UIC Law Review

Volume 27 | Issue 4 Article 6

Summer 1994

PC Peep Show: Computers, Privacy, and Child Pornography, 27 J. Marshall L. Rev. 989 (1994)

John C. Scheller

PC PEEP SHOW: COMPUTERS, PRIVACY, AND CHILD PORNOGRAPHY

INTRODUCTION

Child pornography is a thriving industry.[1] Typically, child pornography is available only through underground networks.[2] These networks effectively escape the reach of the law because they operate covertly.[3] However, the underground networks have inherent limitations because, until recently, pornographic depictions occured mainly in the forms of magazines and videotapes.[4] As a result, the distribution of child pornography required physical transportation and delivery.

Today, however, the child pornography industry is much more technologically advanced. Computers, while introducing society to advanced modes of communication,[5] now enable individuals to view children engaged in explicit sexual behavior.[6] As a result, the child pornography industry is expanding at an alarming rate. The computer makes child pornography easily accessible because it does not require physical transportation. Further, the computer enables

1. ATT'Y GEN. COMM'N ON PORNOGRAPHY, FINAL REPORT 595-96, 628-34 (1986) [hereinafter FINAL REPORT]. *See The Use of Computers to Transmit Material Inciting Crime: Hearings Before the Subcomm. on Security and Terrorism, Senate Judiciary Comm.*, 99th Cong., 1st Sess. 28 (1985) (testimony of Sen. Paul S. Trible) (stating that pedophiles continually exploit new communications technology to assist in the transmission of child pornography).

2. Osborne v. Ohio, 495 U.S. 103, 110 (1990). See *infra* notes 87-90 and accompanying text for a discussion of the "underground" nature of child pornography.

3. FINAL REPORT, *supra* note 1, at 409-10.

4. FINAL REPORT, *supra* note 1, at 409.

5. For a history of communication, see COMMUNICATION & LANGUAGE: NETWORKS OF THOUGHT & ACTION (Sir Gerald Barry et al. eds., 1965). "Communication theory, as it is called, is now one of the basic areas of research into human recourse and understanding." *Id.* at 16. *See* RONALD R. THOMAS, UNDERSTANDING TELECOMMUNICATIONS 14 (1984) (noting that the computer has become the primary instrument for communication since the computer transformed the telephone switching system).

6. *See* Sen. Paul S. Trible, *How to Protect Electronic Speech*, WASH. POST, Jan. 16, 1986, (Letters), at A20 (noting that child molesters use computers to maintain records as well as anonymity.) *See also* FINAL REPORT, *supra* note 1, at 629 (citing Miami Hearing, Vol. I, Paul Hartman, p. 105). "Recently however, pedophile offenders and child pornographers have begun to use personal computers for communications. A person may now subscribe to an information service whereby he or she can contact other subscribers." *Id.* Further, the United States government has seen an explosion of pedophilic activity within the computer field in relation to the distribution of child pornography. *Agents Raid 40 Sites in Child Porn Crackdown*, DET. FREE PRESS, Mar. 5, 1993, at 1A. Federal agents raided 40 locations on March 4, 1993, in an effort to chip away at computer child pornography rings. *Id.*

thousands of individuals to communicate while maintaining the secrecy and covert nature of the underground networks.[7] It is not surprising, then, that computers have replaced magazines and videotapes as the primary means of distributing child pornography.[8]

The computer has emerged as a private peep show in part as a result of inadequate legal guidelines.[9] The computer bulletin board system (BBS),[10] which is the most popular avenue of communication within the computer arena, facilitates this "peep show."[11] BBS

---

7. Charles Babbage is attributed with first envisioning the idea of a device which could calculate mathematics. JOHN CASE, DIGITAL FUTURE: THE PERSONAL COMPUTER EXPLOSION, WHY IT'S HAPPENING AND WHAT IT MEANS 21, 23 (1985). He presented the idea in a paper entitled "On the Theoretical Principles of the Machinery for Calculating Tables" in 1822. *Id.* However, Henry Hollerith developed the first machine that actually counted; he eventually established a company that evolved into today's International Business Machines. *Id.* For a general history of computers and the early inventors, see DAVID RITCHIE, THE COMPUTER PIONEERS (1986).

8. Vicki Torres, *New Puzzle: High-Tech Pedophilia*, L.A. TIMES, Mar. 5, 1993, at M3. BBS users obtain Graphic Interchange Formats (GIFs), which are digitized pictures of magazine photographs and can be viewed on high resolution color screens. Marc Freeman, *Upper Makefield Looks into the Legality of Computer Business; The Home-Based Bulletin Board Service Includes some X-Rated Images*, PHIL. INQUIRER, Mar. 7, 1993, at BCO1. "And with computer technology becoming more sophisticated, offering three-dimensional graphics, digital sound and high-resolution color monitors, the sexually explicit material looks and sounds much like a movie." Susan Kuczka, *Kids, Computers, and Porn*, CHI. TRIB., Aug. 6, 1993, at 1.

9. FINAL REPORT, *supra* note 1, at 630-31. *See also* Michael Ollove, *In Hunt for Sex Criminals, Police Cruise the Silicon Circuit*, PHIL. INQUIRER, July 26, 1993, at BO1. Not only do pedophiles use the BBS to find youngsters, but there are cases where a pedophile has even created a Star Trek board in order to find young people. *Id.*

10. A BBS can be created with a computer which has bulletin board software and a modem which is connected to a phone. Erik Delfino, *The Basics on Setting up an Electronic Bulletin Board System*, ONLINE, Mar. 1993, at 90. Individuals who wish to connect to the BBS can simply dial the BBS through their modem. *Id.* Although a BBS may be focused on a specific field or topic, many BBS networks allow users to communicate on a variety of subjects. *Id.* The five major online services are CompuServe, America Online, Prodigy, GEnie, and Delphi. Rosalind Resnick, *Exploring the Online World: Five Comprehensive Online Services Surveyed: Which is the Best for your Business?*, HOME OFFICE COMPUTING, Feb. 1993, at 72. CompuServe boasts over one million members and allows users to access databases and publications. *Id.* America Online has 200,000 members and offers free software which can be downloaded to a personal computer. *Id.* Prodigy, owned by IBM and Sears, advertises itself as a family service and provides a variety of services including online shopping and personal-finance information and advice. *Id.* at 73. GEnie specializes in business and investment information, but also provides a wide variety of services. *Id.* Delphi offers similar services in business and investment information. *Id.* For a comprehensive overview of computer bulletin boards, see ALFRED GLOSSBRENNER, THE COMPLETE HANDBOOK OF PERSONAL COMPUTER COMMUNICATIONS: EVERYTHING YOU NEED TO KNOW TO GO ONLINE WITH THE WORLD (1983).

11. For a discussion of the inability of the law to keep pace with the burgeoning computer technology, see Jonathan Gilbert, Comment, *Computer Bulletin Board Operator Liability for Users' Misuse*, 54 FORDHAM L. REVIEW 439, 439

networks are popular because they are inexpensive, yet extremely powerful tools for communication.[12] The BBS networks are especially attractive to pedophiles because they not only provide a forum for pedophiles to transmit child pornography, but also offer the added benefits of secrecy and anonymity.[13]

A number of statutes attempt to regulate the transmission of child pornography.[14] However, the current legislation is ineffective because it does not specifically address the transmission of child pornography over computer networks. Therefore, in order to eliminate the thriving child pornography industry, Congress must implement aggressive legislation specifically designed to address this problem.

This legislation must also consider the privacy concerns of the BBS users who are not participating in unlawful activity. These legitimate BBS users argue that their constitutional right to privacy outweighs the state's interest in eliminating child pornography, and thus, protects their communications from governmental surveillance. Any legislation which attempts to eliminate the transmission of child pornography over computer networks must properly account for the privacy rights of legitimate BBS users.

This Note examines the recent epidemic of child pornography on BBS networks. Part I describes BBS networks and the emergence of child pornography, as well as computer-generated child pornography,[15] on these systems. Part II discusses the potential

---

(1985) (discussing the liability of bulletin board operators); Edward J. Naughton, Note, *Is Cyberspace a Public Forum?*, 81 GEO. L.J. 409, 411 (1992) (discussing application of the First Amendment to bulletin board arena); John T. Soma et al., Note, *Legal Analysis of Electronic Bulletin Board Activities*, 7 W. NEW ENG. L. REV. 571, 572 (1985) (examining state laws which regulate the liability of a sysop). *See also* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (dismissing a libel action against a computer service for libel). Some boards which have been established are "pirate boards." JUDY BARRETT, JOYS OF COMPUTER NETWORKING: THE PERSONAL CONNECTION HANDBOOK 45 (1984). These boards are established to allow their users to access and duplicate copyrighted software and other material. *Id.* Another practice on "pirate boards" is "phone phreaking." *Id.* "Phone phreaking" involves obtaining codes to phone companies and charging calls to these codes. *Id.*; *see, e.g.*, Jim Doyle, *FBI Probing Child Porn on Computers*, S.F. CHRON., Dec. 5, 1991, at A23.

12. "Understandably, many people are pessimistic because of our many failures to communicate successfully in spite of the refinements at our disposal, and at the same time, because the dangers of our communicating *too much*." *See* Barry et al., *supra* note 5, at 16.

13. *Child Protection Act: Hearings on H.R. 1704 and Related Bills Before the Subcomm. on Crime of the House Comm. on the Judiciary*, 99th Cong., 2d Sess. 95, 118 (1987).

14. See *infra* notes 146-72 and accompanying text for a discussion of the current legislation which attempts to regulate the transmission of child pornography through computers.

15. Computer-transmitted child pornography is the transmission of actual pornography through a computer. See *supra* notes 6-13 and accompanying text for a discussion of the emergence of child pornography on computers. Com-

conflict between the Fourth Amendment interests of legitimate BBS users and legislation which attempts to eliminate child pornography from BBS networks. Part II also applies a Fourth Amendment analysis to electronic communications and concludes that users do not have a reasonable expectation of privacy when using this medium of communication. Part III examines the failure of current legislation to provide an adequate solution to the problem of computer-transmitted and computer-generated child pornography. Finally, Part IV proposes a new federal statute to prohibit the transmission of child pornography through computer networks.

I. COMPUTERS AND CHILD PORNOGRAPHY

Computers greatly enhance communications between individuals. Unfortunately, child pornography also benefits from computer technology.[16] Section A provides an overview of BBS networks and their role in today's communications. This section also introduces the Clinton Administration's proposal to protect privacy within electronic communications. Section B sets forth the Supreme Court test for obscenity. Finally, Section C discusses society's interest in eradicating child pornography because of its debilitating effects. In addition, this section also discusses the emergence of child pornography on computer networks, particularly the debate over pornographic images generated by the computer itself.

A. Computer Bulletin Boards

A BBS is a simple operation: essentially, it is a computer which allows other computers to connect with it.[17] The BBS receives messages from other computers and allows users to read the messages.[18] The number of users connecting to a BBS can range from a few to thousands.[19] This simple operation allows for quick

puter-generated child pornography is the creation of pornographic images by a computer. See *infra* 75-81 and accompanying text for a discussion of what computer generated child pornography is and the problems it creates for legislation. Computer-generated child pornography are the terms this Note uses to describe the creation of child pornography by a computer. The transmission of child pornography through computers is meant also to imply the transmission of computer-generated child pornography. Thus, this Note will only refer to computer-generated child pornography for emphasis or for direct examination.

16. See FINAL REPORT, *supra* note 1, at 628-34 for a discussion of the abundance of child pornography and communication regarding child pornography on computers. Although federal agents raided over 40 locations in May of 1993 in an effort to cripple the child pornography network, the arrests have revealed that such investigations are only touching the tip of the iceberg. *See Agents Raid 40 Sites in Child Porn Crackdown*, *supra* note 6, at 1A.

17. Delfino, *supra* note 10, at 90-91.

18. JONATHAN D. WALLACE & REES W. MORRISON, SYSLAW: THE SYSOP'S LEGAL MANUAL 9-19 (1988).

19. *Id.* at 1-8.

and expansive communication. A BBS is run by a system operator or "sysop,"[20] who not only monitors the system for security problems, but also conducts routine maintenance checks.[21]

Although the BBS networks provide expansive communication, a BBS is only one part of the vast communication network available through online services.[22] The parent of the BBS networks is Internet.[23] Internet links thousands of BBS networks.[24] The BBS, in turn, is the subsection of the online service which allows communication through a public forum.[25]

In addition to bulletin boards, an online service provides other services which enable users to communicate.[26] For instance, an on-

20. *Id.* The sysop usually is an amateur computer fan. Delfino, *supra* note 10, at 90.

21. WALLACE & MORRISON, *supra* note 18, at 25-26.

22. *See* LAQUEY, *infra* note 24, at 83-84 (noting that online services typically offer a variety of forums for communication). *See also* JOHN S. QUARTERMAN, THE MATRIX: COMPUTER NETWORKS AND CONFERENCING SYSTEMS WORLDWIDE (1990). There are two types of services for computer users: computer-mediated communication and resource sharing. *Id.* at 11. The computer mediated communication services enable users to communicate through either electronic mail, bulletin boards, or conferencing systems. *Id.* at 11-16. The resource sharing service gives users access to various computer databases and files. *Id.*

23. *See* Paul Hilts, *(Inter) Net Effects: Online Services Open Opportunities by Linking PC Users to Worldwide Information Networks*, PUBLISHERS WKLY., June 28, 1993, at 40 (discussing the pervasiveness of Internet and noting that Internet is a computer network which provides access to various databases and networks throughout the world). Delphi provides the easiest access to the Internet of the five major BBS networks. Anthony Gnoffo, Jr., *Prodigy's Problems are its Rivals' Opportunities*, PHIL. INQUIRER, May 16, 1993, at D01. A BBS allows more people to reach each other through online services by acting as a "gateway to national and international hookups like MCI Mail, AT&T Mail, Sprint Mail, and Internet." Vic Sussman, *Communications in New Age*, U.S. NEWS & WORLD REP., Nov. 23, 1992, at 92-93. Internet connects university, government, and industry computers. *Id.*

24. TRACY LAQUEY WITH JEANNE C. RYER, THE INTERNET COMPANION 9 (Keith Wollman & Elizabeth Rogalin eds., 1993). Internet allows users to access thousands of databases throughout the world, usually 24 hours a day. *Id.* at 2. It is estimated that up to 10 million people use Internet to communicate and that as many as 25 million people communicate through Internet and its subsidiary networks. *Id.* at 6. Internet connects over 8,000 networks in 45 countries throughout all the continents. *Id.* Internet fuses the printing press and the telephone by enabling people to communicate and pass information without the use of a middleman or publisher. *Id.* at 2. "This is a new dimension—an electronic, virtual world where time and space have no meaning. . . . The implications of this new global communication and information system are staggering." *Id.* The Internet grew out of a United States Government project aimed at computer networking in 1969. *Id.* at 3. The government still controls various sectors of the Internet, such as NSFNET, run by the National Science Foundation. *Id.* at 27. However, much of the Internet is not controlled by the government but is owned by commercial enterprises. *Id.* at 28.

25. Resnick, *supra* note 10, at 72. *See also* Jolyon Jenkins, *Cyberthreat*, NEW STATESMAN & SOC., May 7, 1993, at 29 (detailing the foundations of computer networks).

26. Delfino, *supra* note 10, at 91.

line service might offer electronic mail (e-mail).[27] E-mail messages provide greater privacy than the posting of messages on BBS networks because a user can send e-mail directly to a party.[28]

E-mail is the most private form of electronic communication because users can secure their e-mail with passwords. However, an outsider may still discover the password and thus, view the e-mail.[29] In order to increase the privacy of e-mail messages, BBS networks and Internet recently developed a system of public-key encryption.[30]

Public-key encryption is the encoding of messages.[31] One system of encryption is called Privacy Enhanced Mail (PEM).[32] With

---

27. A BBS also allows users to view text files or bulletins which the sysop establishes and which do not involve the communications of outside users. *Id.* at 91. A BBS will also allow users to download files to their personal computers. *Id.*

28. Reuven M. Lerner, *Protecting E-Mail*, TECH. REVIEW, Aug.-Sep. 1992, at 11. Although users typically send e-mail with a password known only to the sender and the recipient, it is difficult to prevent other parties from reading the e-mail. *Id.* The e-mail's security is weak because often it will not be received by the intended recipient, usually because of some typo or error in the address. LAQUEY, *supra* note 24, at 122. Further, if the recipient does not view the mail within a short period of time, it will sit within the system, enabling hackers (computer whizzes who explore computer systems and networks, usually for enjoyment) to view it. *Id.* Thus, some have compared the e-mail's security to that of a postcard. *See* Paul Wallich, *Electronic Envelopes?: The Uncertainty of Keeping E-Mail Private*, SCI. AM., Feb. 1993, at 30. The e-mail is only private in that it is not seen by the entire community of BBS users. Delfino, *supra* note 10, at 92.

On a smaller BBS, the sysop will typically be able to view the e-mail passing through the system. A sysop can view the private e-mail of BBS users if he establishes a policy of viewing it and articulates that policy to the BBS users. WALLACE & MORRISON, *supra* note 18, at 19. If the sysop does not establish such a policy, then he cannot view the e-mail. *Id.* Usually, a sysop views the e-mail to prevent the illegal transmission of copyrighted computer games and programs. *Id.*

On the other hand, the large BBS networks and Internet do not view the e-mail of their users. See Resnick, *supra* note 10 and accompanying text for a discussion of the five major BBS networks; *see also* Doyle, *supra* note 11, at A23 (examining the presence of child pornography on America Online and its agent's response that such activity takes place in the private areas, where the company does not monitor the communications). E-mail, then, is more private, especially on the larger BBS networks and Internet, than other forms of communication available on computer networks. This article evaluates the privacy of e-mail within the larger systems. If the proposed legislation can regulate e-mail, which is considered to be the most private of electronic communications, then the proposed legislation will be able to monitor all other forms of electronic communication.

29. LAQUEY, *supra* note 24, at 120.

30. Wallich, *supra* note 28, at 30.

31. *Id.*

32. *Id.* Another program which is attempting to capture public approval is Pretty Good Privacy (PGP). *Id.* "PGP is a possible illegal work of 'guerilla software' originally written by software consultant Philip Zimmermann." *Id.* PGP's philosophy is wholly different than PEM's because the PGP system is based on trust. *Id.* at 32. Users exchange keys with one another or through

PEM, a user has a public key and a private key.[33] A user can send a message to another user by placing the recipient's public key number on the message.[34] In order to view the message, the user must decrypt or decode the message with the private key number.[35] The private key is the only way to access the message.[36] Accordingly, this technology provides greater privacy for e-mail messages.[37]

The Clinton Administration recently proposed a federal system of encrypting messages,[38] called the "Clipper chip."[39] The Clipper chip is an algorithm[40] which prevents individuals outside the intended recipient class from viewing electronic communications.[41] The Clipper chip gives the government a "master key,"[42] which allows officials to decode the messages for security and law enforcement purposes.[43] The Clipper chip affords more privacy protection to electronic communications because it provides individuals with

---

intermediaries, who continue to pass the keys on. *Id.* PEM is not available yet, while PGP is available on both Internet and BBS networks. *Id.*

33. Lerner, *supra* note 28, at 11.

34. Wallich, *supra* note 28, at 32.

35. *Id.* "A user can send secure mail by typing in the recipient's public key. Since the recipient then has to apply his or her private key to decrypt the message, only that person can read the message." Lerner, *supra* note 28, at 11.

36. Wallich, *supra* note 28, at 32.

37. *Id. See* Lerner, *supra* note 28, at 11.

38. Ivars Peterson, *Encrypting Controversy*, 143 SCI. NEWS 394 (1993).

39. *Id.* "[T]he proposed 'key-escrow' technology takes the form of two specially fabricated, tamper-resistant integrated-circuit chips one, known as Clipper, for encrypting digital telephone signals and another, known as Capstone, for encrypting the output of computers." *Id.*

40. An algorithm is "a set of rules for solving a problem in a finite number of steps, as for finding the greatest common divisor." THE RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 52 (2d ed. 1987).

41. Peterson, *supra* note 38, at 395.

42. *Id.*

43. *Id.* Currently the government's system for coding is the Data Encryption Standard (DES). *Id.* at 394-95. DES is a single-key method. *Id.* The government's new proposal is for a two key system which would be released to authorized government officials for security and law enforcement purposes only. *Id.* at 395.

The computer and telephone industries have joined privacy advocates in protesting the implementation of the Clipper chip. *Id.* at 396. Many people have questioned the propriety of the Clinton Administration's proposal and its emphasis on controlling the cryptography market, stating that such centralized regulation of speech may violate the First Amendment. *Id.* The Clinton Administration has momentarily withdrawn the implementation of its proposal until it can further examine the encryption scheme. *Id.* Opponents contend that the Clipper chip grants too much power to the government by equipping it with the means to view electronic communications. In order to view electronic communications, law enforcement must obtain a search warrant. 18 U.S.C. §§ 2511, 2516, 2518, 2703 (1988). The Clinton Administration's proposal provides that the master keys would be given to law enforcement officials only when such officials would be authorized to conduct surveillance. Peterson, *supra* note 38, at 394.

better technology to code their messages.[44]

The Clipper chip complements the statute proposed by this Article because the "master key" supplies the technology needed to intercept electronic communications. The proposed statute will provide the government with the justification to intercept and view these electronically transmitted messages. However, the interception of electronic communications will be strictly limited to the detection of child pornography.

B. Child Pornography

Pornography provides fertile ground for debates about morality and freedom of speech.[45] One argument is that pornography is a social evil and is debilitating to human sexuality.[46] The opposing contention is that the debate over pornography is actually a means of circumventing First Amendment protections.[47] The Supreme Court's numerous confrontations with pornography portray the embittered struggle between these two views.

In *Miller v. California*,[48] the Court noted that an individual does not have a First Amendment right to view pornography when

---

44. Peterson, *supra* note 38 at 394 (citing the White House's announcement of the Clipper chip which "improves 'the security and privacy of telephone communications while meeting the legitimate needs of law enforcement.' "). The Clipper chip has sparked a heated debate between the government and privacy advocates. Philip Elmer-DeWitt, *Battle for the Soul of the Internet* TIME, July 25, 1994, at 50, 54-55. For an excellent discussion of the Clipper chip and it's accompanying controversy, see Steven Levy, *Battle of the Clipper Chip: The Cypherpunk vs. Uncle Sam*, N.Y. TIMES, June 12, 1994, § b (Magazine), at 44.

45. A different, but related, issue which arises within the discussion of computers and child pornography is the ability of children to view pornography on computers. Kuczka, *supra* note 8, at 1. Pornography can be readily obtained through computer networks, and viewed by children who use computers. *Id.* Indeed, teen-age boys often search BBS networks for any subject relating to sex. Ollove, *supra* note 9, at B01 (quoting Warwick, Pennsylvania's police chief, Al Olsen). Illinois has a statute, 720 ILCS 5/11-21 (1993), which covers the transmission of pornography to children. Kuczka, *supra* note 8, at 1.

46. Morality in Media, *Pornography as Obscenity*, *in* PORNOGRAPHY AND SEXUAL VIOLENCE 10, 14 (Gary E. McCuen ed., 1985). Pornography attempts to recreate fantasy and arouse the reader into a surrogate sexual experience which, some contend, eventually dehumanizes the viewer. Ernest van den Haag, *Is Pornography a Cause of Crime?*, *in* THE CASE AGAINST PORNOGRAPHY 161, 163-68 (David Holbrook ed., 1973). Literature, on the other hand, contemplates the importance of the experience, thereby developing the reader. *Id.*

47. Spartist League & Partisan Defense Committee, *Pornography Should Not Be Prohibited*, *in* SEXUAL VALUES: OPPOSING VIEWPOINTS 157, 158-61 (Lisa Orr ed., 1989) (arguing that the First Amendment does not allow the government to censor the people's activities, because of the confining effect that censorship will have on human expression). Another view of pornography is that it is a healthy expression of repressed feeling and fantasy and helps people to become more comfortable with their sexuality, although many psychiatrists doubt the validity of this theory. E. J. Mishan, *The Economic Steam Behind Pornography*, *in* THE CASE AGAINST PORNOGRAPHY, *supra* note 46, at 157.

48. 413 U.S. 15, *reh'g denied*, 414 U.S. 881 (1973).

the material is obscene.[49] The *Miller* Court laid out the following test for determining when pornography is obscene:

> The basic guidelines for the trier of fact must be: (a) whether the 'average person applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[50]

The *Miller* Court recognized that the First Amendment does not protect obscene material.[51] However, the Court warned that the regulation of obscene material is the regulation of expression, and therefore, must be limited.[52] Accordingly, the *Miller* test attempts to balance the harmful effects of obscene pornography against the constitutional right of freedom of expression.[53]

The Court did not directly address the issue of child pornography until 1982, in *New York v. Ferber*.[54] The *Ferber* Court found that the *Miller* obscenity standard did not apply to child pornography[55] because child pornography is *per se* obscene.[56] In *Ferber*, the Court distinguished pornography depicting children from pornography involving adults, and held that the states have more latitude in restricting child pornography.[57] The *Ferber* Court gave five reasons why child pornography is subject to greater censorship than adult pornography:[58] (1) the state has a compelling interest in "safeguarding the physical and psychological well-being of a minor";[59] (2) the creation and distribution of child pornography is

49. Miller v. California, 413 U.S. 15, 24 (1973) *reh'g denied*, 414 U.S. 881 (1973).

50. *Id.*

51. *Id.* at 23. Roth v. United States, 254 U.S. 476, 484-85 (1957), *reh'g denied*, 355 U.S. 852 established that the First Amendment does not protect obscene material. *Miller* developed a new standard for obscenity.

52. *Id.* at 23-24.

53. Many have argued that the community standard basis makes the *Miller* test too indeterminable and difficult to apply. Smith v. United States, 431 U.S. 291, 313-14 (1976) (Stevens, J., dissenting). Justice Stewart best summed up the difficulty when he declared that obscenity is difficult to define but, "I know it when I see it. . . ." Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

54. 458 U.S. 747 (1982). In *Ferber*, the Court held that the test for child pornography was similar to the obscenity test articulated in *Miller*. *Id.* at 764. However, in *Ferber*, the Court found that when applying the test for child pornography the, "trier of fact need not find that the material appeals to the prurient interest of the average person; it is not required that sexual conduct portrayed be done so in a patently offensive manner; and the material at issue need not be considered as a whole." *Id.*

55. New York v. Ferber, 458 U.S. 747, 755-65 (1982).

56. *Id.* at 764.

57. *Id.*

58. *Id.* at 756-64.

59. *Id.* at 756-57 (citing Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982)).

based upon the sexual abuse of children;[60] (3) the ability to make money in the distribution of child pornography provides individuals with the incentive to partake in illegal activity;[61] (4) the value of child pornography is "exceedingly modest, if not de minimis";[62] and (5) child pornography does not fall within the protections of the First Amendment.[63] The most important of these five rationales for stricter censorship of child pornography is the state's compelling interest in protecting children.[64]

C. The State's Compelling Interest in Regulating Child Pornography

The state has a compelling interest in eliminating child pornography because it involves the sexual exploitation of a defenseless class of individuals. The Court in *Jacobsen v. United States*[65] summed up the child pornography problem best. In addressing the need to eradicate this evil, the *Jacobsen* Court stated, "[t]here can be no dispute about the evils of child pornography or the difficulties that laws and law enforcement have encountered in eliminating it."[66]

The evils of child pornography cannot be understated. Child pornography is tantamount to child abuse because it depicts a child engaged in some sort of sexual activity.[67] Typically, this activity can involve other children or adults.[68] Further, child pornography is a "permanent record"[69] of a child's abuse and can haunt the child for years.[70]

Perhaps the most sinister aspect of child pornography is that child abusers use it to lure children to engage in sexual activity.[71] The abuser manipulates the child into believing that sexual activity is acceptable because the children in the pictures are engaged in it.[72] The computer increases these destructive effects because

60. The Court found that child pornography is related to the sexual abuse of children in two ways. *Ferber*, 458 U.S. at 759. First, the photographs record the victim's participation and the child's harm is worsened with the distribution of the material. *Id.* Second, the only way to stop the production of such material is to stop the distribution system. *Id.*

61. *Id.* at 761.

62. *Id.* at 762.

63. *Id.*

64. *Id.* at 776 (Brennan, J., concurring).

65. 112 S. Ct. 1535 (1992).

66. Jacobsen v. United States, 112 S. Ct. 1535, 1540 (1992).

67. FINAL REPORT, *supra* note 1, at 405.

68. *Id.*

69. New York v. Ferber, 458 U.S. 747, 759 (1982).

70. *Id.* n.10. Child pornography goes beyond even the incident because the photograph is a recording of that child's sexual abuse. FINAL REPORT, *supra* note 1, at 411.

71. FINAL REPORT, *supra* note 1, at 411.

72. *Id.*

pedophiles utilize this technology to transmit and receive child pornography anonymously.[73] For these reasons, the emergence of child pornography on computer networks demands spirited legislation.[74]

Nevertheless, opponents of child pornography legislation contend that *Ferber's* "compelling interest" requirement[75] is not applicable to computer-generated child pornography. Computer-generated pornography is the creation of pornographic images by a computer.[76] The "person" in the image is created by the computer, and does not actually exist.[77] Therefore, the images do not exploit actual children.[78]

Opponents of child pornography legislation argue that the justification for eliminating child pornography is the state's interest in

---

73. See *supra* notes 1-15 and accompanying text for a discussion of the emergence of child pornography on computer networks.

74. This article does not weigh society's interest against the limited privacy expectations of legitimate BBS users. However, under this analysis, society's interest in eliminating child pornography outweighs any limited privacy expectation. Society's interest in the disclosure of private information was discussed in United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980). In *Westinghouse,* the court held that an employer had to disclose the medical reports of employees to a research institute where the government showed a proper interest. *Id.* at 579. The court laid out the factors to determine whether "an intrusion into an individual's privacy is justified." The factors to be weighed are: "the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access." *Id.* at 578. Although *Westinghouse* involved the disclosure of a medical record, its reasoning should apply to the disclosure of e-mail because of the similar disclosure sought and the highly sensitive nature of medical records.

In *Ferber,* the Court held that the government's interest in abrogating child pornography is "compelling." 458 U.S. at 756-57. The proposed statute allows law enforcement to view e-mail messages when a slight suspicion arises. Although some of this viewing might encompass glimpses at sensitive information, it is unlikely that any such information will be more sensitive than medical reports. The factors set forth in *Westinghouse* similarly would provide for disclosure of e-mail in an effort to abolish child pornography due to the overwhelming public interest in protecting the victims of child pornography.

75. New York v. Ferber, 458 U.S. 747, 756-57 (1982) (citing Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982)).

76. Joshua Quittner, *Computers Customize Child Porn,* NEWSDAY, Mar. 6, 1993, News, at 74 (quoting special agent Catherine Sanz, "The technology exists to create a pornographic picture and not have a victim."). Although there is presently no evidence that computer-generated child pornography is abundantly present nor that pedophiles are using it to abuse children sexually, the imposition of stricter child pornography laws would probably result in its accelerated use. *Cf.* FINAL REPORT, *supra* note 1, at 602-07 (noting that the child pornography's reaction to various statutes and court decisions was to withdraw to those areas which were unregulated).

77. Quittner, *supra* note 76, at 74.

78. *Id.*

protecting the victim.[79] Because computer-generated child pornography does not have a "victim,"[80] the state does not have a compelling interest. Therefore, say the opponents, the state cannot regulate computer-generated child pornography because an actual child is not victimized.[81]

This argument is flawed because the state's interest in protecting children from the devastating effects of child pornography does not begin and end with the victim.[82] Rather, the state's interest in eliminating child pornography is the protection of all children.[83] Two points support this contention.

First, child pornography "necessarily includes" child abuse.[84] This abuse does not end with the depiction of the child because pedophiles use child pornography to aid in the sexual abuse of other children.[85] Thus, the state's interest in eliminating child pornography is the protection of the child who is directly abused through depiction as a sexual object, as well as the child who may be abused.[86]

Second, legislative and law enforcement attempts to eliminate child pornography in the United States frequently involve the seizure of child pornography from foreign countries.[87] The state's

---

79. *Ferber*, 458 U.S. at 756-57. See *supra* notes 65-74 and accompanying text for a discussion of the state's compelling interest in protecting the well-being of a minor who is a victim of child pornography.

80. Quittner, *supra* note 76, at 74.

81. "When a picture does not constitute child pornography, even though it portrays nudity, it does not become child pornography because it is placed in the hands of a pedophile, or in a forum where pedophiles might enjoy it." United States v. Villard, 885 F.2d 117, 125 (3d Cir. 1989). However, this case involved determining the "lascivity" of a photograph according to 18 U.S.C. § 2256 (1988). *Id.* This discussion assumes the lascivity requirement; otherwise it would not be child pornography.

82. *Cf.* New York v. Ferber, 458 U.S. 747 (1982). "The prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance." *Id.* at 757.

83. *See* FINAL REPORT, *supra* note 1, at 413-14 (noting that child pornography is often used to lure new victims into engaging in sexual conduct).

84. FINAL REPORT, *supra* note 1, at 406. It is well-established that pedophiles use child pornography in order to persuade children to engage in sexual behavior. *Id.* at 411.

85. See *supra* notes 65-74 and accompanying text for a discussion of the continual cycle of abuse that child pornography engenders.

86. In addition, Congress' regulations against child pornography cannot be interpreted as protecting only the victim because the legislation extends to material which is imported into the United States. 18 U.S.C. §§ 2251-52 (1988) pertains to the transportation of child pornography "in interstate or foreign commerce."

87. This fact is well-illustrated by the recent federal raids of BBS networks in an attempt to break up child pornography rings operating in the United States that were receiving foreign-made pornography. *See Agents Raid 40 Sites in Child Porn Crackdown*, *supra* note 6, at 1A (detailing the raid of federal agents on 40 locations to break up a computer child pornography ring). The justification for this raid was Congress' concern over the adverse effects which child pornography creates in the United States. *Id.* The primary adverse effect

interest in seizing foreign-made child pornography is not the protection of foreign children. Rather, the state's interest is the protection of *potential* child victims in the United States. Thus, despite the fact that computer-generated child pornography does not have an actual victim, the state has an interest in eliminating this form of child pornography because of the threat it poses to other children.

Despite the *Ferber* decision[88] holding that the state has a compelling interest in eliminating child pornography, the child pornography industry is thriving. Currently, the computer enhances the "underground" activity[89] of child pornography. Although child pornography is not constitutionally protected, it is extremely difficult to assail because it is concealed.[90] Accordingly, the problem of child pornography and computer-generated child pornography requires vigorous legislation.[91] This legislation however, cannot disregard the privacy rights of legitimate computer users.

II. Privacy Rights of Computer Users

The proposed statute resolves the problem of child pornography on BBS networks by compelling sysops to monitor the transmission of messages regardless of whether probable cause exists.[92] However, while the proposed statute focuses on abolishing child pornog-

---

of child pornography is the great likelihood that it will aid in the further sexual abuse of children. *Id.* Accordingly, computer generated child pornography should be regarded as child pornography because the intent of Congress is to protect all children from the potential abuse which child pornography poses.

88. New York v. Ferber, 458 U.S. 747, 747 (1982).

89. Osborne v. Ohio, 495 U.S. 103, 110 (1990). The child pornography industry has gone underground, where it continues to flourish. *Id.* Child pornography is still available because it has become increasingly difficult to wipe out the industry by only censuring the production and distribution. *Id.* In response to this dilemma, many states have created statutes which forbid the possession of such material. *Id.* at 110-11. Many would argue that the growth of the child pornography industry after *Ferber*, and the implementation of tougher laws, is a natural and foreseeable consequence. *See generally* Larry Flynt, *Educate About Human Sexuality*, *in* Pornography and Sexual Violence, *supra* note 46, at 87 (contending that the solution to the child sexual abuse problem is through legislation and not through the First Amendment).

90. Some groups argue that restraints against child pornography are restraints against individuals' First Amendment rights. Heather Florence, *Don't Trample the First Amendment*, *in* Pornography and Sexual Violence, *supra* note 46, at 94. The ACLU contends that although child pornography is illegal, prosecution of child pornographers and pedophiles is unconstitutional if speech is the vehicle upon which the prosecution is based. *Id.*; *see also* Lorenzo Carcaterra, *Talking with . . . Andrew Vachss*, People Weekly, May 3, 1993, at 32. Andrew Vachss discusses the proposal to decriminalize pedophilia and claims that the groups who promote such positions represent "themselves as child advocates, and this allows them to cloak their activities in the First Amendment." *Id.*

91. Computer-generated child pornography is not considered in any legislation. *E.g.*, 18 U.S.C. §§ 2251-2252, 2256 (1988).

92. *See infra* Appendix.

raphy from BBS networks, it also secures the privacy rights of legitimate users. Nonetheless, legitimate users contend that probable cause is required in order to protect their constitutional right to privacy.[93]

Section A discusses the constitutional right to privacy and analyzes the Supreme Court's test for determining when the Fourth Amendment protects this right. Section B analyzes the expectation of privacy which accompanies e-mail. This analysis specifically focuses on the *Katz v. United States*[94] examination of privacy pursuant to the Fourth Amendment.[95] Finally, Section C evaluates the Electronic Communications Privacy Act[96] (ECPA) and determines that the ECPA does not supply BBS users with a reasonable expectation of privacy.

A. Right to Privacy

The right to privacy[97] is not an enumerated right under the

93. The right of privacy is at question under the proposed statute because sysops can view e-mail regardless of whether probable cause exists. *Cf. Computer Pornography and Child Exploitation Prevention Act, 1985: Hearings on S. 1305 Before the Subcomm. on Juvenile Justice of the Comm. on the Judiciary*, 99th Cong., 1st Sess. 29 (1985) [hereinafter *Hearings*] (testimony of Jack D. Smith, General Counsel, FCC) (asking the legislature to address the privacy rights of computer users under S. 1305). The usual problems surrounding privacy and computers focus on the ability of the government to compile information on an individual's lifestyle, including medical history records. *See* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 576 (3d Cir. 1980) (finding the National Institute for Occupational Safety and Health can obtain employees' medical records for research purposes). *See also* John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 993-1001 (1984) (discussing the government's ability to access personal files and the adversely affected rights of privacy). For instance, the IRS was attempting to evaluate incomes by examining a computerized collection of people's lifestyles. *Id.* at 991.

94. 389 U.S. 347 (1967). See *infra* notes 101-12 and accompanying text for a discussion of *Katz* and privacy expectations under the Fourth Amendment.

95. "The inquiry into whether one can reasonably expect to make communication free from interception is analogous to the inquiry into whether one has a reasonable expectation of privacy, as that term is used in the Fourth Amendment context." Wesley v. WISN Div.—Hearst Corp., 806 F. Supp. 812, 814 (E.D. Wis. 1992).

96. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1849, 1851-53 (codified as amended in scattered sections of 18 U.S.C.).

97. The tort law of privacy emanated from Warren and Brandeis' 1890 law review article, *The Right to Privacy*. *See* 4 HARV. L. REV. 193 (1890). In their article, Warren and Brandeis outlined the "American Tort" without defining the various interests which the tort protected. 2 PRIVACY LAW AND PRACTICE 1.01 (George B. Trubow, ed., 1987) [hereinafter Trubow]. Instead, the article focused on an "inviolate personality." Warren & Brandeis, *supra*, at 205. The article also discussed the "right to be let alone." *Id.* Warren and Brandeis borrowed this idea from Judge Cooley's discourse on torts. Trubow, *supra*, ¶ 1.01. In 1960, William Prosser organized the four causes of action which had been created under the common law's interpretation of privacy. William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). Prosser defined four causes of action in privacy: (1) intrusion upon seclusion; (2) publicity given to private life; (3) pub-

Constitution.[98] Rather, it is a penumbra right which the Constitution implicitly protects.[99] Accordingly, it is difficult to determine when a person has a protectable right to privacy under the Constitution.[100]

In the area of electronic communications, the Fourth Amendment implicitly guarantees the Constitutional right to privacy.[101] In *Katz v. United States*,[102] the Court recognized that the Fourth Amendment did not provide a "general constitutional 'right to privacy.' "[103] However, the Court did find that the Fourth Amendment protects individuals from "certain kinds of governmental intrusion."[104]

Katz arose out of the illegal surveillance of the defendant by means of a recording device on a public telephone booth.[105] In holding that the Fourth Amendment protected people and not places, the *Katz* Court laid the constitutional foundation for privacy in elec-

---

licity placing a person in a false light; and (4) appropriation of name or likeness. These four causes of action have become the modern privacy torts under the Second Restatement of Torts. *Id.* at 389-401.

98. Trubow, *supra* note 97, ¶ 19.02.

99. Griswold v. Connecticut, 381 U.S. 479, 484-85. (1965). In *Griswold*, the Court held that a Connecticut state law which forbade the use of contraceptives to prevent pregnancy was an unconstitutional invasion into marital privacy. *Id.* at 485-86. The *Griswold* Court found that the Constitution creates various "zones of privacy." *Id.* at 484. The Court declared that:

> The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers in any house in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Id.

The Fourteenth Amendment is also applicable to a discussion of privacy, because it makes certain provisions of the Bill of Rights applicable to the states through its Due Process Clause. *See, e.g., id.* at 487-88. (Goldberg, J., concurring).

100. Trubow, *supra* note 97, ¶ 19.02.

101. Katz v. United States, 389 U.S. 347, 350 (1967).

102. 389 U.S. 347 (1967).

103. *Id.* at 350. The Fourth Amendment provides that "[t]he 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. . . ." U.S. CONST. amend. IV.

104. *Katz*, 389 U.S. at 350. The Court recognized that individual privacy can be based upon other provisions of the Constitution including the First, Third, and Fifth Amendments. *Id.* n.4. In addition, the Court has found that a right to privacy can be based upon the Due Process Clause of the Fourteenth Amendment. *See* Roe v. Wade, 410 U.S. 113 (1973).

105. *Katz*, 389 U.S. at 348.

tronic communications.[106] *Katz* created the following two-pronged test to determine whether a person has a protectable privacy interest: 1) the individual must have a "subjective expectation of privacy";[107] and 2) that expectation must be objectively reasonable to society.[108] If an individual establishes both of these requirements, that individual enjoys a "reasonable expectation of privacy"[109] and the government must acquire a warrant before conducting a search. A person who does not possess a reasonable expectation of privacy is not entitled to the protections of a search warrant.

Currently, law enforcement officials can view computer messages pursuant to a warrant when there is probable cause to believe that criminal activity is occurring.[110] The process of obtaining a warrant, however, occasionally grants pedophiles the time needed to close up shop and thus avoid detection.[111] To provide law enforcement with a more suitable vehicle for apprehending these criminals, this Article proposes a statute which compels sysops to view the e-mail of their users regardless of whether probable cause exists.[112] This statute can only be implemented if BBS users do not have a reasonable expectation of privacy.

B. The Warrant Requirement and the Expectation of Privacy within E-mail

In order to determine if the interception of e-mail requires a warrant, one must first determine whether e-mail users have a reasonable expectation of privacy. The telephone and the postal system, well-established areas of communication, provide reasonable expectations of privacy.[113] Opponents of child pornography legislation argue that e-mail is analogous to the telephone and postal system. Therefore, they claim that e-mail users have a reasonable expectation of privacy.[114] However, while e-mail may be similar to

106. *Id.* at 351-52. Although the *Katz* Court did not directly address electronic communications, the protection of people and not places has been adopted in determining the privacy expectation within electronic communications. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).

107. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

108. *Id.*

109. *Id.* at 356 n.16.

110. 18 U.S.C. §§ 2511, 2516, 2518, 2703 (1988).

111. *See generally Hearings*, *supra* note 93, at 11-13 (testimony of Kenneth V. Lanning) (discussing the habits of pedophiles in collecting and organizing child pornography and the difficulty law enforcement officials face in policing the pedophiles' activity).

112. *See infra* Appendix.

113. *See* H.R. REP. No. 99-647, 99th Cong., 2d Sess. 26-27 (1986) (discussing the privacy afforded to various communications in an analysis of the Electronic Communications Privacy Act).

114. *Id.* at 22. The House Report states that the expectation of privacy within e-mail has not been established in any court case. *Id.* The House report

the postal system and the telephone in some respects, a number of fundamental differences exist.

First, unlike the government-run postal system, e-mail is not subject to government regulation because private parties provide it.[115] BBS users contend that the lack of government regulation enables them to enjoy a reasonable expectation of privacy. However, government regulation or surveillance is not the basis for determining whether individuals have a reasonable expectation of privacy.[116] If this were the accepted test, the lack of government regulation would always create a privacy right.[117]

Second, legitimate users contend that e-mail is the transmission of a private conversation[118] similar to a telephone communication.[119] Because the Fourth Amendment protects the telephone,[120] any unwarranted breach into telephone communications is an illegal act.[121] Thus, legitimate BBS users argue that the Fourth Amendment protects e-mail in a similar fashion.

This argument is invalid because e-mail differs from telephone communications in many ways. Unlike a telephone communication, e-mail can linger in a communications system for an indeterminate period of time.[122] Moreover, e-mail transmits textual data and not oral communications.[123] Accordingly, e-mail's use of different telecommunication lines to transmit textual data distinguishes it from telephone communications.[124]

Additionally, e-mail is only a private transmission within the

---

indicates that e-mail should be found to possess a reasonable expectation of privacy. *Id.* However, the report states that such interpretation is speculative. *Id.*

115. *Id.* E-mail is an interactive communication, much like a telephone communication. *Id.* Furthermore, e-mail may be copied and viewed by the sysop whereas postal mail cannot. *Id.*

116. *See Katz*, 389 U.S. at 351 (noting that "the Fourth Amendment protects people, not places"). The expectation of privacy is considered only after there has been intrusion or surveillance by the government, and not before that surveillance occurs. *Id.* at 350.

117. *See* Wesley v. WISN Div.—Hearst Corp., 806 F. Supp. 812, 813 (E.D. Wis. 1992) (finding that defendant recorded plaintiff's conversation at work); Bayges v. Southeastern Penn. Transp. Auth., 144 F.R.D. 269 (E.D. Pa. 1992) (determining the ramifications of defendant employer's inadvertent recording of the plaintiff's conversation).

118. S. REP. No. 99-541, 99th Cong., 2d Sess. 3562 (1986).

119. H.R. REP. No. 99-647, *supra* note 113, at 22.

120. *Id.*

121. 18 U.S.C. § 2701 (1988).

122. LAQUEY, *supra* note 24, at 42.

123. *Id.*

124. See H.R. REP. No. 99-647, *supra* note 113, at 22 for a discussion of e-mail's qualities and noting that e-mail is the transmission of textual data. The House Report compares e-mail to mail, but not to telephone communications, implying that e-mail is wholly unlike telephone communications. *Id.*

user's subjective expectation.[125] An e-mail user transmits messages with the expectation that only the intended recipient will receive and view them. Frequently though, a large percentage of e-mail never reaches its destination due to wrong addresses.[126] Furthermore, recipients of e-mail often allow their messages to remain stored in the network for considerable periods of time.[127] This enables hackers to access them.[128] Moreover, the sysop is able to access messages, and typically copies messages for back up purposes.[129] Finally, users know that e-mail is often viewed by individuals outside the intended class of recipients.[130] Given the lack of security, the ability of hackers to view e-mail, the ability of sysops to view and copy e-mail, as well as common knowledge that e-mail is not completely immune from unauthorized access, users cannot have a reasonable expectation of privacy in e-mail communications.

Wesley v. WISN Div.—Hearst Corp.[131] supports this reasoning. In *Wesley*, the district court held that a radio station employee, whose conversation took place in front of a microphone, did not have a reasonable expectation of privacy.[132] The court concluded that "if a person should know that [his] comments could be artificially detected without too much trouble, or that the means of artificial detection might actually be in place, the person's expectation of

125. Although a user may subjectively believe that the e-mail is private because that person may code the e-mail, this belief is not validated by the typical occurrences which occur within the BBS networks, including the viewing of e-mail messages by many individuals beyond what is expected. See *supra* notes 113-24 and accompanying text discussing that e-mail is not a solely private communication.

126. LAQUEY, *supra* note 24, at 49-50.

127. *Id.* at 50, 122.

128. Hackers are computer whizzes who explore computer networks and systems in an effort to expand their knowledge on computers. *Id.* at 119. On many BBS networks, there are even instructional "cookbook" recipes on how to break into a system and view information. *Id.* Although hacker is a term used frequently by the media to portray individuals who cause damage to systems, a hacker is actually respected in the computer world because the term refers more to a innocent explorer of computers. *Id.* at 118. "Cracker" is the terminology in computer lingo for a person who invades systems and does damage. *Id.* However, this Note will use the term hacker because its usage is so well-known.

129. *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice, House Judiciary Comm.*, 99th Cong., 1st and 2d Sess., 20 (1986) (testimony of Philip M. Walker).

130. See generally LAQUEY, *supra* note 24, at 122, for an examination of the security of e-mail. For a discussion of the obstacles present in protecting one's e-mail from being viewed by others, see Lerner, *supra* note 28, at 11.

131. 806 F. Supp. 812 (E.D. Wis. 1992).

132. Wesley v. WISN Div.—Hearst Corp., 806 F. Supp. 812, 815 (E.D. Wis. 1992). The court found that the reporter's communication was "subject to interception" if it was "readily or practically capable of being intercepted," in accordance with the terminology of Title II of the ECPA. *Id.*

non-interception is [un]reasonable."[133]

E-mail messages are similar to the conversation in *Wesley* for a number of reasons. First, e-mail is subject to detection without too much trouble and the means for detection are in place because sysops can easily view the transmissions of users.[134] In addition, hackers frequently use their own computers to view others e-mail.[135] Finally, because users often transmit e-mail within a BBS network, users know that others on the network can view their messages. Therefore, under *Wesley*, an e-mail user does not possess a reasonable expectation of privacy.[136]] Although BBS users may not have a reasonable expectation of privacy under the Fourth Amendment, they contend that the ECPA protects their transmissions from disclosure. Therefore, legitimate users argue that the ECPA actually creates a reasonable expectation of privacy in e-mail.

C. *Electronic Communications Privacy Act*

The ECPA provides various protections for users of electronic communication services.[137] The relevant provision for this discussion is Title I,[138] which applies to the interception of wire and electronic communications.[139]

Title I recognizes that electronic communications, such as e-mail, are often unintentionally intercepted through "mechanical or safety quality control checks."[140] These unintentional interceptions may reveal information which "appears to pertain to the commission of a crime."[141] When this occurs, the intercepting party can divulge that information to law enforcement.[142] Otherwise, the government must obtain a court order to regulate electronic

133. *Id.*

134. See *supra* note 129 and accompanying text for a discussion of sysops' ability to view BBS users' e-mail.

135. LAQUEY, *supra* note 24, at 116-22.

136. An e-mail user cannot have a reasonable expectation of privacy because the communication can be detected without too much trouble. See *id.* at 122, for a discussion of the ability of individuals to view e-mail messages directed towards other parties. Further, the means for detection are in place because sysops can view the e-mail when necessary. *Id.* Directions for intercepting another person's e-mail are available on many of the BBS networks. *Id.*

Although e-mail users do not have a reasonable expectation of privacy, this does not give the government authorization to access everyone's e-mail. The proposed statute places strict limits on the government's activity, to insure the privacy of electronic communications. *See infra* Appendix.

137. 18 U.S.C. §§ 2510-2521 (1988).

138. *Id.*

139. *Id.*

140. *Id.* § 2511(2)(a)(i).

141. *Id.* § 2511(3)(b)(iv).

142. 18 U.S.C. § 2511(3)(b)(iv) (1988).

communications.[143]

Furthermore, Title I allows "any attorney for the Government" to obtain a court order "authorizing . . . the interception of electronic communications . . . when such interception may provide or has provided evidence of any Federal felony."[144] The precatory nature of this language confers substantial authority upon the government in the surveillance of electronic communications.[145] Therefore, because the ECPA affords the government this broad authority, it does not create a reasonable expectation of privacy, and thus, the proposed statute does not intrude on any constitutionally protected interest of legitimate BBS users.

III. CURRENT LEGISLATION ON PORNOGRAPHY

While there is some legislation that arguably applies to child pornography on BBS networks, the legislation is insufficient because it does not explicitly address the problem. The Protection of Children from Sexual Exploitation Act of 1977[146] and The Child Protection Act of 1984[147] were the only laws that regulated child pornography prior to 1986. Congress replaced these acts in 1986 with The Child Protection and Obscenity Enforcement Act,[148] amended in 1988.[149] The 1988 amendment derived from the findings issued in the report of the Attorney General's Commission on Pornography in 1987.[150]

The Attorney General's Commission addressed many issues regarding pornography, including child pornography and the child pornography industry.[151] The primary concern of the Commission was the tremendous increase in the possession and distribution of

143. 18 U.S.C. § 2511(2)(a)(ii) (1988).

144. 18 U.S.C. § 2516(3) (1988). *E.g.*, Russell S. Burnside, *The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies*, 13 RUTGERS COMPUTER & TECH. L.J. 451, 501 (1987) (stating that this provision of the ECPA provides government with great leeway in the interception of electronic communications).

145. Burnside, *supra* note 144, at 502.

146. 18 U.S.C.S. §§ 2251-2253 (1979). A recent federal prosecution successfully convicted a couple for transmitting "images of bestiality and sexual fetishes over a computer bulletin board." *Pornography conviction alarms users of Internet,* CHI. TRIB., July 31, 1994, § 1, at 11. However, the validity of the ruling is uncertain due to inadequate legislative standards. *See generally* Woody Baird, *Government takes on computer-transmitted porn at Memphis' trial*, CHI. DAILY L. BULL., July 21, 1994, at 2.

147. 18 U.S.C.A. §§ 2251-2255 (West Supp. 1985).

148. 18 U.S.C.A. §§ 2251-2254 (West Supp. 1986).

149. 18 U.S.C. § 2251c(2)(b) (1988).

150. *Child Protection Act*, *supra* note 13, at 42 (testimony of Steven D. Bishop).

151. FINAL REPORT, *supra* note 1, at 405-18, 595-614. The Commission noted that the 1970 Commission on Obscenity and Pornography did not even mention child pornography in its evaluation of the pornography industries. *Id.* at 595.

child pornography and the corresponding decrease in the number of convictions for violations of child pornography laws.[152] Although the Commission noted that the Child Protection Act of 1984[153] did allow law enforcement officials to increase prosecutions for the possession of child pornography,[154] the 1984 Act actually led to very few indictments against the producers of child pornography.[155] Because of the overwhelming interest in protecting the victims of child pornography, the Commission recommended the imposition of more stringent laws.[156]

One of the Commission's recommendations was to prohibit the exchange of information regarding child pornography through computer networks.[157] This information not only disclosed locations where child pornography could be obtained, but also disclosed locations where pedophiles could procure children for pornographic purposes.[158] In an effort to regulate this activity, Congress amended The Child Protection & Obscenity Enforcement Act of 1986[159] in 1988 in order to prohibit the distribution of child pornography advertisements "by any means including a computer."[160]

Unfortunately, the 1988 amendment, much like The Protection of Children from Sexual Exploitation Act of 1977[161] and The Child Protection Act of 1984,[162] censures only a particular characteristic of the child pornography industry.[163] Specifically, the 1988 amendment's focus was to make "any notice or advertisement" seeking in-

---

The 1987 Commission referred to the child pornography industry as a "cottage industry." *Id.* at 406.

152. *Id.* at 415-18, 598-609. The Commission noted that the production and distribution of child pornography is a non-commercial enterprise. *Id.* at 604-05.

153. 18 U.S.C.A. §§ 2251-2255 (West Supp. 1985).

154. FINAL REPORT, *supra* note 1, at 604-07.

155. *Id.* at 606.

156. *Id.* at 417-18, 614.

157. *Id.* at 628. The Commission did not discuss the transmission of images or photographs through the computers because the activity was not pervasive at the time. *See Agents Raid 40 Sites in Child Porn Crackdown*, *supra* note 6, at 1A (detailing the recent federal raid of a child pornography ring established by computers).

158. *Id.* at 630.

159. 18 U.S.C.A. §§ 2251-2254 (West Supp. 1986).

160. 18 U.S.C. § 2251c(2)(b) (1988).

161. 18 U.S.C.S. §§ 2251-2253 (1979).

162. 18 U.S.C.A. §§ 2251-2255 (West Supp. 1985).

163. The 1977 Act was sufficient only to stop the commercial business of child pornography. FINAL REPORT, *supra* note 1, at 602-07. However, in response to the 1977 Act, the child pornography industry merely became a non-commercial entity by moving "underground." *Id.* The 1984 Act was directed at this underground network. *Id.* Unfortunately, the 1984 Act was ineffective against the production stage of child pornography "because of the extraordinary difficulties of investigation and proof, and in part, perhaps, because the more easily used trafficking provisions often may be invoked against suspected producers instead." *Id.* at 606.

formation regarding child pornography illegal.[164] While the 1988 amendment effectively regulates "notices" or "advertisements" for child pornography, it does not effectively regulate the actual transmission of child pornography through a computer; its language is too limited.[165]

In addition to its failure to address the transmission of child pornography through computers, the 1988 amendment also has a number of other shortcomings. First, it does not provide law enforcement with the means to keep pace with modern technology.[166] For instance, despite the 1988 amendment, it is still possible for two people to establish a BBS for the purpose of transmitting pornography.[167] Further, the amendment does not abrogate the probable cause requirement; this ties the hands of law enforcement officials at the same time as pedophiles dart in and out of these tiny BBS networks. The proposed statute eliminates this problem by enabling law enforcement officials to intercept messages on these small BBS networks without probable cause.[168] This will provide law enforcement officials with a better opportunity to eliminate child pornography because they will be able to employ covert means to prevent pedophiles and child pornographers from learning when to close up shop and start a new BBS.

A second problem with the 1988 amendment is that it does not deter individuals who may have an interest in child pornography from accessing one of these computer networks. Computers provide previously unattainable safety assurances to child pornographers and pedophiles.[169] One of the most obvious safety assurances is the

---

164. *Child Protection Act*, *supra* note 13, at 3-4 (testimony of William V. Roth, Jr.).

165. 18 U.S.C. § 2251. *See also Hearings*, *supra* note 93, at 23 (testimony of Sen. Arlen Specter). 18 U.S.C. §§ 1461, 1462, 1465 (1988), and 18 U.S.C. § 2251-2252 prohibit the mailing of child pornography and other obscene material. *Id.* "While it might be argued that some of these statutes cover the use of a computer, explicit legislation on the subject is clearly desireable." *Hearings*, *supra* note 93, at 23 (testimony of Sen. Arlen Specter).

166. Although there have not been a large number of arrests concerning child pornography and computer networks, investigators think the problem stems from the inability of law enforcement to keep abreast of current technology. Ollove, *supra* note 9, at BO1.

167. This private BBS is usually the type employed by pedophiles to transmit information. *See Hearings*, *supra* note 93, at 28 (testimony of Jack D. Smith).

168. *See infra* Appendix.

169. "The relative anonymity that computer communication provide appears to meet the pedophile's need to validate his behavior and share it with others." *Hearings*, *supra* note 93, at 2 (testimony of Sen. Paul S. Trible). Senator Trible's bill, S. 1305, was not accepted because it was too broad. *See* Barry W. Lynn, *'Civil Rights' Ordinances and the Attorney General's Commission: New Development in Pornography Regulation*, 21 HARV. C.R.-C.L. L. REV. 27, 111 (1986) (contending that the bill was too broad because it used terminology like 'facilitating' or 'encouraging,' and theoretically could extend to "teenage com-

anonymity that the BBS networks offer.[170] BBS users can transmit child pornography over the network with little fear of exposure. Consequently, the BBS networks are a very attractive vehicle for the transmission of child pornography. The proposed statute deters child pornographers from entering the computer networks by removing the anonymity of their electronic communications.[171] The statute does this by allowing law enforcement to intercept electronic communications without probable cause.[172]

IV. Proposed Legislation

Current legislation does not explicitly address the transmission of child pornography through computers. Consequently, the specific regulation of electronic communications requires new legislation.[173] The statute proposed in this Note directly addresses the transmission of child pornography and computer-generated child pornography without overlooking the concerns of legitimate users. The proposed statute accomplishes this task through various devices.

First, the statute limits itself to a specific class (child pornographers and pedophiles) and to a specific activity (child pornography).[174] The provisions of the statute explicitly restrict the surveillance of electronic communications to those transmissions involving child pornography.[175] In order to determine whether the transmission of child pornography is occurring, the proposed statute establishes a "slight suspicion" standard.[176]

Under this standard, in order for law enforcement officials to obtain a search warrant, they need only have a "slight suspicion"

---

puter dating services if the services ultimately 'facilitate' sexual conduct between the teens").

170. *See* Burnside, *supra* note 144, at 505 (discussing Congress' enactment of legislation which aimed at preventing the entry of any criminal element into the new area of electronic communications).

171. *See infra* Appendix.

172. See *infra* notes 174-83 and accompanying text for a discussion of the proposed statute's devices which attempt to aid law enforcement.

The only other statutes which arguably address the transmission of child pornography through computers are 18 U.S.C. §§ 1461 and 1462. These sections prohibit the mailing, importation, and transportation of obscene material. Section 1462 prohibits this mailing by means of a "common carrier." Generally, common carriers are telephone and telegraph companies. United States v. Radio Corp., 358 U.S. 334, 349 (1959). Since computer services do not fall into this category, 18 U.S.C. §§ 1461 and 1462 are inapplicable. Legislators have acknowledged the inability of the "common carrier" to include BBS networks. *Hearings*, *supra* note 93, at 25 (testimony of Sen. Arlen Specter). Consequently, the current legislation does not effectively combat this problem.

173. See *supra* notes 146-70 for a discussion of the failings of current legislation.

174. *See infra* Appendix.

175. *Id.*

176. *Id.*

that the transmission of child pornography is occurring. Although this standard replaces the probable cause standard, the "slight suspicion" standard applies only to the interception of child pornography through computers.[177] This standard not only protects legitimate users by confining the surveillance of e-mail to specific circumstances, but also enables law enforcement to effectively police the transmission of child pornography.

Second, the proposed statute protects the privacy of legitimate users by warning against abusive activities by law enforcement.[178] One provision specifically cautions against entrapment activities by law enforcement.[179] This warning aims at protecting the electronic communication user from targeted solicitations. The other provision is a general admonition against abusing the policies and purposes of the statute.[180] These provisions recognize the rights of legitimate users and attempt to insure the privacy of those individuals.

The main purpose of the proposed statute, however, is to protect children from the sexual abuse that necessarily accompanies child pornography. In order to shield our society from this contemptible offense, the proposed statute contains severe penalties against the transmission of child pornography through electronic communications.[181] First, violators of the statute are subject to stiffer prison terms and larger fines than they would be under current legislation.[182] In addition, repeat offenders are similarly subject to harsher penalties.[183] These penalties illustrate the gravity of the problem while attempting to deter pedophiles and child pornographers from transmitting child pornography through computers. This legislation is needed not only because current legislation inadequately addresses the transmission of child pornography through computers, but also because of the pernicious effect that child pornography has on children.

CONCLUSION

Child pornography is arguably the most heinous of offenses. Its very nature undermines the fabric of society by preying upon its weakest and most vulnerable member. The sanctity of the adult-

177. *Id.*
178. *Id.*
179. *See infra* Appendix; Jacobsen v. Ohio, 112 S. Ct. 1535, 1540-43 (1992) (holding that the government had induced the defendant into breaking the law by repeatedly mailing order forms for child pornography to him over a 26-month period, and the government could not prove that he was independently predisposed to seeking to obtain child pornography).
180. *Id.*
181. *Id.*
182. *Id.*
183. *Id.*

child bond, the means by which our young are assimilated and educated, is irrevocably broken. Further, the sacrifice of the child is done for the most perverse of reasons. The price of an adult's sexual satisfaction is a profound loss of innocence.

Furthermore, the act of child pornography is not an end in itself. Rather, it sets the foundation for acts more vile. Photography, film, and computers attempt to capture a perfect and true picture of reality. These media are forever inferior to the behavior and images they depict. Consequently, child prostitution, abduction, and even murder can result from the unsatiated appetite of the voyeur.

While society seeks to eradicate this crime and the evils associated with it, the emergence of child pornography on computer networks presents a new problem for law enforcement. The computer enables pedophiles to reach a large audience, access child pornography, and maintain anonymity. In addition, the computer itself can produce imagery of children engaged in sex.

Current legislation does not adequately address the transmission of child pornography through computers. As a result, pedophiles and child pornographers exploit the burgeoning computer technology to serve their perverse tastes while evading the law. The problem requires new legislation that will pull the plug on the peep show while protecting the privacy rights of legitimate computer users. By destroying the anonymity of these illegal transmissions, the proposed statute not only deters the exchange of child pornography, but also provides the explicit legislation that this crime demands. Moreover, the proposed statute accounts for privacy concerns by retaining a warrant requirement, though the lower standard aids law enforcement officials. Therefore, this Article's proposed statute provides the balanced legislation necessary to combat the technological growth of a crime that destroys the innocent, and thus, threatens the foundation of our society.

APPENDIX

2256(a)(1)[184] Authorized Access to Electronic Communications for Interception of Child Pornography

Enabling Provision: For the purpose of regulating electronic communications for the transmission of child pornography so as to preserve, as far as possible, the sanctity and wholeness of the children of the United States, this statute is hereby enacted.

(a) Definitions

For purposes of this statute:

(1) the term "intercept" means the acquisition of the contents of any electronic communication through the use of any electronic or other device;[185]

(2) the term "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted by an electrical system that affects interstate or foreign commerce;[186]

(3) the term "user" means any person or entity who:

(a) uses an electronic communication service; and

(b) is authorized to engage in such use;[187]

(4) the term "electronic communications system" means any facility for the transmission or storage of electronic communications including a bulletin board system regardless of size;

(5) the term "child pornography" means any visual depiction, including a computer-generated depiction, of a minor engaging in sexually explicit conduct;[188]

(6) the term "computer-generated" means any depiction, image, likeness, or representation which is created, designed, or produced in any way by a computer;

(7) the term "slight suspicion" means a concern which is less than probable cause wherein any person or entity believes, or has reason to believe that child pornography is being transmitted via an electronic communications service.

(b) Interception and Disclosure

For purposes of this section:

(1) Any information pertaining to, or data which is, child pornography which is intercepted inadvertently although no slight suspicion exists shall be divulged to a law enforcement agency. Any

184. Much of the wording in this proposal is taken from 18 U.S.C. §§ 2251-2252, 2510-2512, and 2256.

185. *Id.* § 2510(4).

186. *Id.* § 2510(12).

187. *Id.* § 2510(13).

188. *Id.* § 2256.

person who withholds such information shall be subject to punishment under subsection (e).

(2) It shall not be unlawful for an operator or employee of a switchboard or a provider of an electronic communication service to intercept and disclose that communication which pertains to, or is, child pornography;[189]

(3) It shall not be unlawful for any law enforcement official to intercept such electronic communication when there exists a slight suspicion that such electronic communication pertains to, or is, child pornography;

(4) Notwithstanding any other law, providers of electronic communication services, or their employees, agents, and other persons who do not intercept such information where a slight suspicion arises or who do not disclose such information to law enforcement pursuant to (b)(1) shall be punished as provided under subsection (e);[190]

(5) It shall not be unlawful for an employee or agent of the United States nor any provider of electronic communication service, or employee or person thereof to intercept electronic communication without a court order directing or authorizing such activity.

(c) Limitations on Interception and Disclosure

(1) It shall be unlawful for any person or entity who knowingly intercepts any electronic communication or any portion thereof where a slight suspicion does not exist of information pertaining to, or data which is, child pornography;

(2) Any person or entity who interferes or destroys any such information which pertains to, or data which is, child pornography, shall be subject to punishment under subsection (e).

(d) Cautionary Caveat Against Entrapment

(1) May it be forewarned that this statute is specifically limited to pursuing child pornography and the persons or entities who engage in the distribution, possession, or production of such material;

(2) May it be forewarned that no person, agency, or entity shall abuse the purposes of this statute whether through malicious intervention, entrapment, or repeated unauthorized interception as provided for in subsection (b).

(e) Any individual who violates this section shall be fined not more than $200,000 or imprisoned not more than 20 years, or both, but if such individual has a prior conviction under any section relating to the distribution, production, or possession of child pornography, including this section, such individual shall be fined not more than

189. 18 U.S.C. § 2511(2)(a)(i).
190. *Id.* § 2511(2)(a)(ii).

$400,000 or imprisoned not less than 10 years nor more than 50 years, or both. Any organization which violates this section shall be fined not more than $500,000.[191]

John C. Scheller

191. 18 U.S.C. § 2251(d).