Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 6 *Volume VI*
Number 2 *Volume VI Book 2*

Article 6

1996

Childporn.GIF: Establishing Liability for On-Line Service Providers

Joseph N. Campolo
J.D. Candidate, 1997, Fordham University School of Law

Childporn.GIF: Establishing Liability for On-Line Service Providers

Cover Page Footnote

The author gratefully acknowledges Molly Cusson, Derek Dessler, Beth Kelly, and Alan Levine for editing, Associate Dean Michael M. Martin for inspiring, Peter J. Perez for researching, and Sunday J. Campolo for understanding.

NOTES

Childporn.GIF: Establishing Liability for On-Line Service Providers

Joseph N. Campolo*

I would like to use the law of this land to do everything I possibly can to protect America's children from abuse and violence[1]

INTRODUCTION

The demand for child pornography[2] causes the annual exploitation of countless children.[3] While this demand has already created a thriving industry,[4] the market for child pornography has grown due to recent technological advances.[5] For example, the

---

* J.D. Candidate, 1997, Fordham University School of Law. The author gratefully acknowledges Molly Cusson, Derek Dessler, Beth Kelly, and Alan Levine for editing, Associate Dean Michael M. Martin for inspiring, Peter J. Perez for researching, and Sunday J. Campolo for understanding.

1. Attorney General Janet Reno at the acceptance of her nomination by President Clinton, Feb. 11, 1993. *See* 140 CONG. REC. E1415 (1993).

2. For purposes of this Note, child pornography is defined by the federal standard, which considers any visual representation of a minor under the age of 18 years old engaged in sexually explicit conduct child pornography. *See* 18 U.S.C. §§ 2251-2256 (1994).

3. H.R. REP. NO. 292, 98th Cong., 1st Sess. 1 (1984).

4. ATTORNEY GENERAL'S COMMISSION ON PORNOGRAPHY, U.S. DEPT. OF JUSTICE, FINAL REPORT 600 (1986) [hereinafter FINAL REPORT] ("Child pornography and child prostitution have become highly organized, multi-million dollar industries that operate on a nationwide scale.").

5. Technological advances have allowed a continuous growth in the amount of child pornography available. *See Child Pornography on the Internet: Hearings on S.892 before the Comm. on the Judiciary*, 104th Cong., 1st Sess. 14 (1995) (statement of Dee Jepsen, President, "Enough is Enough").

> Until the late 1970's, pornography was primarily available in magazines and 8mm film loops. It was distributed through the mail, street stalls and porno-

covert[6] nature of the on-line[7] world, facilitated by the Electronic Information Service ("EIS" or "EISs"),[8] has caused a reemergence of child pornography that was once virtually eliminated from society.[9]

EISs have created an "anonymous pedophile superstore"[10]

---

graphic bookstores in the 'bad part of town.' The distasteful locations limited the market. In the 1980's the advent of the VCR was exploited by pornographers. Consumers could purchase videos and watch pornography right in their own homes . . . . Then came the advent of personal computers (PCs), and a whole new world of pornography access rushed in through its floodgate.

Id.

6. *See* Symposium, *First Amendment and the Media: Regulating Interactive Communications on the Information Superhighway*, 5 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 235, 298 (1995) [hereinafter *Fordham Law Symposium*] (comments of J. Robert Flores, Esq., Deputy Chief, United States Dep't of Justice, Criminal Division, Washington D.C.):

> The computer permits anonymous encounters with potentially millions of people. Computers provide a sense of anonymity and security. Users may be alone in their rooms, they can use a made-up name, and can indulge in conduct that they would not otherwise engage in for fear of prosecution. In addition, users can reach thousands of people with one message.

Id.

7. *See* Philip Elmer-Dewitt, *Battle for the Soul of the Internet*, TIME, July 25, 1994, at 50. To connect to the on-line world, all one needs is a personal computer, communications software to set up the connection, a modem, and a phone line. *Id.*

8. "Electronic Information Services," for purposes of this Note, is used to describe commercial on-line service providers. *See* Jube Shiver Jr., *The Cutting Edge: Computing/Technology/Innovation*, L.A. TIMES, Aug. 23, 1995, at 4. The three largest commercial EISs are America Online Inc., CompuServe (a unit of H&R Block Inc.), and Prodigy (a joint venture of I.B.M. and Sears, Roebuck & Co.). *Id.*

9. *See Fordham Law Symposium*, *supra* note 6, at 299, commenting that with the advent of computer distributed child pornography:

> the child pornography magazines which were once popular but which had been virtually eliminated, are back, readily available once more. There has been a reemergence of the European child pornography we formerly had under control. Not only are we seeing all of those pictures again, but we are seeing new pictures: images coming from the Pacific Rim and South America, where children's rights are not considered a priority.

Id. (comments of J. Robert Flores, Esq.).

10. Deborah Yetter, *Man Charged with Using Computer to Lure Girl*, COURIER-J., Aug. 25, 1995, at 1B. The Attorney General's commission defined a pedophile as a person who has a "clear sexual preference for children." FINAL REPORT, *supra* note 4, at 609. Additionally, the FBI has identified common characteristics of pedophiles. *See* United States v. Long, 42 F.3d 1389, 1994 WL 669538 (6th Cir. 1994), where an FBI investigator, based on personal experience and other expert's experience in the field,

where minors are propositioned for sex and where anyone can receive child pornography within minutes.[11] Child pornography has manifested itself on-line through the "trading"[12] of pornographic pictures in "chat" rooms and the posting of pedophilic material on electronic bulletin boards ("EBBs")—two practices that have become popular and commonplace within the EISs.[13] These practices allow EIS users to obtain and save hundreds—and, in some instances, even thousands—of images of child pornography in a

---

stated that pedophiles commonly:

> (a) receive sexual gratification from physical conduct with and fantasies involving children in sexual activities; (b) collect sexually explicit materials for their sexual arousal; (c) rarely dispose of these sexually explicit materials; (d) correspond with other persons having sexual interest in children; (e) prefer with [sic] contact with children of a particular gender or age; (f) collect and retain photographs of children with whom they have been involved; (g) maintain collections of books, magazines and other writings of sexual activities with children; (h) own and operate photographic reproductive equipment; (i) are very concerned with the security of their collection of illicit materials and commonly secret their collection within their residence or safety deposit boxes; (j) keep names, addresses and telephone numbers of children with whom they have been involved; (k) keep a diary containing records of their sexual activities with children.

Id. at *2.

11. *See* Rajiv Chandrasekaran, *Undercover on the Dark Side of Cyberspace*, WASH. POST, Jan. 2, 1996, at D1; Marcia Myers, *FBI Fight Against Crime Goes High-Tech*, BALTIMORE SUN, Sept. 18, 1995, at 1B.

12. The "trading" phenomenon typically occurs as follows: People gather in "chat" rooms which are clearly recognizable as trading rooms by either xxx's or "GIF" spelled out some way in their title. Entering the room sometimes requires sending, via e-mail, an initiation picture before other "traders" will begin to converse with you. Then, people correspond either openly on the screen or privately through "immediate messages" about the pictures they are seeking and the pictures they are willing to trade for it. Traders are often earmarked by their "profiles," a self-created method of describing oneself to the rest of the EIS users. Many traders openly seek "young" material. They send pictures via e-mail to people who reply with a return picture. The picture is then deposited in the recipient's e-mail box, where it can then be read, which means viewing the picture. *See generally Fordham Law Symposium*, *supra* note 6, at 311; Chandrasekaran, *supra* note 11; Henry K. Lee, *Man Accused of Sending Child Porn Over Internet*, S.F. CHRON., Dec. 20, 1995, at A21; Armando Villafranca, *Ex-guard jailed in computer porn case*, HOUSTON CHRON., Dec. 6, 1995, at 25; Jared Sandberg & Glenn R. Simpson, *Porn arrests inflame debate on new laws*, SAN DIEGO U.-TRIB., Sept. 19, 1995, at 3.

13. *See* Myers, *supra* note 11 (discussing how "racier" chat rooms are popular for trading pornographic images).

short time.[14]

Trading or posting child pornography, however, is not the only way minors are victimized on-line. Pedophiles, after establishing a dialogue with minors in the "chat" areas, often send these minors child pornography in order to begin a sexual dialogue with the intent of luring the minor from home.[15] These tactics have become common and effective methods of victimizing minors within the cyber-pedophilic world.[16] Minors are further victimized by the

---

14. *See* Lee, *supra* note 12 (man accused of trading pictures both nationally and internationally had thousands of computer images depicting children engaged in sex acts).

15. Consider this story from a Florida newspaper:

> From his Boca Raton house, DRoach struck up a conversation with the girl on his computer. DRoach, as the man was known on the computer system, found her on one of the on-line services where people chat electronically with others far away. She lived in Lake County. She liked to play on her computer. She was 13. DRoach liked sex. All through June, DRoach corresponded with the girl about sex. His computer messages grew wilder. He told the girl all the things he wanted to do to her. Soon, words weren't enough. He sent a photographic image of himself through the computer. Then he sent one of a young girl and boy having oral sex. Then came a dozen more, of prepubescent girls in every imaginable sexual pose. By July, computer fantasies weren't enough. The girl should be discreet, he advised, when she met him July 19 in Clermont. She should bring $10 to help pay for a motel room. She should arrive at noon. At 12:10 p.m. that day, . . . [p]olice charged [DRoach] with attempted carnal intercourse with a minor, attempting lewd and lascivious acts with a minor and 23 counts of promoting or possessing child pornography. The 13 year old girl never showed up. She didn't exist, except in cyberspace. She was . . . a veteran agent with the Florida Department of Law Enforcement.

Monica Davey, *Vice squad sleuths the Internet*, ST. PETERSBURG TIMES, Aug. 13, 1995, at 1B.

16. *See, e.g.*, Chandrasekaran, *supra* note 11 (FBI agent posing as a 13-year-old girl gets approached within seconds after signing on by an older male who asks "Are you Horny?????" and sends child pornography within minutes; 31-year-old patent lawyer convicted after attempting to meet with an alleged 14-year-old girl he met on an EIS; 58-year-old pleads guilty after arranging to meet with two minors where he possessed a camera, vibrators and condoms); Villafranca, *supra* note 12 (26-year-old man possessing thousands of computer child-pornographic images uses them to solicit young boys through a popular computer on-line service); Amelia Davis, *Computer Chats with 'Teen' Lead Man to Sex Charges*, ST. PETERSBURG TIMES, Nov. 17, 1995, at 3B (47-year-old man arrested after corresponding via "chat room" at least 25 times and sending graphic child pornography numerous times to what he believed was a 15-year-old girl); Nathaniel Sheppard Jr., *Senate Panel Confronts On-Line Pornography*, CHI. TRIB., July 25, 1995, at 6 (14-year-old girl testified she was stalked by a man she met on-line after he tricked her into

EISs' ability to send out pictures to multiple parties, giving pedophiles on-line "an opportunity to victimize children easier, faster and more often."[17]

Despite the media's awareness of on-line child pornography since 1987,[18] EISs themselves ignored the issue until 1995.[19] In fact, it was not until child pornography became prevalent on-line[20]

---

revealing her home address; man arrested after he flies to Florida to rendezvous with a supposed 12-year-old boy he met on-line); Gwyneth K. Shaw & Susan Jacobson, *Man Jailed on OnLine Child Porn Charges; Teen on Computer Actually was Agent*, ORLANDO SENTINEL, July 2, 1995, at B1 (man arrested for arranging to meet a 15-year-old male on-line and for distributing and possessing child pornography); Kim Murphy, *Youngsters Falling Prey to Seducers in Computer Web Crime: Once Candy was the Lure. Now Strangers are using Cyberspace E-Mail to Attract Minors into Harm's Way*, L.A. TIMES, June 11, 1995, at 1 (15-year-old boy disappeared after being seduced by an EIS subscriber who identified himself as "The one who dies with the most boys . . . toys wins"; 13-year-old girl disappeared after communicating with a man identifying himself on-line as George who sent such messages as "[w]e can run around our room naked all day and all night"; 51-year-old man sentenced after pleading guilty to having sex with girls as young as ten and making graphic, sexually oriented e-mail contacts with adolescent and teenage girls in several states).

17. Jim Walsh, *U.S. Cyberporn Raid Reaches to Gilbert*, ARIZ. REP., Sept. 14, 1995, at B1.

18. *There's an X Rated Side to Home Computers, Parents Warned*, L.A. TIMES, Dec. 25, 1987, at 4 (the Justice Department's national obscenity enforcement unit is aware that computers were being used by pedophiles to send messages and pictures of child pornography from computer to computer); *see also* Jared Sandberg, *U.S. Cracks down on On-Line Child Pornography*, WALL ST. J., Sept. 14, 1995, at A3 (stating that awareness of EISs being used to distribute child pornography dates back to at least 1991 when the first conviction was obtained).

19. *See* Sandberg, *supra* note 18 (America Online claims that the problem of on-line child pornography was brought to its attention in 1995).

20. The U.S. Customs Service recently seized thousands of computer disks in a major 18-month investigation on computer-transmitted child pornography. Glen R. Simpson, *U.S. Arrests Three in Customs Probe of Computer Porn*, WALL ST. J., Jan. 12, 1996, at B7. While agents said that they were not sure how prevalent the activity was, the materials seized during the investigation led them to believe that it was more than occasional. *Id.* Also, the FBI recently seized the "largest collection of child pornography ever" from a New Jersey man who was allegedly part of an international ring that distributed the material by methods including computer. Rachel Gottlieb, *State Man Charged in Child Porn Case is Ex Teacher*, HARTFORD COURANT, Jan. 9, 1996, at A3; *see also* Lee, *supra* note 12 (man arrested possessing thousands of computer images depicting children engaged in sex acts that he obtained primarily on-line); Villafranca, *supra* note 12 (man arrested for possessing more than 3,000 images plus 100 computer disks full of teen-age boys, some as young as 9 or 10, in sexually explicit poses); Dorn Checkley, *The Cyberporn*

that the U.S. Congress enacted legislation to prosecute individuals who were caught sending, receiving, or possessing child pornography via computer.[21] Child pornography experts, however, argue that the distribution of child pornography cannot be eliminated simply by arresting the viewer; instead, all parties involved must be held liable: the viewer, the creator, *and* the distributor.[22] Yet law enforcement officials continue to limit their investigations to individuals who use their computers to view or create child pornography, without addressing the issue of an EIS's liability as a distributor or possessor of child pornography.[23] The proliferation of child pornography that continues on the EISs, in the aftermath of the latest on-line Federal Bureau of Investigation ("FBI") sting operation, dubbed "Innocent Images,"[24] demonstrates the ineffec-

---

Cyberflap, PITTSBURGH POST-GAZETTE, July 30, 1995, at E3 (discussing the increase in occurrences of "cyberporn"); Claire C. Marvin, *On-Line Porn Haven*, USA TODAY, Sept. 19, 1995, at 12A (concluding, after spending nine months investigating the "chat" areas provided by on-line services, that "hundreds of thousands" of pornographic pictures are traded daily, with "many" of those pictures being of minors and minors with adults engaged in sex); *Paper Says FBI Plans Big Raids Kiddie Porn*, COLUMBUS DISPATCH, June 21, 1995, at 2B [hereinafter *Paper Says*] (stating that "thousands" of subscribers to America Online have been viewing and downloading child pornography).

21. Protection of Children Against Sexual Exploitation Act, 18 U.S.C. §§ 2251-2259 (1994). The 1988 Amendment to 18 U.S.C. § 2252 changed both subsections (a)(1) and (a)(2) to include "by any means including by computer." *See* Pub. L. No. 100-690, § 7511(b) (1988).

22. *See, e.g.*, Osborne v. Ohio, 495 U.S. 103, 108-11 (1990); New York v. Ferber, 458 U.S. 747, 759-65 (1982); H.R. REP. NO. 536, 98th Cong., 1st Sess. 2 (1983) ("drying up the distribution network is essential to controlling production itself").

23. Both the FBI and the U.S. Attorney's office have acknowledged that EISs are not the subject of these offices past child pornography investigations. *See, e.g.*, *The Child Porn Bust*, WASH. POST, Sept. 17, 1995, at C6; Angie Brunkow, *Patrolman Charged in Child-Porn Sting*, OMAHA WORLD HERALD, Sept. 30, 1995, at 15.

24. In September 1995, the FBI conducted a sting operation on a commercial EIS, dubbed "Innocent Images," which revolved around finding members of EISs who were using the services to distribute child pornography and solicit minors for sex. Stephen Labaton, *Weapons of the new cyber-cop*, PITTSBURGH POST-GAZETTE, Sept. 17, 1995, at A12. Authorities began the investigation in 1991 and accelerated it in 1993 after the abduction of 10-year-old George Stanley Burdynski from his neighborhood in Brentwood, Md. *See* Chandrasekaran, *supra* note 11. He has never been found. *Id.* The operation resulted in 120 homes searched, thousands of pictures seized, and 15 people arrested (with more arrests expected). *Id.* Despite this, child pornography violations still are openly occurring within the EISs. *See supra* notes 16, 20 (examples of violations occurring after the sting

tiveness of controlling the distribution of on-line child pornography solely by pursuing the individual.

This Note argues that EISs that allow their systems to act as a means for distributing and possessing child pornography should be prosecuted under the existing federal child pornography laws. This Note does not contend, however, that EISs actively promote this distribution or possession; rather, it argues that because EISs have not provided effective measures to prevent the distribution of child pornography, they should be held liable for the child pornography on their systems. Part I presents an overview of the evolution of child pornography laws, and explores how the unique characteristics of EISs are used to distribute child pornography. This part also examines the existing federal laws used to prosecute the distribution and possession of child pornography. Part II examines the existing communications laws and demonstrates the courts' inability to effectively categorize an EIS under this framework. Part III asserts that an EIS can and should be prosecuted under the existing child protection laws in order to effectively eliminate child pornography and properly protect members. This Note concludes by arguing that absent the fear of criminal sanctions, an EIS will not have the motivation to properly structure its system in a manner that ensures the safety of minors.

I. THE EVOLUTION OF THE UNITED STATES' CHILD PORNOGRAPHY LAWS

A. *The U.S Government's Power to Restrict Child Pornography*

The power to restrict child pornography in the United States has evolved through the obscenity laws.[25] Obscenity was found not to be constitutionally protected by the Supreme Court in *Roth v. United States*[26] when, after recognizing that the "rejection of obscenity as utterly without redeeming social importance" was implic-

---

operation).

25. *See* David B. Johnson, *Why the Possession of Computer-Generated Child Pornography can be Constitutionally Prohibited*, 4 ALB. L.J. SCI. & TECH. 311, 316 (1994).

26. 354 U.S. 476 (1957).

it in the history of the First Amendment,[27] the Court held that "obscenity is not within the area of constitutionally protected speech or press."[28]

Having determined that obscenity was not protected, the Court was then faced with the task of defining "obscene." It did so in *Miller v. California*,[29] where the Court held that an obscenity offense must be limited to works which appeal to the prurient interest in sex, portray sexual conduct in a patently offensive way, and, when taken as a whole, do not have serious literary, artistic, political, or scientific value.[30]

The Court later applied this definition of obscenity to child pornography. In 1982, the Court, in *New York v. Ferber*,[31] found the test for child pornography to be separate from the obscenity standard enunciated in *Miller*, but nonetheless compared it to the *Miller* test in order to clarify it.[32] The Court offered five reasons in favor of allowing states greater restriction powers concerning child pornography. First, a state's interest in safeguarding the physical and psychological well-being of minors is a compelling interest.[33] Second, since photographs and films exacerbate the

---

27. *Id.* at 484. The Court explained that the original states provided for the prosecution of libel, blasphemy, and profanity, and that the universal judgment that obscenity should be restrained was "reflected in the international agreement of over 50 nations, in the obscenity laws of all the 48 states, and in the 20 obscenity laws enacted by the Congress from 1842 to 1956." *Id.* (footnote omitted).

28. *Id.* at 485.

29. 413 U.S. 15 (1973).

30. *Id.* at 24.

31. 458 U.S. 747 (1982).

32. *Id.* at 764. The modified version, the Court explained, would be adjusted in the following respects: "A 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.*

33. *Id.* at 756-57 (quoting Globe Newspaper Co. v. Superior Ct., 457 U.S. 596, 607 (1982)). The Court noted how it had consistently sustained legislation aimed at the physical and emotional well-being of children, even "when the laws have operated in the sensitive area of constitutionally protected rights." *Id.* at 757 (citing Prince v. Massachusetts, 321 U.S. 158 (1944) (holding that a statute that prohibited the use of children in distributing literature on the street was valid regardless of the statute's effect on the First Amendment); Ginsberg v. New York, 390 U.S. 629 (1968) (sustaining a New York law

sexual abuse of minors by creating a permanent record of their participation, distribution of child pornography must be prevented to effectively stop this recurring abuse.[34] Third, an economic motive exists for producing child pornography due to the market that is created with the advertising and selling of the material.[35] Fourth, any social value offered by child pornography is "exceedingly modest, if not *de minimis*."[36] Fifth, the Court, noting how heavily and pervasively child pornography bears on the welfare of the minor depicted, found that child pornography retains no First Amendment protection.[37] For these reasons, child pornography was held to be *per se* obscene and thus outside the scope of First Amendment protection.[38]

In two subsequent cases, the Supreme Court further permitted the regulation of child pornography. In *Stanley v. Georgia*[39] the Court held that even though obscenity is not constitutionally protected speech, the states do not possess the power to prohibit the possession of obscene material privately held in one's home.[40] Regarding child pornography, however, the Court held in *Osborne v. Ohio*[41] that the states *could* constitutionally criminalize the private possession of child pornography.[42] The Court did so by distinguishing between the interests advanced: while the obscenity statute at issue in *Stanley* was drafted to prevent the corruption of the

---

protecting children from exposure to non-obscene literature); FCC v. Pacifica Found., 438 U.S. 726, 739 (1978) (holding that "the government's interest in the 'well-being of its youth'" justified special treatment of indecent broadcasting)).

34. *Id.* at 759.

35. *Id.* at 761.

36. *Id.* at 762. The Court further noted that "if it were necessary for literary or artistic value, a person over the statutory age who perhaps looked younger could be utilized." *Id.* at 763 (footnote omitted).

37. *Id.* at 763-64.

38. *Id.* at 765. The Court noted, however, that the distribution of material which did not involve live performances would retain First Amendment protection. *Id.* at 764-65. The Court also refused to make this a crime of strict liability, noting that "[a]s with obscenity laws, criminal responsibility may not be imposed without some element of scienter on the part of the defendant." *Id.* at 765.

39. 394 U.S. 557 (1969).

40. *Id.* at 568.

41. 495 U.S. 103 (1990).

42. *Id.* at 111.

minds of its citizens,[43] the child pornography statute in *Osborne* was drafted to protect the victims of child pornography.[44] Additionally, the Court in *Osborne* acknowledged that pedophiles were using child pornography to coax and seduce minors into sexual activity.[45] Thus, with its holding in *Osborne*, the Court clearly enunciated its ability to infringe on the First Amendment in order to protect the interests of minors.

B. *The Abuses Associated with Child Pornography*

Congress, the Supreme Court, and various other courts have concluded, based on the harm to minors who participate in child pornography, that child pornography itself is child abuse.[46] Frequently cited is a 1978 Congressional report which offers a detailed "Profile of the Exploited Children"[47] and concludes that minors

---

43. *Id.* at 109 (citing Stanley v. Georgia, 394 U.S. 557, 565 (1969)).

44. *Osborne*, 495 U.S. at 109.

45. *Id.*; *see also* FINAL REPORT, *supra* note 4, at 649 ("Child pornography is often used as part of a method of seducing child victims. A child who is reluctant to engage in sexual activity with an adult or to pose for sexually explicit photos can sometimes be convinced by viewing other children having fun participating in the activity.").

46. *See, e.g.*, *Osborne*, 495 U.S. at 111; *Ferber*, 458 U.S. at 759; United States v. Rugh, 968 F.2d 750, 755 (8th Cir. 1992). *See generally* FINAL REPORT, *supra* note 4; S. REP. NO. 438, 95th Cong., 1st Sess. (1977), *reprinted in* 1978 U.S.C.C.A.N. 40.

47. S. REP. NO. 438, *supra* note 46. The Senate Judiciary Committee's findings explained how minors become victims of child pornography:

> Who are the exploited children and how do the pornographers . . . lure them into these activities? From evidence gathered by the committee it often appears to be a very easy process. The child victims are typically runaways who come to the city with no money or only enough to sustain themselves for two or three days. It is estimated that 700,000 to one million children run away from home each year so it is not very difficult for pedophiles to find child models or prostitutes. Often adult exploiters pick them up at bus stations, hamburger stands and amusement arcades and offer them money, gifts or drugs for sexual favors. With small children, even candy or a free meal may be sufficient. Not all of the exploited children are runaways. Many of them live with their families, attend school, and conduct what appear to be normal lives. One convicted child pornographer testified before the committee that he was able to recruit approximately 30 young male models over a two-year period, most of whom were not runaways . . . . The typical boy victim was:
>
> - Between the ages of 8 and 17
> - An underachiever in school or at home
> - Usually without previous homosexual experience
> - Came from a home where the parents were absent either

exploited through child pornography were probably: (1) sexually abused; (2) unable to develop healthy adult relationships later in life; (3) sexually dysfunctional; and (4) more likely to become sexual abusers themselves.[48]

In 1986, the U.S. Attorney General's Commission on Pornography ("Commission"), in essence, reaffirmed the Supreme Court's analysis in *Ferber* that child pornography itself is child abuse, and additionally concluded that minors abused through participation in child pornography retained an indelible mark on their psyche.[49] The Commission reported that the effects of involvement in child pornography include depression, suicidal thoughts, feelings of shame, guilt, alienation from family and peers, and massive acute anxiety within the child model.[50] The Commission further found that all victims of child pornography would suffer the agony of knowing that the record of their sexual abuse was in circulation,[51] again paralleling the reasoning of the Court in *Ferber*.[52]

Another finding advanced by the Commission, and adopted by the Supreme Court in *Osborne*, is that photographs of minors engaged in sexual activity are used as tools for further molestation of other minors[53] The Commission explained that adults frequently

---

physically or psychologically
- Had no strong moral or religious affiliations
- Usually had no record of previous delinquency
- Suffered from poor sociological development

Id. at 45.

48. *Id.* at 45-46; *see also Ferber*, 458 U.S. at 758 n.9 (*citing* Schoettle, *Child Exploitation: A Study of Child Pornography*, 19 J. AM. ACAD. CHILD PSYCHIATRY 289, 296 (1980)).

49. FINAL REPORT, *supra* note 4, at 613-14.

50. *Id.*

51. *Id.*

52. *Ferber*, 458 U.S. at 759 n.10.

> [P]ornography poses an even greater threat to the child victim than does sexual abuse or prostitution. Because the child's actions are reduced to a recording, the pornography may haunt him in future years, long after the original misdeed took place. A child who has posed for a camera must go through life knowing that the recording is circulating within the mass distribution system for child pornography.

Id.

53. FINAL REPORT, *supra* note 4, at 649; *see also Osborne*, 495 U.S. at 111.

show minors pictures of other minors engaged in sexual activity with the aim of persuading the recipient that if other minors are doing it, then the behavior must be acceptable.[54] This issue is particularly relevant, for purposes of this Note, because EISs allow pedophiles to communicate with and send images of child pornography directly to minors in an attempt to lure the minors from their homes.[55]

C. *Enforcing the Child Pornography Laws On-Line*

The primary federal[56] tool for prosecuting the distribution of child pornography via computer is the Protection of Children Against Sexual Exploitation Act ("Child Protection Act").[57] In

---

54. *Osborne*, 495 U.S. at 111 n.7.

55. *See supra* note 16 (demonstrating how EISs are successfully used by pedophiles to lure minors away from their home).

56. Not all states have codes regulating the dissemination of child pornography via computer. *See* EDWARD CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW, 116-20 (1994).

57. 18 U.S.C. §§ 2251-2259 (1994). Section 2252 provides, in relevant part:

> (a) Any person who-
>
> (1) knowingly transports or ships in interstate or foreign commerce by any means including by computer or mails, any visual depiction, if-
>
> (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
>
> (B) such visual depiction is of such conduct;
>
> (2) knowingly receives, or distributes, any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution in interstate or foreign commerce or through the mails, if-
>
> (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
>
> (B) such visual depiction is of such conduct; . . . shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2252(a)(1)-(4) (1994). In order to convict someone for knowingly receiving or distributing child pornography under the statute, the prosecutor must prove each element of the statute beyond a reasonable doubt:

> *First*: That the defendant knowingly received [or distributed] certain visual depictions;
>
> *Second*: That such visual depictions were shipped or transported in foreign commerce;
>
> *Third*: That such visual depictions were shipped or transported in foreign com-

addition to forbidding the distribution of child pornography, the Child Protection Act also prohibits the possession of three or more articles of child pornography.[58] Of particular importance, prosecutors can bring a case when there is either actual or constructive possession of the proscribed material.[59] Courts have defined constructive possession as "ownership, dominion or control over an item or control over premises in which the item is concealed."[60]

In its application,[61] however, the Child Protection Act has been

---

merce by any means, including by computer;
Fourth: That the production of such visual depictions involved the use of a minor engaging in sexually explicit conduct;
Fifth: That such visual depictions are of minors engaged in sexually explicit conduct; and
Sixth: That the defendant knew that at least one of the performers in such visual depictions was a minor.

United States v. Kimbrough, 69 F.3d 723, 733 (5th Cir. 1995) (emphases added).

58. 18 U.S.C. § 2252(a)(4)(B) assesses penalties against

any person who:
(B) knowingly possesses 3 or more books, magazines . . . or other matter which contain any visual depiction that has been mailed . . . shipped or transported, by any means including by computer, if-
(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
(ii) such visual depiction is of such conduct; shall be punished as provided in subsection (b) of this section.

Id.

59. United States v. Layne, 43 F.3d 127, 131 (5th Cir. 1995).

60. *Id.*

61. 18 U.S.C. § 2256 provides the relevant definitions to be used when applying this statute. They are as follows:

For the purposes of this chapter, the term-
(1) "minor" means any person under the age of eighteen years;
(2) "sexually explicit conduct" means actual or simulated-
(A) sexual intercourse, including genital-genital, oral-genital, anal-genital,or oral-anal, whether between persons of the same or opposite sex;
(B) bestiality;
(C) masturbation;
(D) sadistic or masochistic abuse; or
(E) lascivious exhibition of the genitals or pubic area of any person;
(3) "producing" means producing, directing, manufacturing, issuing, publishing, or advertising;
(4) "organization" means a person other than an individual;
(5) "visual depiction" includes undeveloped film and videotape;

problematic. The first problem, resolved by the Supreme Court in *United States v. X-Citement Video, Inc.*,[62] concerned the statute's structure and intent. In *X-Citement Video* the Court held that the term "knowingly," as used in the Child Protection Act, applied to those elements concerning both the transport elements of the crime *and* the sexually explicit nature of material.[63] The Court reasoned that Congress clearly could not have intended to apply the Child Protection Act to actors who had no idea of the sexually explicit nature of the material they transported, shipped, received, distributed, or reproduced.[64] The Court's holding in *X-Citement Video*, however, led to the second problem arising from the Child Protection Act, which revolves around what actions are considered "sexually explicit" conduct.[65]

---

(6) "computer" has the meaning given that term in section 1030 of this title; and

(7) "custody or control" includes temporary supervision over r responsibility for a minor whether legally or illegally obtained.

Id.

62. 115 S. Ct. 464 (1994).

63. *Id.* at 466-67.

64. *Id.* at 469-72.

65. *See* 18 U.S.C. § 2256(2); *See also supra* note 61. It is part (2)(E), "lascivious exhibition," which courts have struggled to define. *See* United States v. Knox, 977 F.2d 815 (3d Cir. 1992) (holding that nudity or discernibility of the child's pubic area is not a requirement under the federal statute, and that a lascivious exhibition of a child's pubic area requires only that the material depict some sexually explicit conduct by the minor which appeals to the lascivious interest of the intended audience), *cert. granted*, 113 S. Ct. 2926, *vacated and remanded*, 114 S. Ct. 375 (1993), *aff'd*, 32 F.3d 733 (3d Cir. 1994), *cert. denied*, 1994 WL 512613 (U.S. Jan. 17, 1995); United States v. Maxwell, 42 M.J. 568, 580-81 (A.F. Ct. Crim. App. 1995) (to be lascivious for purposes of federal statute which prohibits receiving or transporting visual depictions of minors engaged in sexually explicit conduct, visual images do not have to show sex or a willingness to engage in it); United States v. Wiegand, 812 F.2d 1239, 1244-45 (9th Cir.) (pictures of a 17-year-old girl would not be lascivious unless they showed sexual activity or willingness to engage in it; "lascivious" when applied to the conduct of children is not a characteristic of the child photographed but of the exhibition which the photographer sets up for an audience of pedophiles), *cert. denied*, 484 U.S. 856 (1987); United States v. Villard, 700 F. Supp. 803, 812 (D. N.J. 1988), *aff'd*, 885 F.2d 117 (3d Cir. 1989) (fact that defendant appeared to be a pedophile and that he apparently enjoyed viewing photos was insufficient to establish photos were child pornography; it was the photos that the jury was to evaluate, not their viewer); United States v. McCormick, 675 F. Supp 223, 224-25 (M.D. Pa. 1987) (photograph which depicted female who appeared to be posing to exhibit her pubic area

The third problem arising under the Child Protection Act is unique to computer violators: a violation specifically requires "the use of a minor engaging in sexually explicit conduct,"[66] meaning that an actual minor must be depicted. Based on the Supreme Court's holding in *Ferber*, if the figure depicted is a wax dummy or an artist's rendition of a minor engaged in sex, there would be no child pornography.[67] Determining if a live model has been used, outside the computer realm, has not presented the courts with a serious problem. This issue was resolved in *United States v. Nolan*[68] where the defendant claimed that proving an actual minor was photographed should be the burden of the prosecutor and should require expert testimony.[69] The court rejected this argument, finding it to be within the range of ordinary competence for someone not a photography expert to determine if they are viewing a photograph rather than an artistic reproduction.[70]

Determining authenticity, however, becomes difficult when the visual reproduction is computer generated,[71] since consumers can

---

depicted "sexually explicit conduct" for purposes of statute); Faloona by Fredrickson v. Hustler Magazine, Inc., 607 F. Supp. 1341, 1354-55 (N.D. Tex. 1985), *aff'd*, 799 F.2d 100 (5th Cir.) (publication of nude pictures of children did not constitute child pornography where nude pictures were used originally in a comprehensive educational text and then later republished in a hardcore magazine), *reh'g denied*, 802 F.2d 455, *cert. denied*, 479 U.S. 1088 (1986); *see also* Annemarie J. Mazzone, *United States v. Knox: Protecting Children from Sexual Exploitation Through the Federal Child Pornography Laws*, 5 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 167 (1994).

66. 18 U.S.C. § 2252(a)(1)(A).

67. New York v. Ferber, 458 U.S. 747, 765 (1982) ("descriptions or other depictions of sexual conduct, not otherwise obscene, which do not involve live performance or photographic or other visual reproduction of live performances, retains [sic] First Amendment protection").

68. 818 F.2d 1015 (1st Cir. 1987).

69. *Id.* at 1017.

70. *Id.* The court noted that it:

> believed the images could not be those of mannequins because in several of the magazines there is a group of pictures of what is obviously the same child in many different poses. This, plus the clarity of most of the pictures . . . made it highly unlikely that the pictures were of something else besides real human beings.

Id. at 1018.

71. *See* Joshua Quittner, *Computers Customize Child Porn*, NEWSDAY, Mar. 6, 1993, at 74.

achieve photo-realistic quality by scanning photographs into digital form.[72] These photos can then be manipulated by using graphics software costing less than $500,[73] allowing the user to transpose features from one picture and place it on another.[74] The result is a computer-generated image that the lay-person is unable to distinguish from an authentic scanned photo. Consequently, while graphic child pornography can be created without ever using an actual minor,[75] such material can still be used to seduce minors. This creates a "loophole" for high-tech pedophiles, and gives rise to the question of what legal standing computer-generated child pornography will be granted.[76] These problems aside, prosecutors, under the Child Protection Act, have obtained many guilty pleas by individual computer violators.[77]

---

72. *See* James R. Norman, *Lights, Cameras, Chips!*, FORBES, Oct. 26, 1992, at 260.

73. *See* Johnson, *supra* note 25, at 314.

74. *Id.* For an in-depth discussion of this issue, see Gary L. Gassman, *SYSOP, User and Programmer Liability: The Constitutionality of Computer Generated Child Pornography*, 13 J. MARSHALL J. COMPUTER & INFO. L. 481 (1995).

75. *A World Briefing*, WASH. TIMES, July 23, 1995, at A8. A Toronto man was convicted of transmitting computer-generated child pornography by computer. *Id.* Investigators said he would "copy pictures of children from books and catalogues onto a computer, alter the images to remove clothing and arrange them into sexual positions . . . . The scenes involved adults, children and animals." *Id.*

76. This controversy has prompted Senator Orrin Hatch (R. Utah) to propose S. 1237, the Child Pornography Prevention Act of 1995, which would, among other things, make computer-generated child pornography illegal.

> As with many of our criminal statutes . . . effective enforcement of our laws against child pornography today faces a new obstacle: The criminal use, or misuse, of new technology which is outside the scope of existing statutes. In order to close this computer-generated loophole and to give our law enforcement authorities the tools they need to stem the increasing flow of high-tech child pornography, I am today introducing the Child Pornography Prevention Act of 1995.

S. 1237, 104th Cong., 1st Sess. 2 (1995) (statement of Sen. Hatch).

77. *See, e.g.*, Gottlieb, *supra* note 20 (six men plead guilty to child pornography charges); Warren Richey, *Former Teacher Sentenced to Jail: Man Molested 11-year-old Boy*, FT. LAUDERDALE SUN-SENTINEL, Dec. 16, 1995, at 3B (teacher pleads guilty to trading child pornography via computer and performing a sexual act on a fifth-grader); *Man Pleads Guilty to On Line Child Porn*, HARTFORD COURANT, Dec. 15, 1995, at A14 (43-year-old man pleads guilty for transmitting child pornography over computer and for possessing more than 300 child pornographic images); Mary A. Mitchell, *Man Admits Sending Porn Via Computer*, CHI. SUN-TIMES, Nov. 21, 1995, at 42 ("computer consultant

Computer violators of the Child Protection Act have also been successfully convicted by juries. For example, in *United States v. Kimbrough*,[78] the first federal computer child pornography case to go to trial, the defendant Kimbrough was convicted for knowingly receiving child pornography which he downloaded from an international electronic bulletin board.[79] As his defense, Kimbrough denied knowing the nature of the material being downloaded, claiming that the file names were vague as to their content.[80] On appeal, the Fifth Circuit rejected his argument, finding that the jury had been properly charged as to the requisite knowledge necessary for a violation to occur.[81]

Subsequent cases involving computers and child pornography have involved members disseminating child pornography on an EIS,[82] and have also resulted in convictions. One such case, *United States v. Maxwell*,[83] was a case of first impression in the U.S. military appellate courts.[84] In *Maxwell*, the judges acknowledged that this case "required [them] to focus upon how well traditional legal concepts are suited to deal with challenges of the computer age" and concluded that "the current body of law [was] well-equipped

---

once convicted of sexual assault pleaded guilty . . . to distributing child pornography on America Online"); Bill Lodge, *Ex-News Employee Pleads Guilty in Child Pornography Case*, DALLAS MORNING NEWS, Nov. 3, 1995, at 32A; *2 Guilty of Soliciting Teens On-Line*, WASH. POST, Nov. 2, 1995, at B4 (two men, one a patent lawyer, plead guilty to using an EIS to set up sexual encounters with teenage girls); *Man Sentenced in Computer Porn*, BOSTON GLOBE, Oct. 21, 1995, at 19 (man pleads guilty to two counts of distributing child pornography he obtained via computer communications).

78. 69 F.3d 723 (5th Cir. 1995).

79. *Id.* at 726.

80. *Id.* at 733-34. Files downloaded were stored on petitioner's computer under a file entitled "BAM Young List." *Id.* at 733. Contents of this file were described as "MBON006.JPG," "MBON007.JPG," "CHERRYA.GIF," "CHERRYB.GIF," "LITSIS.GIF," "INNOCNT.JPG," and "KID013.GIF." *Id.* at 728-29 n.4. Additionally, petitioner's computer contained extra file descriptions, describing the contents as "Eight Years Indian Girl," "Preteen School Girl," and "Bound and Gagged Spread in a Chair." *Id.* at 734.

81. *Id.* at 733.

82. *See, e.g.*, United States v. Chapman, 60 F.3d 894 (1st Cir. 1995) (man convicted of transmitting child pornography over computer network).

83. 42 M.J. 568 (A.F. Ct. Crim. App. 1995).

84. *Id.* at 572.

to deal with th[e] unique scenario."[85]

Maxwell involved a U.S. Air Force Colonel who was convicted of receiving and distributing visual depictions of minors engaged in sexually explicit conduct.[86] The FBI was notified of Maxwell's actions by an EIS member who had received unsolicited child pornography from people only identifiable by their on-line pseudonyms.[87] This led military authorities to obtain a warrant[88] to search the EISs main computer terminal, resulting in a seizure of 12,000-14,000 pages of e-mail messages and 39 high density computer disks containing visual transmissions made, in part, by the defendant.[89] The defendent had used the EIS's e-mail capabilities to disseminate and receive—or "trade"[90]—the pictures.[91] It should be noted, however, that the defendant was permitted to continue using the EIS, even after the EIS had been notified of the suspected illegal conduct by the authorities.[92]

D. *How EISs Facilitate the Transmission of Child Pornography*

Having demonstrated that EISs are being used to disseminate child pornography, it is necessary next to examine how EISs are used in this manner. EISs have grown at a staggering rate: in less than two years their growth has been ten-fold.[93] There is some evidence, however, that this growth has resulted due to a desire for anonymous communication rather than a demand for information.[94]

---

85. *Id.*

86. *Id.* at 573.

87. *Id.* at 574.

88. *Id.* The warrant was issued on Dec. 10, 1991. *Id.*

89. *Id.*

90. *See supra* note 12 (discussing the process of trading pictures via an EIS).

91. *Maxwell*, 42 M.J. at 574. The court described in detail the various facets of the EIS's e-mail capacities. *Id.* at 573-74.

92. *Id.* at 574-75, 579 (the EIS was informed in December 1991 that the appellant was allegedly distributing child pornography; in June, 1992, however, appellant was still using the service).

93. A September 1995 article stated that: "America Online is the fastest growing on-line service, with 3.5 million members," Sandberg, *supra* note 18, whereas an article two years earlier, in September, 1993, stated that America Online had 350,000 members. *Growth Off for On-Line Services*, WASH. POST, Sept. 27, 1993, at F17.

94. *See* Laura Evenson, *Everybody Wanted It: Internet Access*, S.F. CHRON., Dec. 24, 1995, at 29 ("'Communications is the No.1 feature used by our members,' said Pam

It is this anonymous communication that has allowed the reemergence of child pornography.[95]

An EIS provides several functions to its users. As the number of potential uses for cyberspace is inestimable,[96] this Note focuses on the essential functions offered by almost all EISs.[97] These core functions have unique capabilities that pedophiles use to maximize their audience, ensure their anonymity, and gain instant access to minors.[98] This Note will also later develop how the differences in these functions are considered crucial in determining the EISs' First Amendment status.[99] Such a determination is necessary when ascertaining the appropriate responsibility and liability of an EIS.

1. Electronic Mail

Of all on-line activities, the transmission of electronic mail ("e-mail") is the most common,[100] and is also the function used most frequently in transmitting pornographic materials.[101] E-mail has many similarities to its conventional paper counterpart in that it allows individual correspondences,[102] and once an e-mail message is sent[103] it is stored and forwarded at each subsequent site along

---

McGraw, an [America Online] spokeswoman, who added that 'chat and bulletin board messaging account for most of subscribers' time online.'").

95. *See Fordham Law Symposium*, *supra* note 6, at 298-99 ("The advent of computer technology has changed the distribution methods of child pornography . . . . [making] the child pornography magazines which were once popular but which had been virtually eliminated . . . readily available once more.") (comments of J. Robert Flores, Esq.); *see also* Walsh, *supra* note 17 ("Prior to the PC medium and the Internet, it is my professional opinion that law enforcement had child pornography under control.") (quoting Phoenix Police Sgt. Germaine Barnes).

96. CAVAZOS & MORIN, *supra* note 56, at 5.

97. *See* E. Brian Davis, *An Introduction to the Internet*, FED. LAW., May 1995, at 12.

98. *See Fordham Law Symposium*, *supra* note 6, at 304 (comments of Police Officer Kevin Mannion, Manhattan South Vice Enforcement Squad, New York City Police Department).

99. *See infra* part III.

100. *See* Evenson, *supra* note 94 (stating that more than four million e-mail messages are sent daily on America Online alone).

101. *See* Sheppard, *supra* note 16.

102. CAVAZOS & MORIN, *supra* note 56, at 5.

103. On a commercial service, the name a user "logs-on" with is generally his e-mail "address," and is openly posted or available via the services on-line directory. Thus, if a user signed on to America Online with the name "JoeC," anyone using America Online

its path until it reaches the final destination.[104]

Unlike traditional mail, however, a person can respond to, store, or simply delete e-mail instantly and/or automatically.[105] Additionally, creating large mailing lists and instantly disseminating material to that list is a simple task, usually requiring just a few keystrokes. Of particular importance, a picture can be attached to a piece of e-mail[106] (usually in the form of a .GIF[107] file or a .JPG[108] file). Additionally, by using a "zip"[109] compression file program, a user can send dozens of pictures into one short download.[110]

---

could e-mail him by putting "JoeC" in the appropriate place for an address. Significant development in the Internet has allowed members from different services to e-mail one another. Thus, if "Bob" from Prodigy wanted to e-mail "JoeC" from America Online, Bob would type "JoeC@aol.com" in the appropriate spot for the recipient's address. The mail would then be routed, via the Internet, to America Online's database, and put into "JoeC's" box. *See generally id.* at 6.

104. Mark Kassel & Joanne Kassel, *Don't Get Caught in the Net: An Intellectual Property Practitioner's Guide to Using the Internet*, 13 J. MARSHALL J. COMPUTER & INFO. L. 373, 376 (1995).

105. CAVAZOS & MORIN, *supra* note 56, at 5.

106. *See* Dwight Silverman, *Pornography in cyberspace poses dilemma*, HOUSTON CHRON., July 23, 1995, at 1. Pictures are "attached" to e-mail by converting them into encoded text-based codes, which must be decoded, or converted, back into graphic form before being viewed. *Id.*

107. *See Facts on GIF graphics format, available on* CompuServe, Sept. 28, 1995. "GIF, pronounced Jif," stands for "Graphics Interchange Format" and is a "mechanism of storing high-quality color graphics images in a way that can be exchanged between users of differing hardware." *Id.* "The GIF format allows for very high resolution, color images that can be used in any application that requires the display of graphics information." *Id.*

108. *See* Margot Williams, *Overcoming FTP Phobia Opens a Brave New World*, CHI. SUN-TIMES, Jan. 8, 1995, at 21. A .JPG file, pronounced J-PEG, is an encoded binary file that requires decoding before transferring. *Id.* Once decoded, a .JPG file shares the same graphics characteristics as a .GIF file. *See supra*, note 107.

109. Scott Palmer, *Confusing File Names Part of Secret Code for PC Aficionado*, INDIANAPOLIS NEWS, Jan. 3, 1994, at F4.

> When you send a file over the phone lines, you want it to be as small as possible. A compression program shrinks it for you. The most popular compression programs are PkZip (which creates .Zip files), Arc (which creates .Arc files), and LHarc (which creates .Lzh files). To decompress these files, you need the corresponding decompression program.

Id.

110. *See* TOM LITCHY, THE OFFICIAL AMERICA ONLINE FOR WINDOWS TOUR GUIDE, 131-45 (2d ed. 1994). Downloading refers to the process of transferring or copying files from

2. Message Posting

The ability to post public messages instantly is another popular function of EISs. Referred to as "electronic bulletin boards" ("EBBs"),[111] this function has been described as analogous to "electronic town meetings"[112] or "graffiti discussions on public restroom walls,"[113] with each message becoming part of a thread of messages that relate to a particular topic.[114] To "post" messages on a board, the user picks a board which covers an area of interest, reads the messages that are posted there, and posts a reply. While no accurate figure is available as to how much pornographic material is available on EBBs,[115] a significant part of the total volume of EBB titles are erotica based,[116] with pedophilic stories constituting about 10% of all EBBs' contents.[117]

While EBBs are primarily located on the Internet, most EISs afford direct access to certain selected Internet EBBs to their users.[118] These EBBs contain graphic material[119] akin to that found

---

someone else's computer to your own via a modem. *See id.*

111. Other names for EBBs are "message boards" (America OnLine), "forums" (CompuServe), "bulletin boards" (GEnie), and "round tables" (Delphi). *Id.* at 318-19.

112. *See* Robert Gebeloff, *Brave New World Chart your Itinerary in Cyberspace*, RECORD, NORTH. N.J., Aug. 23, 1994, at D1 ("Each [EIS] offers . . . electronic town meetings. Called forums, or in some cases news groups, these areas are divided by subject matter and contain comments on the subject 'posted' by members.").

113. CAVAZOS & MORIN, *supra* note 56, at 6.

114. *Id.*

115. *See* Elmer-Dewit, *supra* note 7 (stating that a study done by a Carnegie Mellon University student concluded that 83.5 percent of Internet postings were pornographic). However, a controversy exists over the integrity of this study. Brock N. Meeks, *The Story of how Time was Duped on Cyberporn*, SAN DIEGO U.-TRIB., July 25, 1995, at 1.

116. Joshua Quittner, *Vice Raid on the Net*, TIME, Apr. 3, 1995, at 63 (the alt.sex newsgroup (EBB) is "so popular it has spawned more than 60 offshoots"). However, due to the firestorm over the graphic titles, pornographers can easily post their material on groups with neutral, non-explicit titles. *See* Susan Benkelman, *Crossing Line of Censorship?*, NEWSDAY, Dec. 30, 1995, at A3 (claiming that much more sexually explicit material can be found on a bulletin board named soc.motss than boards with the alt.sex designation).

117. *See* Laura Davis, et al., *Controlling Computer Access to Pornography: Special Conditions For Sex Offenders*, 59 FED. PROBATION 43 (June 1995).

118. *See* Litchy, *supra* note 110, at 318-19 ("The Internet does not have a monopoly on newsgroups.").

119. On the Microsoft Network on Sept. 5, 1995, the newsgroup rec.nude was on the service. Within this newsgroup, this author found the following postings:

on the Internet.[120] This occurs in part because no approval by the EIS is needed of material one posts to a EBB.[121]

While EBBs are theoretically a text-only feature of the on-line world, graphics files can be turned into text-base code with readily available software and then uploaded to the binary groups on the various bulletin boards.[122] This effectively posts a picture that can be freely downloaded by potentially millions of readers.[123] Additionally, a service now exists which allows users to post to an EBB anonymously,[124] making the already hard task of tracking down violators virtually impossible. Once the picture is downloaded, the EISs usually provide the necessary decoding software to transpose the file back into a picture.[125]

Date: Wednesday, August 16, 1995 1:20 AM
To: rec.nude
Subject: young girl lovers
Anyone interested in joining a pic swapping club of young girl lovers should email me at the above address . . . for those who still don't understand the sort of pics i am referring [sic] to are those similar to JMIS, AA, Sunfr, KDS, Young, ... etc

With a typical response reading:

Date: Monday, September 04, 1995 5:09 PM
To: rec.nude
Subject: RE: young girl lovers
Hi, I would like to join your club, but unfortunately right now I dont have any pictures available, please contact me as soon as possible. Thanks.

(on file with the *Fordham Intellectual Property, Media & Entertainment Law Journal*).

120. Dorn Checkley, *A reasonable regulation, The Cyberporn Cyberflap*, PITTSBURGH POST-GAZETTE, July 30, 1995, at E3. In February 1995, the Associated Press reported that a researcher at Stockholm University's Institute of Computer and System Science, in a seven-day period of monitoring, uncovered 5,651 postings including 800 graphic pictures of adolescents engaged in sexual acts on four Usenet bulletin boards. *Id.*

121. *See* Litchy, *supra* note 110, at 317-22.

122. Silverman, *supra* note 106.

123. *See Fordham Law Symposium*, *supra* note 6, at 298 (comments of J. Robert Flores, Esq.) ("In terms of the technology, millions of people can be reached with one message on the Internet.").

124. Douglas Lavin, *As Regulators Seek to Police Internet, An Offbeat Finnish Service Fights Back*, WALL ST. J., July 17, 1995, at A7. A service in Helsinki, Finland acts as an "anonymous remailer, a service that offers anyone [on-line] a way to send almost anything anonymously almost anywhere." *Id.*

125. *See* Daniel Akst, *The Cutting Edge: COMPUTING/TECHNOLOGY/INNOVATION*, L.A. TIMES, Jan. 10, 1996, at 4 (explaining how and when to use decoding soft-

3. "Chat" Rooms

"Chat" rooms provide a direct line of communication in real-time for EIS users. Most commercial EIS chat rooms[126] operate similarly, allowing users to create a pseudonym[127] for themselves, and communicate by typing messages to other members who know them only by this name.

Some EISs also allow members to create and name the rooms,[128] in order to select a theme of "conversation" that should be occurring. The names selected by members can be sexual in nature, with requests for "young" material sometimes openly posted.[129] Other features available to communicate within chat rooms are "instant messages" ("IMs"), which allow one user to send a private message instantly to another user.[130] IMs appear immediately on the recipient's screen and can only be viewed by the recipient, making it impossible for any outside spectator to monitor the message.[131] Consequently, IMs can be a valuable tool for pedophiles because IMs allow adults the ability to establish a dialogue with minors unchecked by other users.

---

ware programs); John Gilroy, *Ask the Computer Guy*, WASH. POST, Nov. 13, 1995, at F18 (explaining how to obtain the necessary decoding software via an EIS if the EIS does not already provide it).

126. *See* Stacey J. Rappaport, *Rules of the Road: The Constitutional Limits of Restricting Indecent Speech on the Information Superhighway*, 6 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 301, 312-15 (1995).

127. The pseudonym one creates is openly shown on the screen to all, and can be extremely graphic. Examples of graphic names this author found on America Online at 2:00 p.m. on Saturday, Sept. 9, 1995 that specifically referred to "young" exploits are: Lisa13nwet, BigCoc9, Tabbylicks, Ohdaddyooh, YoungTrdr, ButtPlgBoy, BadGirl1605, LilgrlzDad. (on file with the *Fordham Intellectual Property, Media & Entertainment Law Journal*).

128. *See* Sandberg & Simpson, *supra* note 12.

129. At 2:00 p.m. on Saturday, Sept. 9, 1995, on America Online, this author found 503 rooms created by members; of those, 22 rooms openly advertised "young" exploits and trading. These were: I Love Oldr Men, Under 20M4M, Shaved, family affairs, M wnts yf2 watchmejerk, F for F under 20, up my skirt, pre xx fun, GIF trading, TgEiEfNs, BgOiNfDsAGE, almost a teen chat, Lkng 4 fem undr 14, Dady 4 baby fem, xxBxOxYxSxPxIxCxS, Dad4f, OLDRM4Mundr20, PxOxRxNxOxanything, Yngr Trader, Strict Parents, xPxOxRxNxOx, xohhhhDaaaddyyyyy (on file with the *Fordham Intellectual Property, Media & Entertainment Law Journal*).

130. *See* Litchy, *supra* note 110, at 260.

131. *Id.* at 257.

Chat rooms also allow users to create personal "profiles" of themselves. While profiles are designed to contain basic information (i.e., age, sex, hobbies) of the particular user, many profiles have become a method for pedophiles to locate minors and have served as open solicitations for child pornography.[132] Additionally,

---

132. Examples of the way 21 members chose to openly describe themselves on America Online, Sept. 9, 1995, at 2:00pm are:

Member 1-Hobbies: Family fun . . . Kim, my step mom, likes me to report back to her . . . she was my first . . . my "teacher"
Member 2-Birthdate: Gemini82
Hobbies: hiding my screen name and young f gifs from my dad
Occupation: student and sometimes teacher
Member 3-Birthdate: 1980
Hobbies: Girls, older women, discovering sex, 32-B 26 30 (hard nipples) cute tight ass
Occupation: Student, cheerleader, Very BI looking for my first experience (found it) with a woman
Quote: If it's soft and wet I want to lick it, if its long and hard I want to BREAK it . . . .
Member 4-Hobbies: Collecting Jpg and Gif files Hot chat and of course boys and girls not always in that order;)
Member 5-Hobbies: SEX,PORNOS,GIFS FROM HOT YOUNG FEMALES
Member 6-Quote: bi f love gif trading and getting nasty with girls
Member 7-Hobbies: love them all-big and small-old and young
Occupation: sales-student-babysitter
Quote: my personal favorites "girls and boys"
Member 8-Hobbies: Young, beautiful bi and straight females. Love panties, cyber sex, small breasts and Redheads. (No Kiddie Stuff)
Member 9-gif trading, dating girls who like daddies
Member 10-Hobbies: casting the part of my little princess—she's 20-33 yrs old, but can "look" younger
Quote: no pre-teens, teens or males please
Member 11-Birthdate: 1982
Quote: "Here let me swallow that"
Member 13-Birthdate: 1979
Hobbies: . . . . . anything to do with sex :), locals ONLY
Member 14-Quote: Just Suck It! No Teen Gifs!!! Don't ask and don't send!!!
Member 15-Occupation: want to meet and service lonely/sweet girls in area
Quote: also luv trading hot xxx gifs and stories
Member 16-Hobbies: Young gifs, movies, etc.
Member 17-Computers: I am always looking for an older "Strict Mom" with a firm hand.
Hobbies: Bi-Female likes to be spanked
Member 18-Hobbies: Spanking bad girls
Occupation: Spanking bad girls

users do not need the EIS's approval of their user profiles.[133]

4. Gateways

Another prominent feature of EISs is their ability to act as gateways to the Internet.[134] Gateways are the electronic "switches" that direct Internet traffic in and out of certain systems.[135] Information that passes through the gateway computer is first processed by the gateway's computer hardware before being sent to the destination computer for further processing.[136] Internet gateways are built into the larger EISs[137] and tend to make Internet access easy[138] because they use simple menus that are generally well integrated into the EIS's own user interface.[139] Clicking on the designated "icon"[140] allows members Internet access to international countries where child pornography laws are different.[141] While accessing the Internet, however, EIS users are still signed on to and being charged by the EIS.[142]

Member 19-Hobbies: phone sex, trading teen gifs, and more sex
Member 20-Hobbies: B&D, D/s, Reddening little girls butts! WHACK! WHACK! WHACK!
Member 21-Member Name: LilgrlzDad
Hobbies: Taking care of my little girl
Quote: "Finish your veggies, young lady !!"
(on file with the *Fordham Intellectual Property, Media & Entertainment Law Journal*).

133. Shaw & Jacobson, *supra* note 16.

134. Eric Schlachter, *Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions*, 16 HASTINGS COMM. & ENT. L.J. 87, 111 (1993).

135. Clint Swett, *Pacific Bell Looks for Huge Growth on the Internet*, SACRAMENTO BEE, Dec. 20, 1995, at F2.

136. See Schlachter, *supra* note 134, at 111.

137. Robin Frost, *Small Bytes: Cutting the cost of traveling in cyberspace*, WALL ST. J., Dec. 8, 1995, at R18. America Online, CompuServe, and Prodigy all have Internet gateways built into them. *Id.*

138. Fran Gardner, *On-Line Services Show Off Wares*, PORTLAND OREGONIAN, Nov. 16, 1995, at C2. (Carol Wallace, a spokeswoman for Prodigy, stated that Prodigy is "packaging the material on the Internet so [the user] can find it quickly").

139. *See* Frost, *supra* note 137.

140. MICROSOFT CORPORATION, USER'S GUIDE: MICROSOFT WINDOWS AND MS-DOS 6, 43 (1993) (an "icon" is a small picture representing various types of applications and files).

141. *See generally Fordham Law Symposium*, *supra* note 6, at 279-316.

142. *See* Frost, *supra* note 137 (claiming that the big EISs charge "about $9.95 a month, which includes five hours of on-line time, whether on the Internet or in the ser-

II. DETERMINING THE PROPER LEGAL FRAMEWORK FOR AN EIS

A. *The Law and Communications*

Traditionally, a trifurcated communications regulatory structure has existed consisting of print, broadcasting, and common carriage.[143] EISs, however, are multifaceted systems with seemingly no immediate traditional parallel. Currently, the Federal Communications Commission ("FCC") may only make suggestions about how EISs should structure their systems and has no enforcement power if an EIS fails to conform to these suggested guidelines.[144] Thus, looking at the law surrounding the traditional forms of communication affords valuable insight as to how an EIS may be prosecuted if it fails to adequately protect its users from child pornography.

1. Print Publishers

An EIS provides many services similar to those of a newspaper or magazine, such as news headlines and stock quotes.[145] Most EISs also provide EBBs, theoretically identical to traditional bulletin boards,[146] where users can post a message seeking information

---

vice's own databases").

143. *The Message in the Medium: The First Amendment on the Information Superhighway*, 107 HARV. L. REV. 1062, 1069 (1994) [hereinafter *The Message*].

144. Until the passage of the Communications Decency Act, discussed *infra* at notes 255-65, EISs were subject to no governmental regulation. *See* William S. Byassee, *Jurisdiction of Cyberspace: Applying the Real World Precedent to the Virtual Community*, 30 WAKE FOREST L. REV. 197, 200-01 (1995). Now, the "Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications," however, the "Commission shall have no enforcement authority over the failure to utilize such measures." S. REP. NO. 230, 104th Cong., 2d Sess., § 502(2), at 83 (1996).

145. *See* Frost, *supra* note 137 (commercial on-line providers offer services such as publications, on-line shopping, stock market quotes and airline reservations).

146. *See supra* notes 112-17 and accompanying text. In the past hundred years there has been little debate about proprietor liability for the content of traditional bulletin boards under the proprietor's control. *See* David Loundy, *E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability*, 12 COMPUTER L.J. 101, 155 (1993). The law of Great Britain, coupled with American law, is demonstrative. *See, e.g.*, Hellar v. Bianco, 244 P.2d 757, 759 (Cal. App. 1952) (holding that the owner of a tavern became a republisher of a filthy scrawling on a men's room wall as soon as the bartender, an agent of the owner, learned of the libel and did not remove it); Byrne v. Deane, 1 K.B. 818 (1937) (holding that owners of a club who became aware of a defamatory poem written on their walls became republishers of the information once they learned

and responses. These services closely resemble the print media,[147] which traditionally has been virtually free from government restrictions.[148]

Print publishers, however, can incur liability for publishing child pornography because child pornography retains no First Amendment protection.[149] To determine if a print publisher should be held liable for the contents of its publication, however, law enforcement officials must first ascertain whether the publisher performs the duty of a primary publisher or a secondary publisher (i.e., a republisher).[150] If considered a primary publisher, like a newspaper or magazine, then it is presumed that the publisher played an integral part in creating and editing the illegal message disseminated,[151] resulting in liability for the publisher. If found to be a republisher, like a library or bookstore, then no presumption of knowledge exists, and prosecutors have the burden of showing that the republisher knew or had reason to know of the illegal contents.[152]

The issue of publisher liability was addressed by the Supreme Court in *Smith v. California*.[153] In *Smith*, the Court reversed the conviction of a bookseller who was found guilty of violating a strict liability ordinance banning possession of obscene materials.[154] The Court held that booksellers were republishers of the material they sold, and that holding them strictly liable for the contents of the books they sold imposed a severe limitation on constitutionally

---

of and failed to eradicate the poem); *cf.* Scott v. Hull, 259 N.E.2d 160, 162 (Ohio App. 1970) (holding that a storekeeper was not a republisher of graffiti painted on the outside of a store because the viewing of the graffiti was not at the invitation of the owners as it was in the other cases).

147. Loundy, *supra* note 146, at 146. Often, due to electronic word processing and page layout programs used by the majority of print publishers, the only real difference between print media and electronic media is actual paper. *Id.*

148. *See The Message*, *supra* note 143, at 1071.

149. *See* New York v. Ferber, 458 U.S. 747 (1982).

150. *See* Loundy, *supra* note 146, at 146-47.

151. *Id.* at 147.

152. *Id.* at 148.

153. 361 U.S. 147 (1959).

154. *Id.* at 148.

protected matter.[155] The Court reasoned that any bookseller's self-censorship, resulting from strict liability, would result in widespread public censorship,[156] noting that any obscenity law would have an inhibitory or "chilling" effect on the dissemination of materials obscene as well as not obscene.[157] The Court, however, declined to rule on what level of indirect censorship it would tolerate.[158]

Courts still struggle with the issue of publisher liability, except that today's courts are faced with the task of discerning an EIS's publishing status. This issue was first addressed in *Cubby, Inc. v. CompuServe, Inc.*,[159] where defendant CompuServe was sued when one of its contracted customers posted an allegedly libelous statement on an EBB.[160] The plaintiff argued that CompuServe was a publisher of the statements and therefore should be held to a higher standard of liability.[161] CompuServe, however, maintained that it was instead a republisher, with no more editorial control over such a publication than a public library, bookstore, or newsstand.[162] CompuServe further argued that for it to examine every publication it carried would be no more feasible than for any other distributor to do so.[163] The court agreed with CompuServe, and ruled that the proper standard of liability to be applied to CompuServe is whether it knew or had reason to know of the message's content. The court thus held that CompuServe's status was that of a republisher—or

---

155. *Id.* at 153. The Court reasoned:

> For if the bookseller is criminally liable without knowledge of the contents, and the ordinance fulfills its purpose, he will tend to restrict the books he sells to those he has inspected; and thus the State will have imposed a restriction upon the distribution of constitutionally protected as well as obscene literature.

Id.

156. *Id.* at 154.

157. *Id.*

158. *Id.*

159. 776 F. Supp. 135 (S.D.N.Y. 1991).

160. *Id.* At the time of this case, CompuServe had over 150 special interest "forums." *Id.* at 137. The particular forum in this case, "Rumorville USA," was not created by CompuServe but rather published by Don Fitzpatrick Associates. *Id.*

161. *Id.* at 139.

162. *Id.* at 140.

163. *Id.*

distributor—of information.[164]

Other courts, however, have held differently on this issue. For example, in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[165] a New York state court reviewing a libel charge agreed with *Cubby* that a bulletin board found on the Prodigy service was analogous to print medium.[166] The *Stratton* court, however, ruled that the EIS's responsibility was that of a primary publisher—thus reaching the opposite conclusion as the court in *Cubby*. In *Stratton*, the plaintiff, Stratton Oakmont, based their claim on the fact that Prodigy held itself out in national newspaper articles as an EIS that exercised editorial control over the material posted on its service, thereby distinguishing itself from the competition and expressly likening itself to a newspaper.[167] The defendant, Prodigy, insisted that its policies had changed since the newspaper article has appeared, and that Prodigy's latest article did not reflect its policy as of when the allegedly libelous statements were posted.[168] The *Stratton* court found that, unlike CompuServe, Prodigy[169] had indeed positioned itself as a "family" on-line service that claimed it monitored offensive behavior.[170] Based on these distinctions, the court felt com-

---

164. *Id.* The court stated:

> Technology is rapidly transforming the information industry. A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.

Id.

165. 1995 WL 323710 (N.Y. Sup. May 24, 1995).

166. *Id.* at *2, *4.

167. *Id.* at *2. In one article Prodigy stated:

> We make no apology for pursuing a value system that reflects the culture of the millions of American families we aspire to serve. Certainly no responsible newspaper does less when it chooses the type of advertising it publishes, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate.

Id.

168. *Id.*

169. *Id.* at *4 ("By actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and 'bad taste', for example, PRODIGY is clearly making decisions as to content . . . and such decisions constitute editorial control.").

170. *Id.* at *5. In a letter to the New York Times, Prodigy's director of market

pelled to classify Prodigy as a primary publisher rather than a distributor, and held Prodigy directly responsible for their members' postings.[171]

In a third case involving EIS liability, *Stern v. Delphi Internet Services Corp.*,[172] the court had to determine the appropriate liability for an EIS based on an advertisement the EIS made encouraging users to post messages on the service.[173] Specifically, the court had to decide if an EIS was a "news disseminator" for purposes of New York's Civil Rights Law.[174] In *Stern*, the plaintiff, the celebrity Howard Stern, conceded that EISs occasionally engage in activities similar to those of news vendors,[175] but claimed that he never approved the use of his photograph for advertisement purposes.[176] The defendants, Delphi Internet Services, claimed that as a news disseminator it was entitled to disseminate news, and that Howard

---

programs and communications offered examples of postings submitted that Prodigy chose not to publish:

> "I'm thinking of killing myself. Which is less painful: hanging or slashing my wrists?"
>
> "Little girls in tight jeans and T-shirts are a real turn on to guys like me. Write to me at P.O. Box . . . ."

Geoffrey Moore, *The 1st Amendment is Safe at Prodigy*, N.Y. TIMES, Dec. 16, 1990, at 13.

171. *Stratton*, 1995 WL 323710 at *4.

172. 626 N.Y.S.2d 694 (N.Y. Sup. Ct. 1995).

173. *Id.* at 695-96. An advertisement for a subscriber-participation debate Delphi was hosting on its service appeared in a prominent magazine and newspaper which, in addition to portraying a lewd picture of radio talk show celebrity Howard Stern, read "[s]hould this man be the next governor of New York? . . . Maybe it's time to tell the world exactly what you think . . . . So . . . don't put a cork in it. Sit down, jack in, and be heard." *Id.*

174. *Id.* at 697. The court quoted, in part, New York's Civil Rights Law and stated that section 50:

> make[s] commercial misappropriations of a person's name or likeness a misdemeanor. It provides, in relevant part: "a person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without first having obtained the written consent of such person . . . is guilty of a misdemeanor."

Id. at 696 (quoting N.Y. CIV. RIGHTS LAW § 50 (McKinney 1992)).

175. *Id.* at 697.

176. *Id.* at 698.

Stern's candidacy for governor of New York was newsworthy.[177]

The court, in attempting to analyze the status of an EIS, first stated that the Delphi service was "*analogous* to that of a . . . letters-to-the-editor column of a newspaper" because the service required the public to purchase its materials to actually gain access to the information it carried.[178] The court then reasoned that it was "evident that Delphi's on-line service . . . be *analogized* to distributors such as news vendors, bookstores and libraries," echoing the *Cubby* court.[179] The court next ruled that Delphi was in fact a news disseminator,[180] but finally stated that the proper analogy of an EIS is to a television network.[181]

These holdings—*Stratton*, *Cubby*, and *Stern*—result in three implications for the law surrounding EISs. First, under *Cubby*, if an EIS does not exert editorial control, and does not know or have reason to know of the dissemination of illegal material, the EIS cannot be held liable for such illegal material.[182] This raises the second implication, that if the EIS knows or has reason to know of the offensive material it is legally obligated to remedy the situation or face legal liability.[183] However, once any particular EIS attempts to edit or filter out offensive material, that EIS is considered a publisher and held to the same legal standard as the originator of any offensive material.[184] Third, while the court in *Stern* relied on and cited *Cubby*, it failed to realize that the *Cubby* court had predicated its finding on the fact that CompuServe had no control or knowledge of the message posted, because it had been posted by a third party independent contractor.[185] Moreover, under *Stern*, an EIS need not even know of the posted material; it could be directly

177. *Id.*

178. *Id.* at 697 (emphasis added).

179. *Id.* (emphasis added).

180. *Id.* at 698 ("Affording protection to on-line computer services when they are engaged in traditional news dissemination, such as in this case, is the desirable and required result.").

181. *Id.*

182. Loundy, *supra* note 146, at 150-51.

183. *Id.* at 151.

184. *Stratton*, 1995 WL 323710 at *4.

185. *Cubby*, 776 F. Supp. at 138.

responsible for simply soliciting the posted material.[186]

2. Broadcast Media

Not all courts agree, however, that an EIS is analogous to print media. The Wisconsin Court of Appeals, for example, has held that the "nature of bulletin board postings on computer network services cannot be classified as print;"[187] instead, the court analogized EISs to broadcast media.[188] If this analogy is correct, then, because it is the FCC's statutory duty to regulate broadcasters,[189] EISs will likely become regulated by the FCC. Such regulation has traditionally resulted in affording broadcasters the most limited First Amendment protection.[190]

The Supreme Court has put forth two primary reasons—scarcity and intrusiveness—in requiring the FCC to regulate electronic and not print media under the First Amendment.[191] In *Red Lion Broadcasting Co., Inc. v. FCC*,[192] the Supreme Court upheld the constitutionality of regulating broadcast media more strictly than print

186. *Stern*, 626 N.Y.S.2d at 695 ("Delphi set up on its on-line electronic bulletin board, a subscriber-participation debate on the merits of [Howard] Stern's candidacy [for governor of New York].").

187. It's in the Cards, Inc. v. Fuschetto, 535 N.W.2d 11, 14 (Wis. Ct. App. 1995), *review denied*, 537 N.W.2d 574 (Wis. 1995) (refusing to find an EBB a "periodical" due to the sporadic nature of its postings).

188. *Id.* It is important to note that the *Fuschetto* court was dealing with a private, sports-only service which provided only e-mail and EBBs and was located on the Internet—not a commercial EIS. *Id.* at 13-14. The major difference is that before a user could join the SportsNet bulletin board, he would have to first subscribe to an EIS in order to access the Internet.

189. *See* 47 U.S.C. §§ 301-303 (1988). The Communications Act of 1934 "centralized all federal authority not only for licensing, but also for overseeing the conduct of common carriers and broadcasters in a permanent, funded Federal Communications Commission." Fred H. Cate, *The First Amendment and the National Information Infrastructure*, 30 WAKE FOREST L. REV. 1, 30 (1995).

190. *See, e.g.*, FCC v. Pacifica Found., 438 U.S. 726, 748 (1978) (The Supreme Court has "long recognized that each medium of expression presents special First Amendment problems . . . [a]nd of all forms of communication, it is broadcasting that has received the most limited First Amendment protection.").

191. *See* Philip H. Miller, *New Technology, Old Problem: Determining the First Amendment Status of Electronic Information Services*, 61 FORDHAM L. REV. 1147, 1150 (1993).

192. 395 U.S. 367 (1969).

because broadcast channels are a scarce public resource.[193] This argument, known as the "scarcity rationale,"[194] is based on the assumption that a broadcaster, in exchange for receiving the exclusive right to exploit such a valuable commodity, should expect and accept regulation intended to ensure that broadcasters operate in the public interest.[195] Additionally, the Court reasoned that the paramount right at issue was the right of the "viewers and listeners, not the right of the broadcasters."[196] Thus, "scarcity" allowed the Court to transform broadcasters into trustees of the public, requiring them to provide the public with "suitable access to social, political, esthetic, moral, and other ideas and experiences."[197]

The second rationale for distinguishing broadcasters from printed medium is the "intrusiveness" rationale put forth by the Supreme Court in *FCC v. Pacifica Foundation*.[198] In *Pacifica*, the Court upheld the FCC's right to sanction broadcasters for the transmission of obscene and indecent speech,[199] while acknowledging that similar governmental interference could be deemed unconstitutional if the exact material was disseminated in a print publication.[200] The Court focused not on the fact that broadcasters operate under a government license—as it had in *Red Lion*—but instead on the characteristics of the medium itself. First, the Court acknowledged that broadcast media had established a "uniquely pervasive presence" in American society.[201] The Court stressed that indecent material broadcasted over the airwaves confronted the citizen not only in public, but also in the privacy of his home, "where [his] right to be left alone plainly outweighed the First Amendment

193. *See id.* at 388-89; *see also* Miller, *supra* note 191, at 1150.

194. Miller, *supra* note 191, at 1150.

195. *Id.*

196. *Red Lion*, 395 U.S. at 390.

197. *Id.*

198. 438 U.S. 726 (1978).

199. *Id.* at 749-50. The Court held that a broadcaster must "channel" indecent material to times when children are not as likely to be in the audience, or else face sanctions. *Id.*

200. *Id.* at 741-42 n.17.

201. *Id.* at 748.

rights of an intruder."[202] Second, the Court found that broadcasting was "uniquely accessible to children."[203] The Court reasoned that adult bookstores and theaters can be prohibited from making indecent material available to children,[204] and that the ease with which children obtain access to broadcasted materials[205] combined with the "government's interest in the 'well-being of its youth'" justified the special treatment of indecent broadcasting.[206]

For purposes of this Note, *Pacifica* is of particular importance. Read broadly, *Pacifica* permits the government to limit communication systems' or services' First Amendment privileges, regardless of whether the service operates under a government license, if the service is pervasive and easily accessible to children.

3. Cable Television

The Supreme Court has held that cable television warrants a standard of analysis different from that applied to broadcasters.[207] This distinction is explained in the 1994 Supreme Court case, *Turner Broadcasting System, Inc. v. FCC*[208] In *Turner*, the Court addressed the "must carry" provisions of the Cable Television Consumer Protection and Competition Act of 1992 which required cable operators to carry the signals of local broadcast companies.[209]

---

202. *Id.*

203. *Id.* at 749.

204. *Id.*

205. *Id.* at 750. In a concurrence, Justice Powell elaborated on this point:

> In most instances, the dissemination of this kind of speech to children may be limited without also limiting willing adults' access to it. Sellers of printed and recorded matter and exhibitors of motion pictures and live performances may be required to shut their doors to children, but such a requirement has no effect on adults' access. . . . The difficulty is that such a physical separation of the audience cannot be accomplished in the broadcast media.

Id. at 758 (Powell, J., concurring in part).

206. *Id.* at 749.

207. United States v. Midwest Video Corp., 406 U.S. 649 (1972) (holding that the FCC has authority to regulate CATV at least to the "extent reasonably ancillary to the effective performance of the Commission's various responsibilities for the regulation of television broadcasting").

208. 114 S. Ct. 2445 (1994).

209. *Id.* at 2452-53 (construing the Cable Television Consumer Protection and Competition Act, Pub. L. No. 102-385, 106 Stat. 1460 (1992)). Congress overrode a

In a 5-to-4 decision, the Court refused to extend the "scarcity" rationale of *Red Lion* to cable television, holding that the unique physical limitations of the broadcast medium limited the *Red Lion* holding to broadcasters.[210] The Court reasoned that "given the rapid advances in fiber optics and digital compression technology, soon there may be no practical limitation on the number of speakers who may use the cable medium."[211] The Court, in finding that the "must carry" provisions were content-neutral,[212] held that the proper level of scrutiny applicable to content-neutral cable television restrictions is the intermediate level of scrutiny promulgated in *United States v. O'Brien*.[213] *Turner*, however, changed the *O'Brien* standard to read that the restriction on First Amendment freedoms could be no greater than "necessary," rather than "essential," emphasizing the Court's willingness to allow less restrictive means.[214] Consequently, if a regulation is content-based, the Court still continues to apply strict scrutiny, requiring a state to use the least restrictive, narrowly-tailored restriction.[215]

Cable television has been able to defeat regulatory measures more easily than broadcasting, even though both are afforded strict scrutiny protection in content-based restrictions. In *Cruz v. Ferre*[216] the Court of Appeals for the Eleventh Circuit held that the *Pacifica* rationale of broadcasting establishing a "pervasive presence" in

---

Presidential veto and passed the bill on October 5, 1992. *Id.* at 2452.

210. *Id.* at 2456 (citations omitted).

211. *Id.* at 2457.

212. *Id.* at 2459-60. "[L]aws that confer benefits or impose burdens on speech without reference to the ideas or views expressed are in most cases content-neutral." *Id.* at 2459.

213. 391 U.S. 367 (1968).

> [W]hen 'speech' and 'nonspeech' elements are combined in the same course of conduct, . . . government regulation is sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.

Id. at 376-77.

214. *Turner*, 114 S. Ct. at 2469.

215. *Id.* at 2459.

216. 755 F.2d 1415 (11th Cir. 1985).

society and being "uniquely accessible to children" was not applicable to cable television.[217] The *Cruz* court found cable television not as pervasive as broadcast media because a person must "affirmatively elect" both to have cable television come into their home and to purchase any extra adult programming services.[218] Additionally, the court noted that most cable television companies could provide customers with "lockboxes" that parents could use to prohibit access to certain channels.[219] Thus, the court found that prohibiting the dissemination of indecent material on cable television services fell outside the limited exceptions that *Pacifica* had allowed.[220] This language was echoed in *Community Television of Utah, Inc. v. Wilkinson*,[221] where a federal district court similarly held that cable television was not as pervasive as broadcast media, because cable television is not an "uninvited intruder" in the home.[222] Thus, cable programmers continue to remain immune from the Court's holdings in both *Red Lion* and *Pacifica* because cable television is not a scarce resource and is not an uninvited intruder into the home.

4. "Dial-a-Porn"

The Supreme Court analyzed adult services accessed by phone lines in *Sable Communications of California, Inc. v. FCC*[223] Under the amended Communications Act of 1934,[224] lawmakers prohibited the transmission of obscene and indecent communications over interstate telephone lines for commercial purposes.[225] In reviewing the amendment, the Court first concluded that obscene material

---

217. *Id.* at 1420.

218. *Id.*

219. *Id.*

220. *Id.*

221. 611 F. Supp 1099 (D. Utah 1985), *aff'd*, 800 F.2d 989 (10th Cir. 1986), *aff'd*, 480 U.S. 926 (1987).

222. *Id.* at 1113. Though the decision was affirmed by the Tenth Circuit, Judge Baldock wrote a lengthy special concurrence where he argued that the *Pacifica* rational of pervasiveness and accessibility to children was very appropriate when applied to cable. *See* Jones v. Wilkinson, 800 F.2d 989, 1007 (10th Cir. 1986) (Baldock, J., concurring).

223. 492 U.S. 115 (1989).

224. 47 U.S.C. § 223(b) (1982).

225. *Sable*, 492 U.S. at 117-19 (addressing the Communications Act of 1934). This type of communication is commonly known as "dial-a-porn." *Id.* at 119.

could be banned since obscenity retains no constitutional protection.[226] The Court next addressed banning indecent material, noting that "there is a compelling interest in protecting the physical and psychological well-being of minors"[227] that "extends to shielding minors from the influence of literature that is not obscene by adults standards."[228] The Court then distinguished *Sable* from *Pacifica*, noting first that in *Pacifica* the question of a total ban on indecent speech was never before the Court.[229] The Court found that in *Sable* there existed a less "pervasive" form of media than in *Pacifica*,[230] and that the telephone services in question had included safeguards designed to allow access to only adults.[231] The Court did, however, acknowledge that there is "no constitutional impediment" to enacting a law which would require an adult service to absorb all costs of providing efficient safety measures for minors.[232] Ultimately, the Court held that any complete ban on indecent speech was unconstitutional.[233]

---

226. *Id.* at 124.

227. *Id.* at 126.

228. *Id.*

229. *Id.* at 127.

230. *Id.* at 127-28. The Court explained:

> Placing a telephone call is not the same as turning on a radio and being taken by surprise by an indecent message. Unlike an unexpected outburst on a radio-broadcast, the message received by one who places a call to a dial-a-porn service is not so invasive or surprising that it prevents an unwilling listener from avoiding exposure to it.

Id. at 128.

231. *Id.* at 121-23. The Court relied heavily on a report made earlier by the FCC which determined that credit cards, access codes, and scrambling rules were satisfactory solutions to the problems of keeping indecent dial-a-porn messages out of the reach of minors. *Id.* at 128. The FCC, however, insisted that this report was no longer valid, and that these measures would no longer be effective enough. *Id.* The Court, however, found no evidence in the record to support the FCC's new position. *See id.* at 128-29.

232. *Id.* at 125.

233. *Id.* at 130-31.

5. Common Carriers

An argument also exists to classify EISs as a common carrier[234] because EISs provide extensive communications capabilities[235] and their services are accessed via telephone lines.[236] If considered a common carrier, an EIS would be a secondary publisher or distributor of material,[237] which has widely been adopted and applied to the electronic communications media including the telegraph,[238] telephone,[239] and ancillary services such as a telephone answering service.[240] Both the FCC and the courts have found that information transmitted via common carrier is the "sole responsibility or prerogative of the subscriber and not the carrier."[241] The EISs would welcome the heightened "know or have reason to know" standard of liability[242] because EISs claim it would increase the level of protection afforded to such material and would better protect privacy concerns.[243] Additionally, as common carriers, EISs

---

234. National Ass'n of Regulatory Util. Comm'rs v. FCC, 533 F.2d 601, 608-09 (D.C. Cir. 1976).

> A common carrier status is a quasi-public character, which arises out of the undertaking to carry for all people indifferently . . . . This does not mean that the particular services offered must practically be available to the entire public; a specialized carrier whose service is of possible use to only a fraction of the population may nonetheless be a common carrier if he holds himself out to serve indifferently all potential users.

Id. at 608.

235. *See* Evenson, *supra* note 94.

236. *See The Message*, *supra* note 143, at 1066. A user accessing an EIS requires a computer, a modem, and a phone line. The user then calls the "host" of the service. *Id.* "Once connected, the user can communicate over the [service] through the modem, which translates digital data from the sending computer into analog signals appropriate for phone lines." *Id.*

237. *See, e.g.*, Mason v. Western Union Tel. Co., 52 Cal. App.3d 429, 125 Cal. Rptr. 53 (1975); Von Meysenbug v. Western Union Tel. Co., 54 F. Supp. 100 (S.D. Fla. 1944).

238. Western Union Tel. Co. v. Lesesne, 182 F.2d 135 (4th Cir. 1950); O'Brien v. Western Union Tel. Co., 113 F.2d 539 (1st Cir. 1940).

239. Anderson v. New York Tel. Co., 35 N.Y.2d 746, 361 N.Y.S.2d 913, 320 N.E.2d 647 (1974).

240. People v. Lauria, 251 Cal. App. 2d 471, 59 Cal. Rptr. 628 (1967).

241. Frontier Broadcasting Co., 24 F.C.C. 251, 254 (1958); *see also The Message*, *supra* note 143, at 1090-91.

242. *See supra* note 237 (explaining the liability of a common carrier).

243. Constance Johnson, *Anonymity on line? It depends who's asking*, WALL ST. J.,

would have to make transmission services available to the public on a nondiscriminatory basis.[244] This regulatory policy of "universal service" aims at providing access to all households, which is consistent with President Bill Clinton's vision of the "National Information Infrastructure"—a computer network designed with the goal of "linking homes, businesses, labs, schools and libraries around the nation by the year 2015."[245]

B. *Congressional Actions and the EISs*

While courts continue to struggle with the legal status of an EIS, Congress has begun enacting measures aimed at regulating EISs. The relevant measures include the Electronic Communications Privacy Act of 1986 and the Communications Decency Act of 1995.

1. The Electronic Communications Privacy Act of 1986

Congress enacted the Electronic Communications Privacy Act of 1986 ("ECPA")[246] to more adequately address the interception and disclosure of interstate electronic communications.[247] The ECPA provides, in part, that "any person who— . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept . . . any wire, oral, or electronic communication" is subject to a fine or imprisonment.[248] The ECPA further prohibits the intentional use or disclosure of the contents of such communication that is known or could reasonably be known to have been intercepted.[249]

Nov. 24, 1995, at B1. While EISs contend that member privacy is a paramount consideration of theirs, they openly acknowledge that they, willingly cooperate with F.B.I. agents (who use questionable tactics to investigate EISs members) and willingly comply with civil subpoenas and request for discovery on their members' identities. John Byczkowski, *Do On-line services know too much?*, CINCINATTI ENQ., Oct. 15, 1995, at G3.

244. 47 U.S.C. § 202(a) (1988); *see also The Message*, *supra* note 143, at 1090.

245. *Computer Leaders Give Brown Plan for High-Speed Network*, FED. TECH. REP., Jan. 21, 1993, at 3 (addressing President Clinton's plan to establish a National Information Infrastructure).

246. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

247. 18 U.S.C. § 2511 (1994).

248. *Id.* at (1)(a).

249. *Id.* at (1)(c).

Congress also provided EISs with a loophole in the ECPA by exonerating an EIS from any lability if an employee intercepts or discloses an e-mail's contents pursuant to a necessary business duty.[250] Further exceptions are made if the message is inadvertently obtained by the EIS, when the message appears to pertain to a crime, or when the divulgence is being made to a law enforcement officer.[251] Thus, it is not completely accurate when EISs claim they are forbidden from regulating the contents of e-mail[252] because these exceptions tend to swallow the rule.

The ECPA also requires law enforcement agencies wishing to intercept or read e-mail to obtain a search warrant.[253] While the warrant requirement makes it harder for law enforcement agencies to obtain an e-mail's contents, it does not substantially impede efforts because EISs are usually overly-cooperative with law enforcement officials.[254]

---

250. *Id.* at (2)(a)(i).

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

Id.

251. *Id.* at (3)(b)(iv).

252. *See, e.g.*, Sandberg & Simpson, *supra* note 12; Murphy, *supra* note 16.

253. 18 U.S.C. § 2518 (1994). Importantly, new encryption software programs, such as PGP (Pretty Good Privacy) make these files inaccessible to unintended receivers, and thus very hard to regulate. *See Fordham Law Symposium*, *supra* note 6, at 367. Encrypted data requires a password to decode it, which would make some investigations, especially those revolving around child pornography, almost impossible to conduct. *See generally* Vic Sussman, *Policing cyberspace Cops want more power to fight cybercriminal*, U.S. NEWS & WORLD REP., Jan. 23, 1995, at 54-56. Additionally, widespread agreement within the on-line community and entrepreneurs hoping to conduct business on-line, that cryptography is necessary for privacy in a networked universe, forces law enforcement to combat strong issues of privacy. *Id.*

254. *See* Byczkowski, *supra* note 245 (CompuServe and America Online both cooperate with law enforcement officials in tracking down members); *see also* David Josar, *Cops crack down on child porn cases on the Internet*, DETROIT NEWS, Jan. 1, 1996, at B1 (America Online President Steve Case sent e-mail to all users warning them that if the company discovered members sending indecent materials, they would be turned over to

2. The Communications Decency Act of 1995

As originally proposed,[255] the Communications Decency Act of 1995 ("CDA") would have given prosecutors the ability to specifically prosecute EISs for transporting or for allowing minors access to indecent or obscene material.[256] Special interest groups, however—led by the EISs[257]—forced a modification of the CDA[258] allowing EISs to be immune from prosecution if they put forth a "good faith effort" to keep minors safe.[259] As a response, EISs reacted by equipping their services with various safety measures.[260]

---

law enforcement).

255. The Communications Decency Act, as originally proposed, was introduced on February 1, 1995 by Senator James Exon (D. Neb). S. 314, 104th Cong., 1st Sess. (1995).

256. *See id.*; *see also* Nathaniel Sheppard Jr., *On-Line Pornography: Control May Prove as Tricky as Definition*, ST. LOUIS POST-DISPATCH, Dec. 23, 1995; Sandberg & Simpson, *supra* note 12.

257. Kara Swisher, *Ban on On-Line Smut Opposed: High Tech Coalition Pushes Software Allowing Parents to Decide*, WASH. POST, July 18, 1995, at D3. The EISs successfully avoided liability with a strong campaign of effective self-regulation:

> With congressional attention focused on the easy availability of pornography on computer networks, the [EISs] converged to try to head off passage of legislation that would ban obscene material outright [Communications Decency Act]. Their solution: "smut filters," software that's meant to let parents control what children can get with computers, coupled with a nationwide campaign to help educate parents about the technology.

Id.

258. *See* Sheppard, *supra* note 256.

259. Under the enacted Communications Decency Act, the FCC may suggest safe harbors of protection. *See supra* note 144, § 502.

260. *In the porn fight, parents are first, best defense*, USA TODAY, Dec. 7, 1995, at 10A. The protectionary measures offered by the major on-line services are:

> America Online: Allows parents to block access to chat rooms through use of a password. Also can block areas by specifying key words, subject areas or newsgroups;
>
> Prodigy: Runs screening software that monitors bulletin boards and blocks language inappropriate for children. Also lets parents monitor Internet web sites their children have visited;
>
> CompuServe: Offers Internet in a Box for Kids, which contains a SurfWatch program that lets parents monitor and limit access.

Id. In addition, various software is available on the market if the EIS does not have built in safeguards. *Id.* Also, most EISs use "cybercops"—hired monitors who view the activity occurring on-line and ensure that it conforms to the terms of service. Peter Eisler, *Policing the Internet*, USA TODAY, Sept. 5, 1995, at 1. Moreover, EISs are forming a

In February, 1996, President Clinton signed into law the CDA as part of the Telecommunications Act of 1996 ("Telecom Act").[261] The enacted CDA[262] criminalizes, among other things, knowingly transmitting "indecent" material to minors over computer networks.[263] The maximum penalty for such offenses is two years in jail and a fine of up to $250,000.[264] Senator Jim Exon (D. Neb.), the CDA's author, stated that the CDA is a necessary tool for dealing with the problem of on-line child pornography because the CDA helps prevent pedophiles from engaging minors in sexual conversation.[265] This tool, however, again only addresses the problem of individual violators.

---

consortium called the "Information Highway Parental Empowerment Group," formed to create on-line standards for children. *See* Christopher Parkes, *Internet users may form porn patrol*, FIN. TIMES, Sept. 15, 1995, at 4; L.A. Lorek, *Dangers can lurk in On-line world*, FT. LAUDERDALE SUN-SENTINEL, Aug. 30, 1995, at 1B.

261. Pub. L. No. 104-104, 100 Stat. 56 (1996) (to be codified at 47 U.S.C. §§ 151-614).

262. *Id.* at §§ 501-09.

263. *Id.* at § 502(2). The new law amends 47 U.S.C. § 223(d)(B) by adding penalties for the following:

> (d) Whoever-
>
> (B) uses any interactive computer service to display in a manner available to a person under 18 years of age,any comment, request, suggestion, proposal, image, or other communication that in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication.

Id.

264. *Id.*

265. *See* Sen. Jim Exon, *Internet Privacy: How far should federal regulation go?*, COMPUTERWORLD, Feb. 19, 1996, at 74. The Senator stated:

> A recent FBI sting operation [Innocent Images] resulted in the arrest of several people nationwide for distributing child pornography over computers, which shows that some of our child pornography laws also work in the world of cyberspace. But we need more legal tools to deal with this type of problem before more child victims are lured into pornography. Our law will shield children from pornography that is only a few clicks away on their computers, and will make it illegal to engage children in sexual conversations on-line.

Id.

III. PROSECUTING THE EISs

In determining whether an EIS should be prosecuted under the existing criminal laws, prosecutors should proceed carefully. A prosecutor should first analyze the other forms of communication to see what level of responsibility seems appropriate to apply to an EIS. The prosecutor should then determine if the EIS knew or should have known that child pornography was being distributed and/or possessed within the EIS's dominion. Finally, prosecutors should weigh all relevant social and economic policy considerations before proceeding.

A. *Comparing EISs to Other Forms of Communication*

1. EISs as Primary Publishers

An EIS's liability is certain if the EIS is regarded as a primary publisher of the material, because primary publishers are considered creative, knowing participants in the process of publication who are ultimately responsible for material published.[266]

While the *Stratton* court found an EIS to be a primary publisher,[267] Congress has decided differently.[268] The issue has yet to be decided by the Supreme Court; existing precedent, however, could support the argument that EISs should be considered primary publishers. The authority is *Smith*,[269] which the *Cubby* court relied upon in finding that an EIS should be a secondary publisher.[270] The compelling argument presented in *Smith* was that a bookseller's inability to read all books and be aware of their contents restricts the amount of non-obscene material on the market—material

---

266. *See* Robert Charles, *Computer Bulletin Boards and Defamation: Who Should Be Liable? Under What Standard?*, 2 J.L. & TECH. 121, 131 (1987).

267. Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 at *3-*5 (N.Y. Sup. May 24, 1995) (holding that Prodigy is a primary publisher of the material posted on its service).

268. The Conference agreement on the Communications Decency Act § 509 states that "[o]ne of the specific purposes of this section is to overrule *Stratton Oakmont v. Prodigy* and any other similar decisions which have treated such providers as publishers or speakers of content that is not their own because they have restricted access to objectionable material." S. REP. NO. 230, *supra* note 144, § 509, at 194.

269. 361 U.S. 147 (1959).

270. Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135, 139-40 (S.D.N.Y. 1991).

which the state cannot regulate.[271] However, two fundamental differences exist when comparing an EIS's ability to edit out child pornography with other publishers and distributors ability to eliminate obscenity. First, child pornography retains no First Amendment protection[272] making it, unlike obscenity, illegal for any community to possess or distribute.[273] This status places the burden on the EIS to actively remove all child pornography from its service. Second, new technological advances make it easy for an EIS to obtain knowledge of the material it distributes or possesses. Certain words[274] that connote child pornography can instantly be detected and their corresponding files checked by the EIS's monitors for their contents, removing the tedious burden of having to manually read each file to learn its contents. Additionally, while graphics files are difficult to scan for content, some EISs have circumvented this problem by not automatically decoding graphics files, leaving the files in a scrambled format.[275] Users then must go to a "decoding" area within the EIS where pictures can easily be monitored. Any child pornography can then effectively be eliminated before being published.

Arguments against the screening solution—either that people can mask material by using different file names or encrypt[276] it so

---

271. *Smith*, 361 U.S. at 153-54 ("The bookseller's limitation in the amount of reading material with which he could familiarize himself, and his timidity in the face of his absolute criminal liability, thus would tend to restrict the public's access to forms of the printed word which the State could not constitutionally suppress directly.").

272. New York v. Ferber, 458 U.S. 747, 764 (1982); *see also supra* notes 31-45 and accompanying text (discussing the *Ferber* case).

273. The Supreme Court has afforded greater protection for obscene material than child pornography. *Compare* Stanley v. Georgia, 394 U.S. 557 (1969) (the government may not regulate the private possession of obscene materials by an individual at home) *with* Osborne v. Ohio, 495 U.S. 103 (1990) (the government may regulate the private possession of child pornography by an individual at home).

274. *See* Symposium: *Emerging Media Technology and the First Amendment*, 10 YALE L. J. 1619, 1632-34 (1995) (describing the various file screening methods available) [hereinafter *Yale Symposium*].

275. Andy Covell, *Online Services And The Internet: The Network Manager's Friend Or Foe?*, NETWORK COMPUTING, Jan. 15, 1996, at 138 (stating which EISs offer auto-decoding software, and which ones require additional software in order to decode pictures).

276. *See supra* note 253 (explaining the methods of encryption).

that an EIS could never access the contents—were addressed in *Smith*, where the Court seemed to leave open the question of culpability in order to account for such future circumstances.[277] Accordingly, an EIS's options are to either not publish the submitted encrypted item, or argue that its culpability should be mitigated because it was unaware of the material. Thus, if correctly structured, the entire procedure of posting material on an EIS can resemble letters and articles submitted to a newspaper for publication in which editorial discretion is maintained by the newspapers.[278]

2. EIS as Distributors or Common Carriers

EISs contend that they are merely distributors, or common carriers of material, rather than publishers of the material posted on their services.[279] At least one court, the *Cubby* court, agreed. In *Cubby*,[280] the court found EISs analogous to print distributors,[281] which, like common carriers,[282] are held to a "know or have reason to know" standard of liability.[283] In order for an EIS to be consid-

---

277. *Smith*, 361 U.S. at 154.

> We need not and most definitely do not pass today on what sort of mental element is requisite to a constitutionally permissible prosecution of a bookseller for carrying an obscene book in stock; whether honest mistake as to whether its contents in fact constituted obscenity need be an excuse; whether there might be circumstances under which the State constitutionally might require that a bookseller investigate further, or might put on him the burden of explaining why he did not, and what such circumstances might be.

Id. Justice Frankfurter clarified this point in his concurrence, stating that "[h]ow much or how little awareness that a book may be found to be obscene suffices to satisfy scienter, or what kind of evidence may satisfy the how much or the how little, the Court leaves for another day." *Id.* at 161 (Frankfurter, J., concurring).

278. At least one court agrees with this structure. *See* Stern v. Delphi Internet Servs. Corp., 626 N.Y.S.2d 694, 697 (N.Y. Sup. Ct. 1995) (finding that the service is analogous to a letters-to-the-editor column of a newspaper); *see also supra* notes 172-86 and accompanying text (discussing the *Stern* case).

279. *See, e.g.*, America Online, TERMS OF SERVICE § 2.7, *Third Party Content* (Aug. 1995) which states, in relevant part, that "AOL Inc. is a distributor (and not a publisher) of Content supplied by third parties and Members. Accordingly, AOL Inc. has no more editorial control over such Content than does a public library, bookstore, or newsstand."

280. Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

281. *Id.* at 140 ("CompuServe's CIS product is in essence an electronic, for profit library that carries a vast number of publications . . . .").

282. *See supra* note 234 (discussing common carriers).

283. *Cubby*, 776 F. Supp. at 140-41.

ered a distributor or common carrier, the EIS must act as a complete conduit, refusing to apply any editorial discretion over the material.[284] EISs, however, are not complete conduits of information; instead, they are responsible for providing services and information.[285] Additionally, as demonstrated with the debate surrounding the CDA,[286] EISs are being required to provide further control over their services or else face penalties.[287] Moreover, editorial discretion is already being exercised by the EISs, who are beginning to actively eliminate blatant sexual messages.[288] While monitoring seems an essential facet of on-line safety, acting as anything other than a complete conduit precludes an EIS from being considered a common carrier.

Relying on *Smith*, however, the *Cubby* court felt that holding an EIS responsible for its postings would place too great a restriction on constitutionally protected material.[289] Accordingly, various libertarians argue that unless EISs are considered distributors or common carriers of the information they process, a substantial "chilling effect" will occur on the exchange of constitutionally protected material.[290] This argument, however, is not compelling

---

284. *See The Message*, *supra* note 143, at 1090-91.

285. *Easy-access, on-line pornography draws fire*, BALTIMORE EVENING SUN, July 25, 1995, at 1A (in addition to information, an EIS's normal fare is shopping and games).

286. *See supra* notes 255-58 and accompanying text (discussing the Communications Decency Act).

287. *See supra* notes 255-58 and accompanying text.

288. *See Fordham Law Symposium*, *supra* note 6, at 311-12. In fact, EISs exert editorial control, especially when the word "young" is being used to describe a chat room. *Id.* Additionally, both America Online and CompuServe specifically reserve the right to edit out material they deem unsuitable to be posted on their service. *See* AMERICA ONLINE TERMS OF SERVICE § 4.2 (Aug. 1995) ("AOL Inc. reserves the right to prohibit conduct, communication, or Content [sic] which it deems in its discretion to be harmful to individual members . . . ."); COMPUSERVE INFORMATION OPERATING RULES (Sept. 1995) ("CompuServe reserves the right in its sole discretion to edit or delete any information . . . .").

289. *Cubby*, 776 F. Supp. at 139-41. Applying the same reasoning as the Supreme Court in *Smith*, the *Cubby* court held that "the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information." *Id.* at 140.

290. *See generally Yale Symposium*, *supra* note 274.

when considering child pornography. The "chilling effect" that accompanies the enactment of any restriction stems from the spillover effect which erroneously omits protected material.[291] For example, in libel situations, truths may be omitted because there exists no way for the EIS to verify the statement.[292] Likewise, due to the subjective nature of the *Miller* community standards test,[293] material not yet deemed obscene may also be erroneously eliminated. Thus, under an obscenity statute, EIS monitors would be inclined to remove any potentially obscene picture rather than attempt to conform to this inconsistent standard. Child pornography, however, presents no such problem, as all child pornography is *per se* illegal.[294] Monitors attempting to conform to a child pornography statute are therefore only concerned with removing any material that objectively depicts a minor in a questionable manner. Consequently, requiring the removal of child pornography rather than the broad category of obscenity vastly reduces any "chilling effect," as the only protected material that may erroneously be eliminated is a picture where an older model is attempting to appear like a minor.

3. EISs as Broadcasters

Even if EISs are not found analogous to primary publishers, they still may be considered broadcasters. Based on the Supreme Court's holding in *Pacifica*, broadcaster status makes prosecution of an EIS for child pornography inevitable. In *Pacifica*[295] the Court acknowledged that it allows the FCC enormous discretion when regulating broadcasters because broadcasters have established a "uniquely pervasive presence" in American lives.[296] This analysis

---

291. *See* Smith v. California, 361 U.S. 147, 154-55 ("Doubtless any form of criminal obscenity statute applicable to a bookseller will induce some tendency to self censorship and have some inhibitory effect on the dissemination of material not obscene . . . .").

292. *See, e.g.*, Cubby, 776 F. Supp. at 140 ("it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements . . .").

293. *See* Miller v. California, 413 U.S. 15 (1973).

294. *See supra* notes 31-45 and accompanying text (discussing the illegality of child pornography).

295. 438 U.S. 726 (1978).

296. *Id.* at 748.

can be readily applied to EISs. The rapid increase in both the number of people on-line[297] and the "http"[298] or "WWW"[299] that accompanies most modern advertisements indicate that EISs are also establishing a "uniquely pervasive presence" in American society. Additionally, the Court stressed in *Pacifica* that the material presented over the airwaves confronts the citizen "not only in public, but also in the privacy of his own home,"[300] where an individual's right not to be invaded by obscene material prevails.[301] With EISs, people are being infiltrated by unsolicited child pornography predominantly in their homes,[302] thus infringing on their right not to be invaded. Moreover, this open dissemination of child pornography via EISs injures minors because child pornography victimizes the portrayed minor every time the picture is displayed.[303] Finally, the Court's statement in *Pacifica* that "broad-

297. Lorek, *supra* note 260. ("More than one-third of all households have a personal computer and many are hooked to the Internet . . . and millions more people subscribe to commercial on-line services including America Online, Prodigy and CompuServe.").

298. *See generally* Kassel & Kassel, *supra* note 104, at 386 ("'http' refers to Hyper Text Transfer Protocol, which are the links that allow the user to follow a continuous trail of information wherever it may lead, whether to another part of the document you are in or to a remote terminal located around the world, simply by clicking your mouse on the appropriate hypertext link.").

299. *Id.* at 384-85. "'WWW' refers to the 'World Wide Web,' or the 'Web,' which links together textual, audio, and pictorial information, allowing the user to retrieve not only standard textual material . . . but also to directly view images and hear sound recordings that supplement the texts on Web Sites." *Id.*

300. *Pacifica*, 438 U.S. at 748.

301. Red Lion Broadcasting Co. v. FCC, 395 U.S. 367, 390 (1969) ("It is the right of the viewers and listeners, not the right of the broadcasters, which is paramount.").

302. Kara Swisher & John Schwartz, *Walking the Beat in Cyberspace; On-Line Services Struggle with how to Combat Smut and Protect Privacy*, WASH. POST, Sept. 15, 1995, at F1 (man receives an unsolicited piece of e-mail entitled "14years.jpg" which when decompressed was "two 14-year-old boys doing something you can't print"); Smith & Mosely, *Child Porn Shows Up in PC Mailbox*, ST. LOUIS POST-DISPATCH, Aug. 27, 1995, at 1D (man returned from hiatus to find 15-20 pieces of unsolicited e-mail which included solicitations for phone-sex companies, photographs of naked men and women, and graphic photographs of children, some engaged in sex acts).

303. *See* United States v. Rugh, 968 F.2d 750, 756 (8th Cir. 1992) (quoting S. REP. NO. 438, 95th Cong., 2d Sess., at 9 (1978) and concluding that "[f]rom this, we have no trouble concluding that the primary victim under 18 U.S.C. § 2252(a)(2) is the exploited child.").

casting is uniquely accessible to children"[304] and therefore needs close monitoring also applies to EISs. President Clinton strongly supports a "National Information Infrastructure" which would "link every home, business, lab, classroom and library by the year 2015" through on-line services.[305] Accordingly, the President has proposed linking California's public facilities as a model for this endeavor, claiming that he "want[s] to get the children of America hooked on education through computers."[306] This has triggered one EIS to offer "unlimited, free access to its online service for California's public schools in the coming year."[307] Thus, making the online world uniquely accessible to minors, according to *Pacifica*, allows a state to make the necessary infringements to ensure the safety of those minors.

4. EISs as Cable Television

EISs could certainly argue that they resemble services like cable television[308] rather than broadcasters. They would do so knowing that, if successful, they could be subject to a more lenient standard of analysis than broadcasters.[309] Courts have generally used a lesser standard for cable television providers because the service providers have adequately structured their systems to protect viewers from unwanted material.[310] Following these holdings, EISs could claim that they should not be held liable for harms to minors because they also have adequately structured their systems to protect users from unwanted material. As with cable, EISs could argue that people must "affirmatively elect"[311] to connect with an EIS, and that therefore it is not the "uninvited intruder"

---

304. *Pacifica*, 438 U.S. at 749.

305. Cate, *supra* note 189, at 6.

306. Susan Yoachum & Edward Epstein, *Internet in Every School*, S.F. CHRON., Sept. 22, 1995, at A1.

307. *Id.*

308. *See supra* notes 207-23 and accompanying text (discussing the cable television industry).

309. *See* Turner Broadcasting System, Inc. v. FCC, 114 S. Ct. 2445, 2457 (1994).

310. *See, e.g.*, Cruz v. Ferre, 755 F.2d 1415 (11th Cir. 1985); Community Television of Utah, Inc. v. Wilkinson, 611 F. Supp. 1099 (D. Utah 1985), *aff'd*, 800 F.2d 989 (9th Cir.), *aff'd*, 480 U.S. 926 (1987).

311. *Cruz*, 755 F.2d at 1420.

broadcasting presents into the home.[312] Also, in accordance with cable "lockboxes,"[313] EISs offer "parental controls"[314] which parents can use to prohibit minors access to certain areas.

These contentions, however, are inappropriate when analyzing EISs and child pornography for three reasons. First, in the cable television cases the courts weighed the rights of adults to receive indecent material, a right which retains First Amendment protection.[315] There is no right, however, to receive unprotected material such as child pornography.[316]

Second, cable television programmers are required, in addition to providing lockboxes, to post warnings of adult material and scramble unaccessed channels to further prevent access by minors.[317] On an EIS, however, no requirement exists to post warn-

---

312. *Wilkinson*, 611 F. Supp. at 1113.

313. *See Cruz*, 755 F.2d at 1420.

314. See Swisher & Schwartz, *supra* note 302.

> [P]arental controls range from blocking out or restricting access to some areas of the service to children, prominently posting on-line rules . . . [to] offering new software that can filter out files that contain pornographic material and stepping up the presence of human 'guides' throughout the system to monitor the bulletin boards and popular 'chat rooms.'

Id. Additionally, the National Center for Missing and Exploited Children in Arlington, Va. now distributes a brochure outlining precautions parents need to take. Highlights include:

> - Never give out personal information such as your address, telephone number or the name and location of your school.
> - Never agree to get together with someone you meet on-line.
> - Do not respond to any messages that are mean or make you feel uncomfortable.

The center's entire pamphlet is available free of charge by calling 1-800-843-5678. *Child Safety on the Information Highway*, Nat. Ctr. for Missing & Exploited Children (1995).

315. *See, e.g.*, FCC v. Pacifica Found., 438 U.S. 726 (1978).

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

317. Section 505 of the Communications Decency Act amended 47 U.S.C. § 641 to read as follows:

> Sec. 641. Scrambling of Sexually Explicit Adult Video Service Programming
> (a) REQUIREMENT- In providing sexually explicit adult programming or other programming that is indecent on any channel of its service primarily dedicated to sexually-oriented programming, a multichannel video programming distributor shall fully scramble or otherwise fully block the video and audio portion of such channel so that one not a subscriber to such channel or programming does not receive it.

ings of the dangers on advertisements for the services, on the disks used to load the services, or during the installation process; thus, no such warnings appear at any of these stages. Thus, while an adult must set up an account with an EIS—a credit card or checking account is generally needed to set up an account—the adult setting up the account is not notified of any dangers until they are signed on to the EIS. Once signed on, warnings must be actively sought by the member, and once found, are not specific as to the type of dangers minors encounter on-line.[318] Consequently, effective parental controls on the EIS have become ineffective because parents do not have accurate information describing the dangers to minors[319] These lack of warnings, combined with advertisements claiming EISs are "family fun,"[320] make minors more vulnerable to attacks on-line because parents are left with a false sense of securi-

---

S. REP. NO. 230, *supra* note 144, at 84.

318. *See, e.g.*, A Letter to Parents from Steve Case, President, America Online, Aug. 31, 1995:

> As a parent, I try to share in my children's online experiences. But I'm also keenly aware of potential dangers in the online universe—as there are in everyday life—so I make it a point to restrict their exposure to the areas of the service I feel would be inappropriate. That's the reason we have an ever-expanding parental controls area. It lets you—the parent—guide your children to what you believe is appropriate, and what's not. And it gives you the tools so that when your children are online, their environment is tailored to meet their expectations.

(on file with the *Fordham Intellectual Property, Media & Entertainment Law Journal*).

319. Senator Exon, the CDA's sponsor, is skeptical about the efficiency of these parental controls:

> Any kind of blocking device is an important step in the right direction . . ., though I heard precious little from the industry until I rang their bell. We may need these tools but we also need more federal laws . . . . I mean, if we gave everyone a bulletproof vest, it does not mean we should repeal the murder laws.

Swisher, *supra* note 257 (comment of Sen. Exon); *see also Teens stray under the spell of cybersex*, STAR LEDGER, Jun. 10, 1995 ("Thousands of parents feel secure that their child is in their room on the computer being productive . . . [b]ut a lot of parents don't know how to use the services kids do."); *Welcome to America Online's Parental Controls Center*, Aug. 9, 1995 (explaining what the controls can block, but no mention as to why parents would want to block these areas) (on file with the *Fordham Intellectual Property, Media & Entertainment Law Journal*).

320. *See, e.g.*, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 at *5 (N.Y. Sup. May 24, 1995) (finding that an EIS had held itself out to be "family-oriented").

ty.

The third difference between the safety features found on cable television systems and EISs is that, unlike cable television, there is no system of "scrambling" adult material once signed on to an EIS. EISs require members to seek out protection and block offensive material rather than utilizing a more sensible system, such as requiring members to affirmatively seek out and sign up for adult material. EISs, however, have little, if any, incentive to warn parents of the dangers because growth of on-line service remains tremendous[321] and people are not on-line to access information; they are overwhelmingly using EISs to communicate electronically.[322] While "cybercops" are hired by the EISs to monitor the chat rooms and EBBs, these monitors do nothing unless a complaint is received.[323] This security system allows pedophiles to misuse the EISs,[324] and continues to allow the daily distribution and solicitation of child pornography.[325] Thus, EISs have not conformed to the cable system of security for children, and should not be granted the higher level of protection the Supreme Court has given to cable television.

5. EISs Analogous to "Dial-a-Porn" Telephone Services

Though not identical, an analogy can be drawn between EISs and dial-a porn telephone services in that a telephone is used to access adult material. In *Sable*, the Court reasoned that placing a telephone call to a specific service was completely different from receiving a surprise indecent message via broadcast communica-

---

321. *See supra* note 93 (demonstrating the tremendous growth in on-line subscribers).

322. Evenson, *supra* note 94 (communications is the primary reason members access EISs).

323. Eisler, *supra* note 260 ("We only go in if someone sends an alert . . . . As long as nobody complains, they can do what they want." (quoting Ana Pouso, supervisor of Prodigy's cybercops)).

324. Lorek, *supra* note 297 ("'We're seeing more and more pedophiles using computer on-line services to meet and talk to children.'" (comments of Jo McLachlan, safety and education instructor, Adam Walsh Foundation, Orange, Cal.)).

325. *See* Chandrasekaran, *supra* note 11. The FBI reports that the Landover, Md. squad alone, receives at least two or three complaints a day about on-line child pornography and messages seeking sex with minors. *Id.*

tion.[326] While it is true that an EIS user must affirmatively elect to sign on to the service, EIS members are receiving unsolicited child pornography in their "mailboxes"[327] because the current safety controls are unable to prevent this occurrence.[328] Additionally, *Sable* recognized that the primary reason for regulating communication is to protect "the physical and psychological well-being of minors"[329] which can include at times "shielding minors from the influence of literature that is not obscene by adult standards."[330] This reasoning can directly be applied to shielding minors from child pornography on an EIS. Finally, the Court in *Sable*, as it did when it analyzed safeguards in the cable television industry,[331] again acknowledged the importance of providing such safeguards to ensure that minors are not able to access adult material.[332] The Court found that credit card requirements, access codes, and scrambling rules were enough protection, despite the government's insistence that a total ban was the only effective method of protecting minors.[333] These protectionary methods, again, are not adequate when discussing child pornography and an EIS. With child pornography, there is no right under any circumstances to view or possess the material.[334] Thus, the issue is not just how to keep minors away from child pornography, but how to ensure that no one, including adults, has access to such material. Additionally, if a minor was able to bypass the safeguards and access dial-a-porn, the verbal interaction required with an adult operator acts as an additional safety measure, alerting the operator that there may be a minor involved. This safety measure does not exist with an EIS because minors are able to identify themselves as adults and utilize

326. Sable Communications v. FCC, 492 U.S. 115, 127-28 (1989).

327. *See supra* note 286 (discussing members of EISs who received unsolicited child pornography).

328. *See, e.g.*, Smith & Mosely, *supra* note 302.

329. *Sable*, 492 U.S. at 126.

330. *Id.*

331. *See supra* text accompanying note 310-13 (discussing parental controls provided by cable television).

332. *Sable*, 492 U.S. at 128-29.

333. *Id.*

334. *See supra* notes 31-45 (discussing the *per se* ban on child pornography).

the service simply by typing in the appropriate commands; no visual or verbal interaction is necessary.

This dehumanization presented by EISs also thwarts other forms of safety that the EISs promote; primarily, the community "watchdogs," which entail adults on-line reporting violations of the law to the EISs or law enforcement authorities.[335] While this has effectively protected minors numerous times,[336] it cannot provide adequate security for minors who identify themselves as adults, or for situations where adults identify themselves as minors in order to approach minors undetected. Thus, EISs should retain full liability for child pornography and offenses involving minors until the safety measures available on EISs afford users sufficient protection from unwanted, illegal material.

B. Establishing if an EIS has the Requisite Knowledge for Prosecution Under the Existing Child Pornography Laws

The cases in which individuals have thus far been prosecuted have provided sufficient proof that a jury could reasonably conclude that an EIS "knew or should have known" that its system distributed child pornography, because the mere descriptions of the material gave adequate notice as to the contents.[337] Furthermore,

---

335. One prominent community group of watchdogs, the Guardian Angels, has devoted a segment of its time to actively parol the EISs. *See Cyber Angels a Hindrance as they 'Net Surf for Porno* (Nat'l Pub. Radio broadcast, Sept. 25, 1995).

336. *See, e.g.*, United States v. Chapman, 60 F.3d 894 (1st Cir. 1995) (EIS user reports child pornography violator to FBI and acts in a sting operation with the FBI); United States v. Maxwell, 42 M.J. 568 (A.F. Ct. Crim. App. 1995) (EIS user reports multiple child pornography violators to FBI).

337. At least four circuit courts have held that the descriptions of the material can be used to determine knowledge of the material's content as well as to satisfy the "probable cause" threshold for issuing a warrant. *See* United States v. Kimbrough, 69 F.3d 723, 734 (5th Cir. 1995) (allowing descriptions of .GIF files "Bound and Gagged Spread in a Chair," "Eight Years Indian Girl" & "Preeteen School Girl" could sufficiently support a conviction for knowingly receiving sado-masochistic material and child pornography); United States v. Driscoll, 59 F.3d 173 (7th Cir. 1995) (finding that checking off "Teen Sex," "Pre-teen Sex," and "Animal Encounters" is enough to show that one knew the type of material they were receiving); United States v. Long, 42 F.3d 1389 (6th Cir. 1994) (finding that merely ordering tapes bearing the name "Seventeen" & "Your Key to 14 Candid Amateur Teenies, Volume 3" with a written description claiming: "Peer into a forbidden teenage world: 12 very young but extremely randy girls show themselves for the first time in front of the camera. Real amateur items, full of candid camera shots of

courts have ruled that constructive possession satisfies the possessory requirements under the Child Protection Act.[338] As previously demonstrated, some child pornography is not scrambled or hidden in any manner; instead it is openly described and portrayed within the EIS.[339] Additionally, child pornography is also traded in rooms with obvious names[340] which are open to all members, including minors. Those EISs with monitors are clearly aware—or should be clearly aware—of these rooms and the activities that occur within them because such monitors are assigned to patrol the rooms and shut them down if certain activity occurs.[341] These monitors, while seemingly ineffective for purposes of protecting minors,[342] have established knowledge of the child pornography on behalf of the EIS. Therefore, prosecutors should be able to make a strong case against the EISs for any child pornography that is openly displayed or described within the system.

C. *Deciding to Prosecute*

The decision to prosecute an EIS is not an easy one. Prosecutors[343] applying the Child Protection Act to individual violators struggle to ascertain the requisite intent.[344] Many people come

---

real school girls . . .," was enough to show knowledge that the tape contained child pornography); United States v. Browles, 37 F.3d 1314 (8th Cir. 1994) (finding that even though the government failed to prove the actual individuals depicted were under 18, and resolution of the images were blurred, testimony indicated that defendant had used the word "teenies" when ordering the material, and this was a term used in child pornography circles to refer to minors).

338. *See, e.g.*, United States v. Layne, 43 F.3d 127, 131 (5th Cir. 1995) (finding that possession under 18 U.S.C. § 2252(a)(4)(B) can be ownership, dominion or control over premises in which an item is concealed).

339. *See supra* notes 127-32 (demonstrating the open nature of graphic language implying child pornography).

340. *See supra* note 129 (showing the various graphic names of rooms found on an EIS).

341. *See supra* note 288 (EIS monitors shut down various chat rooms when the word "young" appeared).

342. *See supra* note 323 (showing that monitors on Prodigy only go in if someone sends out an alert).

343. The Department of Justice's Criminal Division's Child Exploitation and Obscenity Section handles these particular cases. *See infra* note 352.

344. *See Fordham Law Symposium*, *supra* note 6, at 298.

across computer pornography inadvertently[345] while "surfing";[346] others receive the material completely unsolicited.[347] This has forced investigators and prosecutors to proceed cautiously and direct their efforts to the individuals they know are "predisposed to engaging in behavior which sexually exploits children."[348] Investigations are also being strictly limited to large distributors.[349] Images must be explicit and clearly depict minors,[350] and the only arrests made to date for solicitation are of those individuals who arrange and actually show up at face-to-face meetings with a minor.[351] Once satisfied that these conditions have been met, however, prosecution is aggressive,[352] and penalties are substantial[353] if the defendant is convicted.

---

345. Meeks, *supra* note 115. Carnegie-Mellon University Professor Sara Kiesler has contended that when people access sexually oriented material, it is mostly out of curiosity and "there is not a high percentage of repeat access." *Id.*

346. "Surfing" is a slang term used to describe behavior on the Internet analogous to "clicking" around the stations of a television with a remote control.

347. *See supra* note 302 (members of an EIS received child pornography unsolicited).

348. *See Fordham Law Symposium, supra* note 6, at 301.

349. "Operation Longarm" was the first investigation to specifically target child-porn swapping over computers. This investigation did not involve a commercial EIS but instead focused on a private Electronic Bulletin Board, located in Denmark, whose members paid $80 a year to access and download child pornography. *See COMPUTER PORN: High tech child pornography ring busted*, TIME, Mar. 15, 1993, at 22. The investigation led to federal Customs agents raiding over one hundred homes in eighteen different states. *Id.*

350. *See* Chandrasekaran, *supra* note 11 (comments of FBI Agent Kevin Stafford).

351. *Id.*

352. The Department of Justice's position is that "[t]he Criminal Division's Child Exploitation and Obscenity Section is aggressively investigating and prosecuting the distribution of child pornography and obscenity through computer networks, and the use of computers to locate minors for the purposes of sexual exploitation." Letter from George C. Burgasser, Acting Chief, U.S. Department of Justice, Criminal Division, and J. Robert Flores, Acting Deputy Chief, U.S. Department of Justice, Criminal Division, to Joseph N. Campolo, Student, Fordham Law School (Sept. 29, 1995) (on file with the *Fordham Intellectual Property, Media & Entertainment Law Journal*).

353. *Clinton Signs Child Porn Bill*, FT. LAUDERDALE SUN-SENTINEL, Dec. 24, 1995, at 3A. Penalties for people convicted of causing a child to engage in sexually explicit conduct before a camera were increased from the range of 57 to 71 months to 70 to 87 months. *Id.* Sentences for those convicted of distributing visual depictions of such activity increased from 18 to 24 months to 24 to 30 months. *Id.* The sentencing increases double if a computer is used to transmit child pornography. *Id.*

Even proceeding carefully, however, it is evident that child pornography not only exists, but is pervasive,[354] on EISs. Additionally, EISs have known this for at least five (and probably nine) years.[355] Instead of being responsible and confronting the issue when memberships were a fraction of the current numbers,[356] EISs ignored the problem.[357] Moreover, the tremendous growth of the on-line community,[358] combined with both the ability to send out material to unlimited amounts of people and receive child pornography completely unsolicited,[359] has greatly expanded the child pornography market.[360] Additionally, there has been a renewed commercial interest in child pornography since it appeared on-line.[361] As the elimination of all commercial interests is a predominate motivation behind the Child Protection Act,[362] this new com-

---

354. *Easy access, on-line pornography draws fire*, BALTIMORE EVE. SUN, Jul. 25, 1995, at 1A (Barry Crimmins, an investigative journalist who went undercover on-line as a 12-year-old boy, testified to a Senate Committee that pornography is 'pervasive' on on-line services, and that "when you go [on-line] as a child, the pedophiles come after you like they're flies and you're rancid meat.").

355. *See supra* note 18 and accompanying text (showing awareness of the presence of child pornography on EISs since 1987).

356. *See* United States v. Maxwell, 42 M.J. 568, 573 (A.F. Ct. Crim. App. 1995) (finding that America Online had 215,000 members in 1991 when Maxwell was charged with distributing child pornography over the service).

357. *See supra* notes 18-19 (demonstrating how EISs claimed ignorance of child pornography on their systems until 1995, even though the media was reporting it since 1987).

358. *See* Evenson, *supra* note 94 (Dec. 1995 estimate that 10 million U.S. households are on-line, compared to 4 million in 1994). Additionally, more than 50 million pieces of electronic mail get sent daily. *Id.*

359. *See supra* note 302 (members of an EIS receive unsolicited child pornography).

360. *See* Smith & Mosely, *supra* note 302 (2,000 people accessed photographs including children engaged in sex acts with animals); *Paper Says*, *supra* note 20 (FBI identified more than 3,000 people nationally who have viewed child pornography and claimed that "thousands" of subscribers to an EIS have been viewing the pictures).

361. *See Fordham Law Symposium*, *supra* note 6, at 299.

> If a pornographer can get a thousand people out of the many millions who use computers to sign up for a child pornography bulletin board system, charge them $85 a year, with unlimited downloading privileges, he can make fairly painless $85,000. What is the overhead? Maybe $3,000 to $4,000 . . . . This symbiotic relationship keeps the child pornographers in business.

Id. at 298-99 (comments of J. Robert Flores, Esq.).

362. *See* United States v. Langford, 688 F.2d 1088 (7th Cir.), *cert. denied*, 461 U.S. 959 (1982) (18 U.S.C. § 2252 was intended "to eradicate the entire commercial chain involved in the production, distribution and sale of child pornography").

mercial interest should provide a further incentive to prosecute.

This is not to say that the need for technological advances in communications is not also a compelling social interest. Recently, corporate spending on information technology in the United States reached $200 billion,[363] and information services and products accounted for between ten and twelve percent of the United State's Gross Domestic Product.[364] The Supreme Court uses "strict scrutiny" when reviewing any infringing measure directed at communication, requiring a compelling interest narrowly tailored before the Court will even consider regulating speech presumed to be protected.[365] Communication services, however, are not unapproachable by the law, and the Court has clearly stated that one of the allowable infringements on the free flow of communication is the safety of minors.[366]

Holding EISs liable for child pornography will obtain a result consistent both with society's demands,[367] and with the Justice Department's that it "[is] not going to let new technology make victims of innocent children."[368] Congress's inability to realize how severely minors are being harmed by this new technology[369] allows EISs to continue to ignore the fact that child pornography exists within their "communities."[370] While the Communications Decency Act may help prevent pedophiles from engaging minors

---

363. Ralph King Jr., *Magic Formula*, WALL ST. J., Nov. 14, 1994, at R18.

364. Cate, *supra* note 189, at 4.

365. Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989).

366. *Id.*

367. In a Time/CNN poll, 48 percent of people polled were against FCC regulation of all sexual content on computer networks. *See* Philip Elmer-Dewitt, *Superhighway*, TIME, July 3, 1995, at 38. However, when pollers were asked if children who use computers need to be shielded from pornographic material, the result was nearly unanimous in favor of such regulation. *Pornography via Computers? Make it Illegal, Callers Say*, ORLANDO SENTINEL, Aug. 15, 1995, at B1.

368. Josar, *supra* note 254 (comments of James Wilder, a Justice Department spokesman).

369. The original Communications Decency Act proposed making on-line providers liable directly. *See* Sandberg & Simpson, *supra* note 12. However, Senator Exon, the bill's architect, was "persuaded" to target only end-users. *Id.*

370. *See supra* notes 16-20 and accompanying text.

in a sexual dialogue,[371] it provides little incentive for EISs to change because EISs are specifically immune from prosecution under this act.[372] This legislation has produced no extra protection for minors: the day after the CDA was signed the same pornography was still available on-line,[373] and CompuServe reinstated the 200 sex based EBBs it had previously eliminated.[374]

D. *As Currently Structured, EISs Can and Should be Held Liable for Child Pornography Distributed and Possessed Within Their Systems Regardless of What Form of Communication They Emulate*

This Note demonstrates how EISs can and should be prosecuted for allowing their systems to promote child pornography despite the constitutional status other modes of communication have received from the Supreme Court.[375] Prosecution is attainable because the Supreme Court has consistently allowed constitutional infringements on communication when it is clear that minors are being harmed. If EISs are found by a court to be analogous to print publishers, EISs can be held liable for child pornography either as a primary[376] or secondary[377] publisher. Such liability stems from the fact that EISs, due to their monitoring and editing abilities,[378] know or should know the contents of the material people publish on their services. If considered analogous to broadcasters, EISs will face rigorous scrutiny by the Court which has been adamant about ensuring that minors remain protected from broadcasted obscene messages.[379] Likewise, EISs are not able to hide behind the safety net that courts have granted cable television,[380] because EISs

---

371. *See supra* note 265.

372. *See supra* notes 260-65 (discussing the Communications Decency Act).

373. *See* Elizabeth Weise, *On-line Porn Available Despite New Statute*, STAR-LEDGER, Feb. 10, 1996, at 3.

374. *See* Peter H. Lewis, *CompuServe to Leave Internet Censorship to Individual User*, L.A. DAILY NEWS, Feb. 14, 1996, at N10.

375. *See supra* part III.

376. *See supra* part III.A.1.

377. *See supra* part III.A.2.

378. *See supra* notes 266-78 and accompanying text.

379. *See supra* part III.A.3.

380. *See supra* note 310 and accompanying text (demonstrating the favorable treat-

have not properly structured their systems to provide adequate security for minors.[381] Finally, if considered analogous to dial-a-porn telephone services, EISs again face the problem of inadequate security measures for minors who access the service.[382] Thus, prosecution is attainable and necessary because EISs continue to ignore the problems inherent within their systems that allow the victimization of minors.

CONCLUSION

This Note does not dispute that individuals should be the primary focus of prosecutions for possessing and/or distributing child pornography. Nor does it dispute the notion that protecting speech and encouraging technological advances are paramount societal interests. It does argue, however, that corporations, in the form of EISs, who profit at the expense of thousands of minors should be held accountable for their actions.

EISs have inadvertently created a world where minors are victimized by child pornography in their own homes. Knowledge of this victimization has been occurring for numerous years, and yet the industry still refuses to make the appropriate changes necessary to ensure the protection of the minors who use the service. Thus, EISs must be held liable for child pornography on their systems; only then will EISs ensure a safe environment for all users.

---

ment cable television has received from the courts).

381. *See supra* part III.A.4.

382. *See supra* part III.A.5.