term intercept. *Turk's* interpretation of the term intercept survives because Congress retained the original statutory definition in the amended Wiretap Act of 1986.[227] Nevertheless, the Fifth Circuit disregarded the importance of *Turk*, and

219. Black's Law Dictionary 811 (6th ed. 1990).

220. Appellants' Brief, *supra* note 1, at 13.

221. Amicus Curiae Brief, *supra* note 15, at 9.

222. *Id.*

223. *See* 18 U.S.C. § 2510.

224. *Steve Jackson Games*, 36 F.3d at 461-62, 463.

225. United States v. Turk, 526 F.2d 654 (5th Cir. 1976), *cert. denied*, 429 U.S. 823 (1976).

226. *Id.* at 657-58.

227. *Jackson Games*, 816 F. Supp. at 442 (stating that "Congress intended no change in the existing definition of intercept" when it amended the statute in 1986).

relied solely upon the statutory definitions contained in the ECPA. Considering that the lower court relied almost exclusively upon *Turk*[228] when it concluded that the Secret Service did not intercept the e-mail, the Fifth Circuit should have reviewed the district court's reasoning.

In *Turk*, police officers arrested two men for transporting cocaine and firearms.[229] The police recovered a cassette tape among items removed from one defendant's car at the time of the arrest.[230] Subsequently, the police played the tape and listened to a recorded conversation between the defendants.[231] The defendants sued, claiming that the officers illegally intercepted their private conversation under the Federal Wiretap Act.

The *Turk* court analyzed the meaning of "intercept" using the definition expressed in the Federal Wiretap Act[232] to decide if the police violated the statute and intercepted the conversation when they listened to the tape.[233] At that time, the Federal Wiretap Act stated that "intercept" meant an "aural acquisition of the contents of any . . . oral . . . communication through the use of any . . . device."[234] The court stated that an acquisition refers to "activity" at the time of the communication.[235] The court determined that an acquisition amounts to an interception[236] only when the person responsible for acquiring the conversation is the same person accused of violating the statute.[237] The court concluded that the police did not "intercept" the oral communication because they did not acquire it contemporaneously with its making.[238] Consequently, the *Turk* court held that the replaying of a recorded conversation did not amount to an interception within the meaning of the Federal Wiretap Act.[239]

When the district court decided the *Jackson Games* case it analogized the prerecorded conversation in *Turk* to the e-mail messages contained on Illuminati. The court determined that the Secret Service did

228. *Jackson Games*, 816 F. Supp. at 441-42.

229. *Turk*, 526 F.2d at 656.

230. *Id.*

231. *Id.*

232. *Turk*, 526 F.2d at 657-58; *see supra* notes 18-19 (detailing the relevant text of the ECPA, 18 U.S.C. §§ 2510-2521, 2701-2711).

233. *Turk*, 526 F.2d at 657-58; *see supra* note 18 (citing text of the Wiretap Act, 18 U.S.C. §§ 2510-2521).

234. *Turk*, 526 F.2d at 656 (quoting the pre-amendment 18 U.S.C. § 2510(4) (1968)).

235. *Id.* at 658.

236. *See supra* note 115 (defining statutory meaning of the term "intercept," 18 U.S.C. § 2510(4)).

237. *Turk*, 526 F.2d at 659.

238. *Id.* at 658.

239. *Id.* at 659; *see supra* note 18 (listing relevant text of the Wiretap Act, 18 U.S.C. §§ 2510-2511).

not intercept the e-mail because it did not acquire the communications contemporaneously with their transmission.[240] However, the district court failed to acknowledge the factual distinctions between the two cases. The *Turk* holding applies only to prerecorded conversations subsequently replayed.[241] In contrast, the *Jackson Games* case involved unread e-mail messages.[242] Although the Fifth Circuit addressed only the issue of whether the seizure of the BBS containing unread e-mail amounted to an interception under the Federal Wiretap Act, the court should have reviewed *Turk* and the lower court's opinion in its entirety. By failing to examine the lower court's analysis, the Fifth Circuit implicitly accepted the district court's faulty comparison of *Turk's* prerecorded conversation to the e-mail of *Jackson Games*.

When a computer user sends an e-mail message, it rests within the BBS's mailbox until the intended recipient is notified of receipt, retrieves, and finally reads the message.[243] However, if the e-mail remains unread within the BBS, the intended recipient has not yet "played it."[244] A prerecorded conversation amounts to a completed conversation between individuals; unreceived, unread e-mail messages do not. Hence, replayed recorded communications and unread e-mail messages are not analogous.

Notwithstanding the difference between replayed prerecorded communications and unread e-mail, the Fifth Circuit should have applied the *Turk* definition of interception[245] to the *Jackson Games* case. The *Turk* court stated that a contemporaneous acquisition requires that the acquisition of a communication and the act of communication occur simultaneously.[246] Applying this definition of intercept, the *Turk* court ruled that a person who merely replays a conversation does not intercept it, unless the person participated in its original recording.[247] Therefore, the *Turk* court held that replaying a pre-recorded conversation is not an interception[248] under the Federal Wiretap Act.[249]

---

240. *See Jackson Games*, 816 F. Supp. at 442.

241. *Turk*, 526 F.2d at 657-58.

242. Reply Brief, *supra* note 173, at 1.

243. Reply Brief, *supra* note 173, at 2.

244. *See generally Turk*, 526 F.2d at 657-58 (stating that police did not intercept the communication when they listened to a conversation previously recorded on a cassette tape). The officers merely "replayed" the conversation. *Id.* at 658. *Turk* held that the police did not intercept the defendants' conversation because the police did not *acquire it contemporaneously* (emphasis added by author); *see also* Appellants' Brief, *supra* note 1, at 14; Reply Brief, *supra* note 173, at 2.

245. *See supra* note 115 (quoting statutory definition of intercept, 18 U.S.C. § 2510(4)).

246. *Turk*, 526 F. 2d at 658.

247. *Id.*

248. *See supra* note 115 (statutory definition of intercept, 18 U.S.C. § 2510(4)).

Unlike the circumstances of *Turk*, the Secret Service acquired the unread e-mail from SJG contemporaneously with its initial dispatch from sender to intended recipient. An unread e-mail message is "in-transit" until it reaches its final destination.[250] For example, after an e-mail message is sent to an intended recipient, the e-mail remains subject to final transmission until the intended recipient actually receives notification of mail, accesses the e-mail service, and retrieves the message from the BBS mailbox and reads it.[251] The Secret Service illegally intercepted 162 pieces of e-mail still in the process of transmission because the e-mail existed in an unretrieved and unread state on the BBS.[252] If the Fifth Circuit had properly applied *Turk's* contemporaneous acquisition interpretation of the Federal Wiretap Act,[253] the court would have determined that the Secret Service intercepted the private and unread e-mail in clear violation of the Federal Wiretap Act when it seized the Illuminati BBS.

VI. CONCLUSION

In *Jackson Games*, the Fifth Circuit disregarded Congressional intent to provide higher privacy protection for e-mail. In 1986, Congress specifically amended the original Wiretap Act to include protection for electronic communications.[254] Moreover, the House and Senate Reports repeatedly express a desire to provide the same high level of protection for e-mail as current federal law provides for telephone communications and first class mail.[255]

Nevertheless, the Fifth Circuit's opinion limits e-mail protection. The court held that e-mail contained in electronic storage on a BBS, regardless of whether it is read or unread, is subject only to the meager protections of the Stored Wire Act.[256] The opinion fails to acknowledge that a greater intrusion occurs when government precludes an individ-

249. *Turk*, 526 F.2d at 659. *See supra* note 18 (citing relevant text of the Wiretap Act, 18 U.S.C. §§ 2510-2521).

250. *See* Appellants' Brief, *supra* note 1, at 6 (stating that "in-transit" in connection to unread e-mail means "sent but not yet received"); *see also* Reply Brief, *supra* note 173, at 4 (discussing the e-mail at issue as "in-transit" communication); Letter Brief, *supra* note 170, at 3 (arguing that the issue in *Jackson Games* is whether intentional seizure and destruction of in-transit electronic communication amounts to an interception" under the Wiretap Act).

251. Appellants' Brief, *supra* note 1, at 5.

252. *See* Appellants' Brief, *supra* note 1, at 6; *see also* Amicus Curiae Brief, *supra* note 15, at 9.

253. *See supra* note 18 (citing relevant text of the Wiretap Act, 18 U.S.C. §§ 2510-2521).

254. H.R. REP. No. 647, 99th Cong., 2d Sess., at 7; S. REP. No. 541, 99th Cong., 2d Sess., at 1.

255. *See supra* notes 185-93 and accompanying text.

256. *Jackson Games*, 36 F.3d at 461-62.

ual from receiving a communication than when it merely accesses a completed message.[257]

In addition, the *Jackson Games* decision indicates that the heightened protection provided by the Federal Wiretap Act only applies to e-mail that is actually transmitting between computer terminals.[258] Because e-mail transmits from the sender to the BBS mailbox almost instantaneously, it is nearly impossible for e-mail to be "intercepted" within the Fifth Circuit's interpretation of the Federal Wiretap Act. Thus, the Fifth Circuit's decision makes the Federal Wiretap Act virtually inapplicable to e-mail.

More importantly, the *Jackson Games* decision allows the government to seize private unread communications with relative ease. Subject only to the requirements of the Stored Wire Act, the government may interrupt the free flow of communication, searching and seizing BBSs and e-mail, without facing the risk of federal violations which carry substantial fines.

Clearly, the law must not cripple government efforts to combat the growing problem of computer crime.[259] Businesses and individual computer users need protection from hackers who illegally break into increasingly complex and expensive computer information and communications systems. However, the law cannot allow the government to disregard computer users' constitutional speech and privacy rights in its quest to deter crime.[260] Otherwise, the government deprives citizens of the very protection that the laws propose to provide. As our society enters a new era of technological change, we must not leave our civil liberties behind.

NICOLE GIALLONARDO

257. Appellants' Brief at 16 n.4.

258. *Jackson Games*, 36 F.3d at 463.

259. *See supra* note 61 (discussing the magnitude of computer crime).

260. Mitchell Kapor, *Civil Liberties in Cyberspace: When Does Hacking Turn From an Exercise of Civil Liberties Into Crime?*, SCIENTIFIC AMERICAN, Sept. 1991, at 164; *see also* Amicus Curiae Brief at 3-4.