105TH CONGRESS
*2d Session*
HOUSE OF REPRESENTATIVES
REPORT
105–775

# CHILD ONLINE PROTECTION ACT

OCTOBER 5, 1998.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BLILEY, from the Committee on Commerce, submitted the following

# REPORT

[To accompany H.R. 3783]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, to whom was referred the bill (H.R. 3783) to amend section 223 of the Communications Act of 1934 to require persons who are engaged in the business of selling or transferring, by means of the World Wide Web, material that is harmful to minors to restrict access to such material by minors, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS



69–006

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

**SECTION 1. SHORT TITLE.**

This Act may be cited as the "Child Online Protection Act".

**SEC. 2. CONGRESSIONAL FINDINGS.**

The Congress finds that—

(1) while custody, care, and nurture of the child resides first with the parent, the widespread availability of the Internet presents opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control;

(2) the protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling governmental interest;

(3) to date, while the industry has developed innovative ways to help parents and educators restrict material that is harmful to minors through parental control protections and self-regulation, such efforts have not provided a national solution to the problem of minors accessing harmful material on the World Wide Web;

(4) a prohibition on the distribution of material harmful to minors, combined with legitimate defenses, is currently the most effective means by which to satisfy the compelling government interest; and

(5) notwithstanding the existence of protections that limit the distribution over the World Wide Web of material that is harmful to minors, parents, educators, and industry must continue efforts to protect children from dangers posed by the Internet.

**SEC. 3. REQUIREMENT TO RESTRICT ACCESS BY MINORS TO MATERIALS SOLD BY MEANS OF THE WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.**

Part I of title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended by adding at the end the following new section:

**"SEC. 231. RESTRICTION OF ACCESS BY MINORS TO MATERIALS SOLD BY MEANS OF WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.**

"(a) REQUIREMENT TO RESTRICT ACCESS.—

"(1) PROHIBITED CONDUCT.—Whoever, in interstate or foreign commerce, by means of the World Wide Web, knowingly makes any communication for commercial purposes that includes any material that is harmful to minors, without restricting access to such material by minors pursuant to subsection (c), shall be fined not more than $50,000, imprisoned not more than 6 months, or both.

"(2) INTENTIONAL VIOLATIONS.—In addition to the penalties under paragraph (1), whoever intentionally violates such paragraph shall be subject to a fine of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

"(3) CIVIL PENALTY.—In addition to the penalties under paragraphs (1) and (2), whoever violates paragraph (1) shall be subject to a civil penalty of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

"(b) INAPPLICABILITY OF CARRIERS AND OTHER SERVICE PROVIDERS.—For purposes of subsection (a), a person shall not be considered to make any communication for commercial purposes to the extent that such person is—

"(1) a telecommunications carrier engaged in the provision of a telecommunications service;

"(2) a person engaged in the business of providing an Internet access service;

"(3) a person engaged in the business of providing an Internet information location tool; or

"(4) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication made by another person, without selection or alteration of the content of the communication, except that such person's deletion of a particular communication or material made by another person in a manner consistent with subsection (c) or section 230 shall not constitute such selection or alteration of the content of the communication.

"(c) AFFIRMATIVE DEFENSE.—

"(1) DEFENSE.—It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors—

"(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; or

"(B) by any other reasonable measures that are feasible under available technology.

"(2) PROTECTION FOR USE OF DEFENSES.—No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this subsection or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.

"(d) PRIVACY PROTECTION REQUIREMENTS.—

"(1) DISCLOSURE OF INFORMATION LIMITED.—A person making a communication described in subsection (a)—

"(A) shall not disclose any information collected for the purposes of restricting access to such communications to individuals 17 years of age or older without the prior written or electronic consent of—

"(i) the individual concerned, if the individual is an adult; or

"(ii) the individual's parent or guardian, if the individual is under 17 years of age; and

"(B) shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the person making such communication and the recipient of such communication.

"(2) EXCEPTIONS.—A person making a communication described in subsection (a) may disclose such information if the disclosure is—

"(A) necessary to make the communication or conduct a legitimate business activity related to making the communication; or

"(B) made pursuant to a court order authorizing such disclosure.

"(e) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

"(1) BY MEANS OF THE WORLD WIDE WEB.—The term 'by means of the World Wide Web' means by placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol.

"(2) COMMERCIAL PURPOSES; ENGAGED IN THE BUSINESS.—

"(A) COMMERCIAL PURPOSES.—A person shall be considered to make a communication for commercial purposes only if such person is engaged in the business of making such communications.

"(B) ENGAGED IN THE BUSINESS.—The term 'engaged in the business' means that the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income). A person may be considered to be engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to minors, only if the person knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web.

"(3) INTERNET.—The term 'Internet' means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit information.

"(4) INTERNET ACCESS SERVICE.—The term 'Internet access service' means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.

"(5) INTERNET INFORMATION LOCATION TOOL.—The term 'Internet information location tool' means a service that refers or links users to an online location on the World Wide Web. Such term includes directories, indices, references, pointers, and hypertext links.

"(6) MATERIAL THAT IS HARMFUL TO MINORS.—The term 'material that is harmful to minors' means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that—

"(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, that such material is designed to appeal to or panders to the prurient interest;

"(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or female breast; and

"(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

"(7) MINOR.—The term 'minor' means any person under 17 years of age.".

**SEC. 4. NOTICE REQUIREMENT.**

(a) NOTICE.—Section 230 of the Communications Act of 1934 (47 U.S.C. 230) is amended—

(1) by redesignating subsections (d) and (e) as subsections (e) and (f), respectively;

(2) by inserting after subsection (c) the following new subsection:

"(d) OBLIGATIONS OF INTERACTIVE COMPUTER SERVICE.—A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.".

(b) CONFORMING AMENDMENT.—Section 223(h)(2) of the Communications Act of 1934 (47 U.S.C. 223(h)(2)) is amended by striking "230(e)(2)" and inserting "230(f)(2)".

**SEC. 5. STUDY BY COMMISSION ON ONLINE CHILD PROTECTION.**

(a) ESTABLISHMENT.—There is hereby established a temporary Commission to be known as the Commission on Online Child Protection (in this section referred to as the "Commission") for the purpose of conducting a study under this section regarding methods to help reduce access by minors to material that is harmful to minors on the Internet.

(b) MEMBERSHIP.—The Commission shall be composed of 17 members, as follows:

(1) INDUSTRY MEMBERS.—The Commission shall include—

(A) 2 members who are engaged in the business of providing Internet filtering or blocking services or software;

(B) 2 members who are engaged in the business of providing Internet access services;

(C) 2 members who are engaged in the business of providing labeling or ratings services;

(D) 2 members who are engaged in the business of providing Internet portal or search services;

(E) 2 members who are engaged in the business of providing domain name registration services; and

(F) 4 members who are engaged in the business of making content available over the Internet.

Of the members of the Commission by reason of each subparagraph of this paragraph, an equal number shall be appointed by the Speaker of the House of Representatives and by the Majority Leader of the Senate.

(2) EX OFFICIO MEMBERS.—The Commission shall include the following officials:

(A) The Assistant Secretary (or the Assistant Secretary's designee).

(B) The Attorney General (or the Attorney General's designee).

(C) The Chairman of the Federal Trade Commission (or the Chairman's designee).

(c) STUDY.—

(1) IN GENERAL.—The duty of the Commission shall be to conduct a study (and submit a report under subsection (d) on the study) to identify technological or other methods, if any, to help reduce access by minors to material that is harmful to minors on the Internet that—

(A) the Commission determines meet the requirements for use as affirmative defenses for purposes of section 231(c) of the Communications Act of 1934 (as added by this Act); or

(B) may be used in any other manner to help reduce such access.

Any methods so identified shall be used as the basis for making legislative recommendations to the Congress under subsection (d)(3).

(2) SPECIFIC METHODS.—In carrying out the study, the Commission shall identify and analyze various technological tools and methods for protecting minors from material that is harmful to minors, which shall include—

(A) a common resource for parents to use to help protect minors (such as a "one-click-away" resource);

(B) filtering or blocking software or services;

(C) labeling or rating systems;

(D) age verification systems;

(E) the establishment of a domain name for posting of any material that is harmful to minors; and

(F) any other existing or proposed technologies or methods for reducing access by minors to such material.

(3) ANALYSIS.—In analyzing technologies and other methods identified pursuant to paragraph (2), the Commission shall examine—

(A) the cost of such technologies and methods;

(B) the effects of such technologies and methods on law enforcement entities;

(C) the effects of such technologies and methods on privacy;

(D) the extent to which material that is harmful to minors is globally distributed and the effect of such technologies and methods on such distribution; and

(E) the accessibility of such technologies and methods to parents.

(d) REPORT.—Not later than 1 year after the enactment of this Act, the Commission shall submit a report to the Congress containing the results of the study under this section, which shall include—

(1) a description of the technologies and methods identified by the study and the results of the analysis of each such technology and method;

(2) the conclusions and recommendations of the Commission regarding each such technology or method;

(3) recommendations for legislative or administrative actions to implement the conclusions of the committee; and

(4) a description of the technologies or methods identified by the study that may be used as affirmative defenses for purposes of section 231(c) of the Communications Act of 1934 (as added by this Act).

(e) STAFF AND RESOURCES.—The Assistant Secretary for Communication and Information of the Department of Commerce shall provide to the Commission such staff and resources as the Assistant Secretary determines necessary for the Commission to perform its duty efficiently and in accordance with this section.

(f) TERMINATION.—The Commission shall terminate 30 days after the submission of the report under subsection (d).

(g) INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Commission.

## PURPOSE AND SUMMARY

The purpose of H.R. 3783 is to amend the Communications Act of 1934 by prohibiting the sale of pornographic materials on the World Wide Web (or the Web) to minors. H.R. 3783 has been carefully drafted to respond to the Supreme Court's decision in *Reno* v. *ACLU,* 117 S.Ct. 2329 (1997) and the Committee believes that the bill strikes the appropriate balance between preserving the First Amendment rights of adults and protecting children from harmful material on the World Wide Web. Notwithstanding H.R. 3783, the Committee recognizes that parents, educators, and industry must continue to play a role and find ways to help protect children from being exposed to harmful material that can be found on the Internet.

H.R. 3783 prohibits a person from knowingly making, by means of the World Wide Web, any communication for commercial purposes that is harmful to minors, unless such person makes a good faith effort to restrict access by minors. A person violating H.R. 3783 could be subject to criminal and civil penalties. The bill explicitly states that only entities engaged in the commercial busi-

ness of making communications that contain material harmful to minors could be held liable under the bill. These entities include a person who knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web. The general prohibition would not be applicable to entities that merely access, transport, or link the communications of another person.

The bill provides examples of ways a business would be in compliance with the law by identifying "affirmative defenses" to prosecution. Such examples include the use of a credit card, debit account, adult access code, or adult personal identification number. There is also a general affirmative defense for a business that makes a good faith effort to restrict a minor's access to material harmful to minors. In addition, the bill requires providers of interactive computer services to notify customers, at the time the customer signs up for service, that parental control protections, such as computer hardware, software, and filtering services, are commercially available that may assist the customer in limiting access to material that is harmful to minors. Finally, the bill establishes a Commission on Online Child Protection that is required to study technological and other methods to help reduce access by minors to material that is harmful to minors on the Internet. The Commission is required to submit its findings within one year from the date of enactment of the bill.

H.R. 3783 presents no ban on the distribution or display of material harmful to minors, nor does it impose any unreasonable burdens on adults. Rather, it simply requires the sellers of such material to recast their messages so that they are not readily available to children. Thus, the Committee believes that H.R. 3783 is currently the most effective, yet least restrictive, way to reduce a minor's access to harmful material.

## BACKGROUND AND NEED FOR LEGISLATION

### I. BACKGROUND

#### *A. Electronic commerce*

For over two hundred years, the Congress of the United States has sought to protect and facilitate the development of interstate and foreign commerce. From regulating matters regarding ports of entry into the United States (18th century) to the creation of a national railroad system (19th century) to establishing communications policy (20th century), Congress' duty remains constant: to uphold the responsibilities delegated to the Congress by the people with respect to the regulation of commerce among the several States.

As the Nation approaches the next millennium, Congress must stand ready to "keep pace with the progress of the country, and adapt [itself] to the new developments of time and circumstances." *Pensacola Tel. Co.* v. *Western Union Tel. Co.,* 96 U.S. 1, 9 (1878)). One such development is the explosive growth of electronic commerce. In general, electronic commerce is the term used to describe the buying, selling, or transfer of goods and services over electromagnetic transmission media. The media could include wireline and wireless networks, both of which have been previously held to

be interstate in nature. While electronic commerce is becoming a more common way to conduct business, many industries have been engaged in it for years. Bank-wire transactions, the use of automatic-teller machines, credit card verifications, and the purchase of goods or services over the telephone all constitute a type of electronic commerce.

The growth of electronic commerce is having a profound impact on the nation's economy. Over the past decade, the information technology sector of our economy has grown rapidly and is seen by many as playing a leading role in the current economic expansion. According to The Emerging Digital Economy, a recent Department of Commerce report on electronic commerce, the information technology sector now constitutes 8.2 percent of the nation's GDP, up from 4.5 percent in 1985. At the end of 1997, approximately 7.4 million Americans were employed in this field. Many are predicting even stronger growth in the future. Estimates of the total value of economic activity conducted electronically in 2002 range from $200 billion to more than $500 billion, compared to just $2.6 billion in 1996. While other mediums have been used to enable electronic commerce in the past, the growth and use of the Internet will likely be the basis for additional growth in the future.

*B. The Internet*

The Internet was largely the domain of academic researchers from its creation in the late 1960s until the start of the 1990s. In 1991, the National Science Foundation lifted its restriction on commercial activity on the Internet. Also in 1991, the World Wide Web was created. In 1993, the first commercially available Web browser was introduced, thus allowing millions of consumers and businesses an easy method of navigating on the Internet. These events, combined with the widespread availability of inexpensive yet powerful personal computers (that allowed computer users to access graphics, audio, and video on the World Wide Web in addition to text), led to the dramatic growth of the Internet and online services.

*C. Adult entertainment industry*

One such market that has flourished on the Internet is sale of pornography. According to Wired Magazine, there are approximately 28,000 adult Web sites promoting pornography on the Internet and these sites generate close to $925 million in annual revenues. While legitimate U.S. businesses should remain free from unnecessary government regulation, the adult entertainment industry has traditionally been subject to restrictions because of the danger posed by pornographic material to children. Parents, educators, and civic groups agree that exposure to pornography shapes a child's perspective on sexual activity in a manner that may be inconsistent with the goal of healthy sexual development. For example, some pornography consists of photographs, videos, magazines, and games that are violent, abusive, and degrading, and certainly counterproductive to learning about sexual activity in an appropriate educational or home setting.

Publishers of pornography, like all publishers in the United States, are protected by the First Amendment which provides that

"Congress shall make no law . . . abridging the freedom of speech." U.S. Const., Amdt. 1. The amendment prohibits government restrictions on "the freedom of speech," but not all speech such as obscenity or child pornography. Thus, while the Internet is the medium of choice for electronic commerce, it is also the medium of choice that stimulates a marketplace of ideas generated from Web pages, newsgroups, listservs, chat rooms, e-mail, and bulletin board services, all of which have the ability to reach more Americans on more topics, including pornography, than we have seen from traditional mediums of communications in the past.

*D. The Communications Decency Act of 1996*

As part of the Telecommunications Act of 1996 (the Telecommunications Act), Congress enacted two statutory provisions designed to protect minors from "indecent" and "patently offensive" communications on the Internet. These statutory provisions were included in Title V of the Telecommunications Act, known as the Communications Decency Act of 1996 (the CDA) and were codified as part of the Communications Act of 1934, as amended (the Act). 47 U.S.C. §223. The first provision, Section 223(a) of the Act, prohibited the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. The second provision, Section 223(d) of the Act, prohibited the sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age.

The breadth of these provisions were qualified by two affirmative defenses. One covers those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications. Section 223(e)(5)(A). The other covers those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code. Section 223(e)(5)(B).

Immediately after the Telecommunications Act was signed into law, two lawsuits were filed challenging the constitutionality of Sections 223(a)(1) and 223(d). The two cases were consolidated and the Federal Court for the Eastern District of Pennsylvania held that part of Section 223(a)(1) was unconstitutional with respect to "indecent" communications (but not obscenity) and that all of Section 223(d) was unconstitutional. *ACLU* v. *Reno,* 929 F.Supp. 824 (E.D.Pa. 1996), aff'd, *Reno*, 117 S.Ct. at 2329. The government appealed the case to the Supreme Court and in *Reno*, the Court affirmed the lower court's ruling. 117 S.Ct. at 2329. The Court concluded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech and that the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive. Id. at 2346.

Specifically, the Court noted the lack of legislative hearings, the use of different linguistic forms for "indecent," the broad definition of indecent, the heightened level of review because of the criminal nature of the statute, the broad applicability of the statute to commercial and noncommercial speech, the failure of the government to consider less restrictive alternatives, and unreliable affirmative defenses as fundamental problems with the CDA. Although the Court stated that the "CDA's burden on protected speech cannot be

justified," id. at 2346, it went on to say that such problems "could be avoided by a more carefully drafted statute." Id.

*E. Section 230 of the Communications Act*

In addition to Section 223, as part of the Telecommunications Act, Congress added Section 230 to the Communications Act. 47 U.S.C. §230. Section 230 states that providers and users of interactive computer services shall not be treated as publishers of any information provided by another information content provider. Section 230 also provides liability protections for providers and users of interactive computer services by permitting them to remove or restrict access to inappropriate materials.

## II. THE CONTINUED NEED FOR LEGISLATION

*A. The growth of the Internet*

Over the past several years, the popularity and use of the Internet has grown dramatically. Since January 1996 (one month before the CDA was enacted), the number of host computers (i.e., machines physically connected to the Internet) has more than tripled from approximately 9.4 million hosts to more than 29.6 million hosts. The number of users has also increased. According to a recent study by Nielsen Media Research, approximately 70.2 million adults use the Internet in the United States. This figure represents an increase from approximately 52 million adults using the Internet a mere nine months ago. With respect to children using the Internet, the Chairman of the Federal Trade Commission recently stated that the population of minors on the Internet has almost doubled to 16 million from a year ago. Testimony of Robert Pitosfsky, Chairman, Federal Trade Commission, before the Senate Committee on Commerce, Science, and Transportation (September 22, 1998).

In addition, a national effort is underway to connect every school and library to the Internet. See In the Matter of Federal-State Joint Board on Universal Service, Report and Order, CC Docket 96–45, FCC 97–157 (May 8, 1997). According to a 1997 U.S. Department of Education survey, 78 percent of all public schools have access to the Internet. Of these schools, approximately 27 percent of the classrooms that are used for instructional purposes have access to the Internet, with at least 43 percent of the schools that have Internet access in 5 or more instructional classrooms. Furthermore, the Department of Education predicts that 95 percent of all schools will have access to the Internet by the year 2000. Internet Access in Public Schools, National Center for Education Statistics, U.S. Department of Education (Feb. 1998).

While clearly the Internet is not yet as "invasive" as broadcasting, its popularity and growth because of electronic commerce and expansive Federal subsidy programs make it widely accessible for minors. The Committee recognizes that parents are responsible for the custody, care, and nurture of the child, but the widespread availability of the Internet presents opportunities for minors to access information on the Internet that can frustrate parental supervision and control. Moreover, because of sophisticated, yet easy to use navigating software, minors who can read and type are capable

of conducting Web searches as easily as operating a television remote. While a four-year old may not be as capable as a thirteen year old, given the right tools (e.g., a child trackball and browser software) each has the ability to "surf" the Net and will likely be exposed to harmful material.

*B. The availability of material harmful to minors*

As the Internet has grown, so has the availability of on-line pornography. In 1996, there were estimates that almost 50 percent of the content available on the Web was unsuitable for children. "Half of 'Net Content Said Unsuitable for Children," Reuters Financial Service (January 10, 1996). Two years later, as of 1998, the estimates have increased to almost 70 percent of the traffic on the Web is adult-oriented material. "The Net's Dirty Little Secret: Sex Sells," Upside Publishing Company (April 1998). Sexually explicit material on the Internet includes text, pictures, and communications via chat rooms. Purveyors of such material generally display many unrestricted and sexually explicit images to advertise and entice the consumer into engaging in a commercial transaction. Currently, minors can move from Web page to Web page, viewing and downloading this material without restriction. Once posted on the Internet, sexually explicit material has entered all communities.

While much of the sexually explicit material is accessed deliberately, minors often stumble upon it by mistake. There are numerous hard-core pornography sites on the Internet using "copycat URLs" to take advantage of innocent mistakes to bring traffic to their graphic sexual images. First, children searching the Internet for the official Web site of the White House can be confronted by hard-core pornography by mistyping "www.whitehouse.com" rather than "www.whitehouse.gov." Second, children who mistype "www.betscape.com" instead of "www.netscape.com" or "www.sharware.com" instead of "www.shareware.com" will be confronted with live sex shows and other X-rated pictures. Finally, brand names are often misused in ways that direct people to sexually explicit material. Testimony of Enough is Enough, Hearing on Legislative Proposals to Protect Children from Inappropriate Materials on the Internet, House Commerce Committee (September 11, 1998) (Committee Hearing). Another set of examples involves children using Internet search engines to look up innocent information. Searches for toys, dollhouses, girls, boys, pets, teen, cheerleader, actress, gang, beanie babies, bambi, and doggy will lead to material harmful to minors. Testimony of Enough is Enough, Committee Hearing; Testimony of National Law Center for Children and Families, Committee Hearing.

Moreover, even though some Web sites contain warnings that the material on that Web site is adult-oriented, most provide no warnings, or if they do provide a warning, there is sexually explicit material on the same page as the warning. Consequently, the odds are no longer slim that a user will enter a sexually explicit site by accident. Contra 929 F. Supp. at 16.

*C. Exposure to sexually explicit material harms children*

A child's sexual development occurs gradually throughout childhood. Exposure to pornography shapes children's sexual perspectives by providing them with information on sexual activity intended for adults. The type of information provided by pornography, however, does not provide children with a normal sexual perspective. Unlike learning provided in an educational or home setting, exposure to pornography is counterproductive to the goal of healthy and appropriate sexual development in children. It teaches without supervision or guidance, inundating children's minds with graphic messages about their bodies, their own sexuality, and those of adults and children around them. Dr. Gary Brooks, Assistant Chief of Psychology Services, Department of Veterans Affairs, The Centerfold Syndrome (1996).

Testimony before the Committee also highlighted the dangers of exposing minors to harmful material. One witness testified that pornography produces "permission-giving beliefs" for sexual pathology and sexual violence and that pornography produces distortions that change an individual's belief system. As a result, children exposed to pornography can become victims or victimizers, encouraged by the strong sexual images contained in pornography found on the World Wide Web. Testimony of Dr. Mary Anne Layden, Committee Hearing. Similarly, testimony has been inserted into the record describing the body of research indicating that pornography has significant impact on attitudes and values, and that such impact is clearly harmful to minors. Testimony of Enough is Enough, Committee Hearing.

## III. CONSTITUTIONALITY OF H.R. 3783

*A. Congress has a compelling interest in protecting children*

The Supreme Court's precedent is clear in establishing the government's compelling interest in protecting children from exposure to sexually explicit material. The Court has repeatedly articulated such an interest in *Ginsberg* v. *New York,* 390 U.S. 629, 636–43 (1968); *FCC* v. *Pacifica Foundation,* 438 U.S. 726, 748–50 (1978); *New York* v. *Ferber,* 458 U.S. 747, 757 (1982); *Sable Communications of Cal.* v. *FCC,* 492 U.S. 115, 126–128 (1989); *Denver Area Ed. Tel. Consortium* v. *FCC,* 116 S.Ct. 2374, 2391 (1996); and 117 S.Ct. at 2346, 2348. As stated by the Court in *Ferber:* "It is evident beyond the need for elaboration that the State's interest in safeguarding the physical and psychological well-being of a 'minor' is 'compelling'." 458 U.S. at 757. "This interest extends to shielding minors from the influence of literature that is not obscene by adult standards." 492 U.S. at 126. Whether the restrictions have required pornography to be sold behind the counter at a drug store, on blinder racks at a convenient store, in a shrink wrap at a news stand, or broadcast between certain hours of the night, the restrictions have sought to shield children from exposure to material that could distort their views of sexuality. The purpose of H.R. 3783 is to extend those protections in cyberspace by restricting the sale of material harmful to minors over the World Wide Web.

Though the primary responsibility for protecting the welfare of children resides with the parent, the parent deserves the support

of the law. This principle is of particular importance as it relates to shielding children from exposure to sexually explicit material over the Web, where they may be exposed to such material outside the home, at a friend's house, at the local library or school. "While the supervision of children's reading may be best left to their parents, the knowledge that parental control or guidance cannot always be provided and society's transcendent interest in protecting the welfare of children justify reasonable regulation of the sale of material to them." *People* v. *Kahan,* 15 N.Y.2d 311, 312, 206 N.E.2d 333, 334 (1965), cited in *Ginsberg,* 390 U.S. at 640.

*B. H.R. 3783 is narrowly tailored*

The Committee recognizes the First Amendment rights of adults and carefully drafted H.R. 3783 not to impose an unnecessary burden on those rights. For example, the prohibition on making communications that are harmful to minors applies only to material posted on the World Wide Web. The World Wide Web is one type of remote information retrieval system, among many. H.R. 3783 does not apply to content distributed through other aspects of the Internet such as one-to-one messaging (e-mail), one-to-many messaging (list-serv), distributed message databases (USENET newsgroups); real time communications (Internet relay chat); real time remote utilization (telnet) or remote information retrieval other than the World Wide Web (ftp and gopher).

H.R. 3783 is also limited to the commercial distribution of material harmful to minors and does not affect noncommercial speech. In addition, the bill defines harmful to minors in a manner that parallels many State statutes that have been upheld by the Supreme Court and only restricts access for minors 16 years old or younger. Finally, H.R. 3783 provides maximum flexibility for entities engaged in the business of selling pornography by providing them with a host of good faith defenses from prosecution if they adopt reasonable measures to restrict a minor's access to material that is harmful.

*C. H.R. 3783 is consistent with Reno v. ACLU*

H.R. 3783 addresses the specific concerns raised by the Supreme Court in *Reno* v. *ACLU.* In ruling against the indecency portions of the CDA, the Court stated that "the government interest in protecting children from harmful materials . . . does not justify an unnecessary broad suppression of speech addressed to adults." 117 S.Ct. at 2346. H.R. 3783 was crafted in a way to respond to the Supreme Court's concerns and thus should not result in an unnecessary broad suppression of speech.

*1. The definition of harmful to minors*

The principal concern of the Court with the CDA was that the "indecency" and "patently offensive" content standards used in the challenged sections of the CDA were overly vague as applied to the Internet. The Court also noted that the CDA's definition of "indecency" did not conform with Ginsberg because it lacked an element ensuring that material of serious literary, artistic, political, or scientific value would not be swept up in the statute. 117 S.Ct. at 2345.

H.R. 3783 conforms to the standards identified in *Ginsberg,* as modified by the Supreme Court in *Miller* v. *California,* 413 U.S. 15 (1973). H.R. 3783 modifies the "patently offensive" language by explicitly describing the material that is harmful to minors. In particular, it includes material that displays an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals or female breast. H.R. 3783 mirrors many of the State laws already in place, which have been upheld by the Supreme Court. The new harmful to minors definition also includes the requirement that the material is harmful to minors only if "taken as whole, lacks serious literary, artistic, political, or scientific value for minors."

The "harmful to minors" standard is also familiar to the Federal courts, even though that standard is not used in present Federal statutes, since the Federal district courts and Federal appellate courts have routinely heard challenges to State "harmful to minors" display laws and upheld those laws on a regular basis over the years. See, e.g., *Crawford* v. *Lungren,* 96 F.3d 380 (9th Cir. 1996), cert. denied, 117 S. Ct. 1249 (1997); *American Booksellers* v. *Webb,* 919 F.2d 1493 (11th Cir. 1990); *American Booksellers Ass'n* v. *Com. of Va,* 882 F.2d 125 (4th Cir. 1989); *Upper Midwest Booksellers* v. *City of Minneapolis,* 780 F.2d 1389 (8th Cir. 1985); *M.S. News Co.* v. *Casado,* 721 F.2d 1281 (10th Cir. 1983).

*2. Scope limited to commercial transactions*

The Court in *Reno* also criticized the CDA for its breadth with respect to commercial and non-commercial transactions. The Court stated that the "[b]readth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in *Ginsberg* and *Pacifica,* the scope of the CDA is not limited to commercial speech or commercial entities. Its open-ended prohibitions embrace all non-profit entities and individuals posting indecent messages or displaying them in the presence of minors." 117 S.Ct. at 2347. By contrast, H.R. 3783 applies only to commercial transactions involving the display of material that is harmful to minors over the World Wide Web. It does not prohibit non-commercial activities over the Web, or over the Internet for that matter, and thus the concerns raised by the Supreme Court are no longer applicable. The Committee notes that a large quantity of information will still be available to minors who are capable of accessing these non-commercial sites on the Web and on the Internet. As a result, as part of Section 5 of H.R. 3783, the Committee anticipates that the industry will suggest legislative proposals on how to address the difficult issue of restricting a minor's access to inappropriate material with respect to these aspects of the Internet.

*3. Age verification systems are technologically and economically feasible*

The Court in *Reno* also was concerned that age verification systems under the CDA were not technologically feasible for certain non-commercial, private, and on-line services such as e-mail and chat rooms. 117 S.Ct. at 2347. Or, even where technological feasibility was acknowledged, the Court was concerned that such measures would be cost prohibitive to some non-commercial content

providers. Id. The Court recognized, however, with regard to restricting access by minors by requiring use of a verified credit card or adult verification, that "[s]uch verification is not only technologically available but is used by commercial providers of sexually explicit material. These providers, therefore, would be protected by the defense." 117 S.Ct. at 2349.

H.R. 3783 provides a legitimate defense for commercial purveyors of pornography. As discussed above, H.R. 3783 does not apply to noncommercial sites, nor does it apply to those aspects of the Internet outside the World Wide Web. Thus, the Committee agrees with the Supreme Court that commercial distributors of material harmful to minors will be protected by these defenses if they make a good faith effort to restrict a minor's access to harmful material.

Unlike other restrictive approaches, age verification systems stop a minor's access at the source of the communication and require no independent judgments to be made about the content of the material. The Committee notes that the FCC's dial-a-porn regulations, which were upheld in *Dial Information Services Corp.* v. *Thornburgh,* 938 F.2d 1535 (2d Cir. 1991), cert. denied, 502 U.S. 1072 (1992), and cited with approval in *Sable,* 429 U.S. 115 (1989), provided a defense to prosecution by allowing a provider, before the transmission of a message, to restrict customer access by requiring either payment by credit card or authorization by access or identification code. In *Sable*, the Court found that such commercial restrictions would be effective in excluding most juveniles, stating: "the FCC's technological approach to restricting dial-a-porn messages to adults who seek them would be extremely effective, and only a few of the most enterprising and disobedient young people would manage to secure access to such messages." 429 U.S. at 130.

In fact, the use of the age verification means prescribed under H.R. 3783 are standard practice among some commercial distributors of pornography on the Web. Testimony before the Committee revealed that adult verification services are effective and can be used successfully to screen minors from adult material. Testimony of Laith Paul Alsarraf, Cybernet Ventures, Committee Hearing. One such service is sold by Cybernet Ventures, an industry leader in age verification systems. This service utilizes age verification software that contains a script that is embedded into a Web page. The script is placed at the entrance of a website that may contain material that is harmful to minors thus preventing further access or exposure of the website's content by requiring a personal identification number, which is only available to adults. If a consumer does not have a personal identification number (PIN), a link is provided for them to obtain one from the age verification system associated with that site. Consumers may obtain a PIN instantly by submitting an application to an age verification system. The credit card and other information submitted by a consumer are verified by a proprietary age verification system to determine validity. If the information is deemed to be valid, a working adult PIN is issued. The process of verifying the information submitted generally takes less than one minute and often only 5 to 10 seconds. Consumers may also apply for a PIN by fax. Id. Testimony received by the Committee shows that there are at least 25 organizations assigning adult PINs and age verification services today. Testi-

mony of National Law Center for Children and Family, Committee Hearing (Tab K).

It is not only economically feasible for commercial content providers to comply with the bill, but profitable for them to do so. Adult verification systems generally require the user to pay for entrance to a site, although users have many ways to subscribe. Given that the scope of the bill is limited to commercial activity, and that the age verification system procedures prescribed under the bill represent standard procedures for conducting commercial activity on pornographic Web sites, the effect of the bill is simply to reorder the process in such a way as to require age verification before pornography is made available, essentially requiring the commercial pornographer to put sexually explicit images "behind the counter." The commercial pornographer is not otherwise restricted in his trade.

*4. Parents maintain control and minor is defined as those under 17*

In *Reno*, the Court expressed concern that the CDA wrested primary authority over the child from the parent if the statute is construed to make criminal a parental choice to make sexually explicit material available to a minor. 117 S.Ct. at 2348. H.R. 3783 contains no restriction on the discretion of the parent to purchase material for their children who are under the age of 17. In other words, a parent should not be liable under H.R. 3783 for merely sharing sexually explicit material with a minor. In addition, a minor is defined under the bill as persons under 17 years of age.

*5. Congress may regulate services offered over the Internet*

The Supreme Court also questioned Congress's role in regulating the Internet. The Court distinguished the Internet from other distribution mediums and stated that "[n]either before nor after the enactment of the CDA have the vast democratic fora of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry." 117 S.Ct. at 2343. Regulation of the Internet does, however, fall within the jurisdiction of the Congress under its Article I, Section 8, Clause 3 authority. Regardless of whether Congress exercises its authority under this section, the power of Congress to regulate in this area remains constant. During the 105th Congress, bills have moved through both House and Senate authorizing committees that address intellectual property rights over the Internet, whether the Internet should be taxed, and how communications over the Internet can be kept secure through the use of encryption technologies. Merely because the Internet itself has not been widely regulated because of its organizational structure and lack of dominance by a single entity should not imply that Congress cannot regulate certain activity conducted over the Internet, including regulating the display of harmful material to children on the Web. In fact, in *Reno*, the Supreme Court explicitly upheld Congress's ability to regulate obscene communications transmitted over the Internet. 117 S.Ct. at 2350.

*6. Legislative hearings highlight the problem*

In *Reno,* the Court noted that Congress did not hold legislative hearings on the CDA, nor did Congress reach any detailed findings addressing the problem of distributing indecent materials to minors over the Internet. 117 S.Ct. at 2348. On the other hand, both the House and Senate during the 105th Congress have extensively considered ways to reduce a minor's access to harmful material. The Senate Committee on Commerce, Science, and Transportation held a hearing to consider ways to protect children on the Internet on February 10, 1998, as did the House Committee on Commerce on September 11, 1998. The testimony received highlighted the problem of children getting easy access to pornography and the need for Congressional action to stop the widespread distribution of material harmful to minors.

*D. Alternatives considered by the committee*

In light of the *Reno* decision, the Committee has thoughtfully and thoroughly considered a number of ways to help protect children from being exposed to harmful material. Each proposal has merit, but the Committee concludes that H.R. 3783 is currently the most effective, yet least restrictive approach that should be taken given the current state of technology. The alternatives considered generally involve zoning and blocking techniques that rely on screening material after it has been posted on the Internet or retrieved by the end-user. The Committee believes that it is more effective to screen the material prior to it being sent or posted to minors, and that such a restriction imposes minimal burdens on adults. The Committee's general conclusion is supported by the Second Circuit in the *Dial Information Services* decision, where the appellate court stated:

> Common sense dictates that a presubscription requirement, like requirements for payment by credit card before a message is transmitted, for use of an authorized access or identification card before transmission . . . is more likely to achieve the goal sought than blocking after one or more occasions of access. It always is more effective to lock the barn door *before* the horse is stolen. 938 F.2d at 1542.

*1. Market-based solutions in general*

The industry has taken some significant steps to reduce a child's access to inappropriate material. There have been a number of online summits where policymakers and industry have discussed the "ugly" side of the Internet (e.g., kidsonline.org and americalinksup.org). Given the public policy sensitivities and potential demand for new products, the industry has developed new technologies that will help screen material for parents and educators. Some of the new products include Secure Learning (Spyglass, Inc.), NetWatch (Netscape Communications), Kids CyberHighway (AT&T), Cyber Patrol (The Learning Company), Disney's Internet Guide (The Walt Disney Company), Parental Controls (AOL), Net Nanny (Net Nanny Software, Inc.), X-Stop (Log On Data Corp.), Net Shepherd (Net Shepherd, Inc.) and Internet Explorer that incorporates a content advisor feature (Micro-

soft). In addition, there have been a number of educational trade shows that help inform educators about new products that enhance online safety for children. The Committee applauds the efforts of industry and is confident that demand for new products will continue to grow.

Unfortunately, industry-led efforts have not provided a national or uniform solution to the problem of children accessing harmful material. To quote the CEO of Net Nanny, one of the leading filtering software developers in the nation:

> Asking us to come up with one specific technological solution to the child safety issue is an extremely difficult proposition because we are not all in the same line of business. Some of us are filtering companies, others are ISPs and still others are search engine and browser companies. No single company has complete control over the access points to the Internet or is responsible for all the content that is produced online.

Letter from Gordon Ross, President and CEO, Net Nanny Software International, Inc. to The Honorable Joseph Lieberman and The Honorable Rick White, Members of Congress (August 4, 1998). H.R. 3783 provides a national solution and places the burden on the appropriate entity, the person selling the harmful material on the Web.

*2. Zoning techniques*

A number of proposals have been suggested that would identify or classify material harmful to minors. "Zoning" effectively places the seller of pornography in a red-light district in cyberspace. While each of these proposals are technically feasible today, mandating their use raises a host of additional issues that jeopardize their success and effectiveness. In addition, zoning techniques alone do not solve the problem of minor's accessing harmful material. Zoning techniques must be combined with a blocking or filtering service and may require the same type of age verification system specified in H.R. 3783.

a. Tagging

Tagging is a term used to describe information about a Web page. Some tags, known as "meta tags," do not affect how the Web page is displayed. Instead, meta tags provide information such as who created the page, how often the page is updated, what the page is about, and which keywords represent the page's content. Many search engines use tags when building their indices. As a result of tagging, websites may contain information that will alert users of adult content. In order for tagging to be used as an effective zoning technique, a requirement of tagging must be complied with by every provider of material harmful to minors. A requirement would then need to be imposed on the hardware and software community to develop products that would include capabilities to block "tagged" material. The Committee does not believe that level of regulation of the computer industry is warranted at this time, nor does it believe that it has the luxury of time to wait for indus-

try to develop uniform blocking standards while material harmful to minors is being distributed to children today.

b. Ratings

Voluntary ratings systems of Web sites have been somewhat successful. Several systems have already been developed and show promise in allowing parents to block objectionable material. The most popular rating systems rely on the Platform for Internet Content Selection (PICS) protocol. PICS is not a rating system, but rather a technical standard that can be used to enable the rating of sites. Two current rating systems (RSACi and SafeSurf) allow websites to self-rate using the PICS protocol. Under RSACi, the owner of the Website rates itself on a scale of 0–4 in four categories (sex, violence, nudity, and language). A third system, NetShepherd, uses a third party to rate all sites. The drawbacks of rating systems are that few sites are actually rated today and it is unlikely that commercial websites would rate themselves. Alexa Internet reports that in August 1997 they searched a collection of 88,647 Web pages . . . and found 2363 had RSACi labels and 483 had SafeSurf labels. Technology Inventory, Internet Online Summit—Focus of Children (7/29/98). To mandate self-rating would raise additional First Amendment issues because entities such as online newspapers could be asked to rate their content. Furthermore, without the use of filters or other screening methods, ratings could actually help a minor find adult material.

c. Domain name zoning

Segregating adult content was also considered by the Committee. Schemes have been proposed to create a generic top level domain on the Internet that would be specifically reserved for adult content. For example, a set of domain names could be adult only, such as "www.site1.adult" or "www.site1.xxx." There are no technical barriers to creating an adult domain, and it would be very easy to block all websites within an adult domain. Unfortunately, the domain name registration system is in a state of flux. The Internet industry is currently in the process of creating a self-governing structure that will manage the future domain name system and IP number allocation process. In addition, changes made to the top level domains under the new self-governing structure, will have international consequences and the United States should not act without reaching broad industry and international consensus. With respect to the creation of a second level domain within the .us domain, such as "www.site1.xxx.us," which clearly is within the control of the United States, zoning the adult entertainment industry by itself does not solve the problem. Moving commercial sellers of material harmful to minors into a ".xxx.us" domain, like tagging, must be combined with a blocking service. As stated above, the Committee is reluctant to begin regulating the computer industry or waiting for uniform blocking techniques to be developed. Anything short of a mandate on regulating the source of the pornographic material would not result in sufficiently protecting children from accessing material that is harmful.

*3. Blocking or filtering techniques*

Blocking and filtering techniques vary and can be as simple as blocking access to particular sites or as complicated as reviewing each page of material posted on the Web based on key words. In addition, some techniques can be used in conjunction with the zoning methods discussed above, while other approaches operate independently of zoning techniques. While blocking and filtering techniques may be effective for many parents, schools, and libraries, the Committee does not believe, however, that they are as effective as the approach taken in H.R. 3783. In fact, the Committee is concerned that a national mandate requiring the use of blocking or filtering could lead to private censorship or inadvertent blocking. The Committee also does not believe that any of these approaches are currently any less restrictive than the age verification services that are now widely used by the adult entertainment industry and adults.

In general, blocking or filtering software programs work in conjunction with Internet browsers such as Netscape Navigator and Microsoft's Internet Explorer, and are either installed directly onto individual computers or onto a host server used with a network of computers. Blocking or filtering software could also be installed at the site of the Internet access provider. Software to block access to websites has existed for many years. Other products do not prohibit access to sites, but provide parents with a record of which websites a minor has visited.

In order to block Internet sites, a software vendor identifies categories of material to be restricted and then configures the software to block sites containing those categories of speech. Some software blocking vendors employ individuals who browse the Internet for sites to block, while others use automated searching tools to identify which sites to block. New products are constantly being developed, however, that could improve the effectiveness of the blocking software. For example, at least one product has been designed that is capable of analyzing the content being retrieved by the computer. By analyzing the content, rather than a predefined list of sites, the product is capable of screening inappropriate material from chat rooms, e-mail, attached documents, search engines, and web browsers. Such products will help parents and educators reduce a minor's exposure to sexually explicit material.

Mandating blocking or filtering software, however, is not the preferred solution. Because of the discretionary means to screen information, there is a chance that protected, harmless, or innocent speech would be accidentally or inappropriately blocked. Software that blocks a minor's access to "breast," for example, may also screen that minor from accessing information about "breast cancer." In addition, simple blocking techniques that would screen tagged material are not currently available in existing Internet browsers. Moreover, the Committee notes that blocking and filtering software and services can be expensive and may discourage adults or schools from using them. For example, the cost of most products for home use range from $14.95 to $199.50 depending on the quality of the software program. Presumably parents would want to purchase the best product for their use. Other software used for schools or multiple users may cost anywhere from $1,050

to $4,250. See Internet World, "www.internetworld.com" (May 18, 1998). Even if a customer incurs a single nonrecurring cost, he or she may also incur recurring costs because the software needs to be continually updated to respond to the ever-changing content on the World Wide Web. Filters may be very useful tools for parents and educators, but the law should impose duties on the source of the problem, not the victims.

Finally, the Committee remains concerned that all blocking software requires the exercise of subjective human judgment by the vendor or purchaser to decide what speech is acceptable and what is unacceptable. In some cases, the library of restricted words, URLs, or content is not visible to users and may result in hidden censorship if the blocking or filtering service includes matters beyond adult content such as addressing politics or religion.

*E. International distribution of pornography*

Throughout the legislative debate, opponents of H.R. 3783 have argued that 40 percent or more of the pornography sold in the United States originates from foreign countries and that a domestic legislative solution will not stop material from being sent into the United States. To date, however, no reliable statistics exist on the world-wide distribution of pornography over the Internet. A 1996 finding by the lower court ruling in *Reno* is often misquoted by opponents of legislation. They argue that "40% or more" of the material that is harmful to minors is produced outside of the United States. In fact, the lower court concluded that "[a] large percentage, perhaps 40 percent or more, of *content* on the Internet originates outside the United States." 929 F. Supp. at 848 (emphasis added). "Content" is not synonymous with "material harmful to minors." While data regarding the origination of material that is harmful to minors are unavailable, the fact remains that much of the harmful material is produced and posted in the United States. In describing the $8 billion dollar adult entertainment industry, of which commercial pornography is included, the Executive Director of the Free Speech Coalition testified that "[t]hose eight billions are homegrown American products, generating more dollars, jobs and taxes in a burgeoning export trade." Testimony of Jeffrey J. Douglas, Committee Hearing. Clearly domestic restrictions in the United States will help reduce a child's access to pornography, and it may even help protect children in foreign nations who are the recipients of this "burgeoning export trade." To the extent that an international problem exists, the Committee has requested that the Commission on Online Child Protection study the matter and report back to Congress.

## HEARINGS

On September 11, 1998, the Subcommittee on Telecommunications, Trade, and Consumer Protection held a legislative hearing on methods to prevent the distribution of material that is harmful to minors over the Internet. The Subcommittee received testimony from: The Honorable Dan Coats, U.S. Senate, State of Indiana; The Honorable Bob Franks, U.S. House of Representatives, Seventh District, State of New Jersey; The Honorable Ernest J. Istook, Jr., U.S. House of Representatives, Fifth District, State of Oklahoma;

Mr. Stephen R. Wiley, Chief, Violent Crimes and Major Offenders Section, Federal Bureau of Investigations; Mr. Jerry Berman, Director, Center for Democracy and Technology; Mr. Jeffrey J. Douglas, Executive Director, Free Speech Coalition; Mr. Laith Paul Alsarraf, President and CEO, Cybernet Ventures, Inc.; Dr. Mary Anne Layden, Center for Cognitive Therapy, Department of Psychology, University of Pennsylvania; Dr. Larry Lessig, Professor, Harvard Law School; Mr. Peter Nickerson, Chief Executive Officer, N2H2; Mr. Andrew L. Kupser, Chief Executive Officer, Northwest Internet Services, LLC; Mr. John Bastian, Chief Executive Officer, Security Software Systems Inc.; and Ms. Agnes M. Griffen, Director, Tucson-Pima Public Library.

## COMMITTEE CONSIDERATION

On September 17, 1998, the Subcommittee on Telecommunications, Trade, and Consumer Protection met in open markup session and approved H.R. 3783, the Child Online Protection Act, for Full Committee consideration, amended, by a voice vote. On September 24, 1998, the Full Committee met in open markup session and ordered H.R. 3783, reported to the House, amended, by a voice vote, a quorum being present.

## ROLLCALL VOTES

Clause 2(l)(2)(B) of rule XI of the Rules of the House requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto. There were no recorded votes taken in connection with ordering H.R. 3783 reported. An Amendment in the Nature of Substitute offered by Mr. Oxley was adopted by a voice vote. A motion by Mr. Bliley to order H.R. 3783 reported to the House, amended, was agreed to by a voice vote, a quorum being present.

## COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 2(l)(3)(A) of rule XI of the Rules of the House of Representatives, the Committee held a legislative hearing and made findings that are reflected in this report.

## COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

Pursuant to clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives, no oversight findings have been submitted to the Committee by the Committee on Government Reform and Oversight.

## NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 2(l)(3)(B) of rule XI of the Rules of the House of Representatives, the Committee finds that H.R. 3783, the Child Online Protection Act, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 2(l)(3)(C) of rule XI of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
*Washington, DC, October 1, 1998.*

Hon. TOM BLILEY,
*Chairman, Committee on Commerce,*
*U.S. House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3783, Child Online Protection Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Hadley (for federal costs), Hester Grippando (for revenues), and Jean Wooster (for the private-sector impact).

Sincerely,

JUNE E. O'NEILL, *Director.*

Enclosure.

*H.R. 3783—Child Online Protection Act*

Summary: H.R. 3783 would amend the Communications Act of 1934 to require persons engaged in interstate or foreign commerce in the distribution of material that is harmful to minors in or through the World Wide Web to restrict access to such Internet material by persons under 17 years old. The bill would impose civil and criminal penalties on persons who violate this requirement and would establish a commission to study ways of reducing access by children to harmful materials on the Internet.

CBO estimates that implementing this bill would cost about $1 million in 1999, assuming appropriation of the necessary amounts. Because the bill would establish new criminal penalties and thus could affect receipts, pay-as-you-go procedures would apply, but CBO estimates that any changes in receipts would be less than $500,000 a year.

H.R. 3783 would impose both intergovernmental and private-sector mandates, as defined by the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the costs of the mandates would fall well below the thresholds established in UMRA. (The thresholds are $50 million for intergovernmental mandates and $100 million for private sector mandates, adjusted annually for inflation after 1996.)

Estimated cost to the Federal Government: Under H.R. 3783, CBO expects that the Federal Communications Commission (FCC) would issue a regulation to prescribe procedures to be used to re-

strict access to Internet material that is considered harmful to minors. Based on information from the FCC, we estimate that this regulation would cost less than $500,000 to promulgate. That spending would be subject to appropriation of the necessary amounts, but under current law the FCC is authorized to collect fees from the telecommunications industry sufficient to offset the cost of its regulatory program. Therefore, CBO estimates that this provision would have no net cost to the government.

The bill also would amend the Communications Act of 1934 to impose criminal and civil penalties on any person who violates the requirement to restrict access to material that is harmful to minors. Enacting H.R. 3783 could increase governmental receipts from the collection of fines, but CBO estimates that any such increase would be less than $500,000 annually. Criminal fines are deposited in the Crime Victims Fund and are spent in the following year. Thus, any change in direct spending from the fund would also amount to less than $500,000 annually.

Finally, the bill would establish a one-year commission to study ways to reduce access by minors to harmful material on the Internet. Based on information from the National Telecommunications and Information Administration and the experience of similar commissions, CBO estimates that implementing this provision would cost about $1 million in 1999, subject to appropriation of the necessary amount.

Pay-as-you-go considerations: The Balanced Budget and Emergency Deficit Control Act sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. CBO estimates that any increases in governmental receipts and direct spending would each total less than $500,000 a year.

Intergovernmental and private-sector impact: H.R. 3783 would impose both intergovernmental and private-sector mandates, as defined in UMRA. CBO estimates that the costs of the mandates imposed on providers of interactive computer services, including public educational institutions and perhaps some libraries, and on commercial interstate and foreign distributors of "material that is harmful to minors" would be small and would fall below the thresholds established in UMRA.

Section 5 would require that providers of interactive computer services (most of which are private) notify customers that parental control protections are commercially available. According to information from representatives of private-sector Internet providers and their trade association, most providers currently supply the required information to their customers, and some also offer software or filtering services. Furthermore, the cost to those public and private providers that may not currently supply this information would be minimal. Because some public college, universities, perhaps some public libraries offer Internet access, this requirement would impose an intergovernmental mandate on those entities. Based on information from the National Association of State Colleges and Land Grant Universities and the Public Library Association, CBO estimates that the cost of complying with this requirement would be minimal since it would not require significant alteration in most of the agreements currently used.

Section 3 would also impose a private-sector mandate on commercial interstate and foreign distributors who knowingly cause or solicit "material that is harmful to minors" to be posted on the World Wide Web. This section would require that those distributors restrict access to minors of such material. The use of a credit card, debit account, adult access code, adult personal identification number, or any feasible measures would constitute compliance. Based on information from representatives of the industry, commercial adult-content Web sites currently require the use a credit card or some type of age verification for membership or subscription payment. Thus, CBO estimates that those commercial interstate and foreign distributors would not incur any additional costs.

Previous CBO estimate: On March 30, 1998, CBO transmitted an estimate of S. 1482, a bill to amend section 223 of the Communications Act of 1934 to establish a prohibition on commercial distribution on the World Wide Web of material that is harmful to minors, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on March 12, 1998. That bill would not establish a new commission (as H.R. 3783 would); therefore, CBO estimated that S. 1482 would have no significant net effect on the federal budget.

Estimate prepared by: Federal costs: Mark Hadley; Federal revenues: Hester Grippando; Impact on the private sector: Jean Wooster.

Estimate approved by: Paul N. Van de Water, Assistant Director for Budget Analysis.

## FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

## ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

## CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 3, which grants Congress the power to regulate commerce with foreign nations, among the several States, and with the Indian tribes.

## APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

## SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

*Section 1. Short title*

Section 1 establishes the short title of the bill as the "Child Online Protection Act."

*Section 2. Congressional findings*

Section 2 lists the Congressional findings.

*Section 3. Requirements to restrict access by minors to materials sold by means of the World Wide Web that are harmful to minors*

Section 3 amends the Communications Act of 1934 by adding a new section 231, entitled "Restriction of Access by Minors to Materials Sold by Means of the World Wide Web that are Harmful to Minors."

New subsection 231(a) provides that whoever, in interstate or foreign commerce, by means of the World Wide Web, knowingly makes any communication for commercial purposes that includes any material that is harmful to minors without restricting access to such material shall be fined or imprisoned.

The Committee believes that this restriction will help reduce a minor's access to sexually explicit material on the World Wide Web. The restriction is narrowly drafted and is limited to entities making communications for commercial purposes that include material harmful to minors. The restrictions do not apply to other communications on the Internet that involve electronic mail, newsgroups, or chat rooms. The key words used in the prohibition, such as "commercial purposes," and "harmful to minors" are defined in new subsection 231(c). In addition, like any criminal statute, a person who is a conspirator or otherwise aids and abets the offender may be prosecuted under this statute.

New subsection 231(b) clarifies that certain entities do not "make any communication for commercial purposes" if they are engaged in certain transmission or access related activities. In particular, this subsection clarifies that, for purposes of subsection (a), a person shall not be considered to be engaged in making communications for commercial purposes to the extent that such person is (1) a telecommunications carrier engaged in the provision of telecommunications services; (2) a person engaged in the business of providing Internet access services; (3) a person engaged in the business of referring or linking users to an online location on the World Wide Web and includes the provision of directories, indices, references, points, and hypertext links services; or (4) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation of a communication made by another person, without the selection or alteration of the content of the communication.

The Committee believes that these entities do not knowingly cause the material that is harmful to minors to be posted on the World Wide Web, nor do they knowingly solicit such material to be posted on the World Wide Web. The Committee notes, however, that subsection 231(b) applies only "to the extent that such person" is engaged in these other activities. For example, if an Internet access provider also has a web site selling harmful material on the

World Wide Web, then that site would be subject to the general restriction set forth in new subsection 231(a).

New subsection 231(c) states that it is affirmative defense to prosecution under this section if the defendant, in good faith, has restricted access by minors to material that is harmful to minors. The new subsection provides two ways to be eligible for the affirmative defense. The first defense, subparagraph 231(c)(1)(A), permits the person posting the harmful material on the Web to employ the use of a credit card, debit account, adult access code, or adult personal identification number as a means to prove age. The second defense, subparagraph 231(c)(1)(B), allows the defendant to use any other reasonable measures that are feasible under available technology. New subsection 231(c) also permits a good faith defense for entities that attempt to restrict or prevent the transmission of, or access to, a communication specified in this section.

For purposes of this subsection, the Committee believes that purveyors of material harmful to minors have sufficient tools available today to make a good faith attempt to restrict access to their web sites. Credit card verification is commonly used today in both the dial-a-porn and Internet context and it should be easy to use and implement for commercial entities that sell pornography on the Web. In addition, adult access codes and adult personal identification numbers could be issued by mail or fax after reasonably ascertaining that the applicant is not a minor. The Committee does not consider data such as zip codes, telephone numbers, or mere warning pages as a good faith attempt to restrict access. This information is unrelated to the age of the person wishing to access the material and thus should not constitute a defense to prosecution.

The fact that some uncertainty exists surrounding what constitutes a good faith effort to restrict access under subparagraph 231(c)(1)(B) should not undermine the legitimacy of the criminal statute. Entities selling material that is harmful to minors could utilize the subparagraph 231(c)(1)(A) defenses until other defenses under subparagraph 231(c)(1)(B) became available. The Committee believes that technologies will evolve and new age verification systems, such as use of digital certificates, tags, student identifiers, etc. could be used to reduce access and thus, could become effective affirmative defenses. As a result, the bill incorporates needed and limitless flexibility. In addition, the Committee also tasked the industry to study age verification methods pursuant to Section 5 of the bill, which could provide additional help regarding the subparagraph 231(c)(1)(B) defenses.

New subsection 231(d) prohibits a person who collects information about another individual for purposes of restricting access to material that is harmful to minors from disclosing any information collected. The Committee intends to ease the concerns of adults who may be required to disclose certain information about themselves in order to gain access to material that they have a right to receive.

New paragraph 231(e)(1) defines the World Wide Web as the placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol.

In general, the Web utilizes a hypertext formatting language called hypertext markup language (HTML), and programs that browse the Web can display HTML documents containing text, images, sound, animation and moving video. Any HTML document can include links to other types of information or resources, so that while viewing an HTML document that, for example, describes resources available on the Internet, one can "click" using a computer mouse on the description of the resource and be immediately connected to the resource itself. Such hyperlinks allow information to be accessed and organized in very flexible ways, and allow people to locate and efficiently view related information even if the information is stored on numerous computers all around the world. Most sellers of material that is harmful to minors have home pages on the Web that provide links to sexually explicit material, although the home pages themselves often contain hard-core or soft-core pornographic "teasers" that contain material harmful to minors.

New paragraph 231(e)(2) defines commercial purposes as a person who makes a communication when such person is engaged in the business of making such communication. "Engaged in the business" is defined as a person who makes a communication via the Web that is harmful to minors and such person makes the communication as a regular course of such person's trade or business. The Committee notes that the term "engaged in the business," 18 U.S.C. § 1466, has been held constitutional and not unconstitutionally vague as the term is applied to obscenity law. *U.S.* v. *Skinner,* 25 F.3d 1314 (6th Cir. 1994).

New paragraph 231(e)(3) defines the Internet as a combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected world-wide network of computer networks that employ the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol or any successor protocol.

New paragraph 231(e)(4) defines Internet access service as a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may include access to proprietary content, information, and other services as part of a package of services offered to consumers, and paragraph (5) defines Internet information location tool as a service that refers or links users to an online location on the World Wide Web.

New paragraph 231(e)(6) defines material that is harmful to minors as any communication that (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, that such material is designed to appeal to or panders to the prurient interest; (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated normal or perverted sexual act or contact, or a lewd exhibition of the genitals or female breast; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

The Committee intends for the definition of material harmful to minors to parallel the *Ginsberg* and *Miller* definitions of obscenity and harmful to minors, as those definitions were later refined in *Smith* v. *United States,* 431 U.S. 291, at 300–02, 309 (1977) and

*Pope* v. *Illinois,* 481 U.S. 497, at 500–01 (1987). In essence, the Committee intends to adopt the "variable obscenity" standard for minors. The Committee recognizes that the applicability of community standards in the context of the Web is controversial, but understands it as an "adult" standard, rather than a "geographic" standard, and one that is reasonably constant among adults in America with respect to what is suitable for minors. In addition, when a person posts material on the Web, he makes it available, simultaneously, to all communities in the world where a computer can be plugged in. Thus, the person posting the material is engaged in interstate commerce and is subjecting himself to the jurisdiction of all communities in a manner similar to the way obscenity laws apply today. See *United States* v. *Thomas,* 74 F.3d 701 (6th Cir. 1996), cert. denied, 117 S.Ct. 74 (1996); *Sable,* 492 U.S. at 126–27. Furthermore, it is well established that "there is no constitutional impediment to the government's power to prosecute pornography dealers in any district into which the material is sent." *United States* v. *Bagnell,* 679 F.2d 826, 830 (11th Cir. 1982), cert. denied, 460 U.S. 1047 (1983).

The Committee also notes that the "harmful to minors" standard has been tested and refined for thirty years to limit its reach to materials that are clearly pornographic and inappropriate for minor children of the age groups to which it is directed. Cases such as *Erznoznik* v. *City of Jacksonville,* 422 U.S. 205 (1975) and *Board of Education* v. *Pico,* 457 U.S. 853 (1982), prevent the traditional "harmful to minors" test from being extended to entertainment, library, or news materials that merely contain nudity or sexual information, regardless of how controversial they may be for their political or sexual viewpoints.

New paragraph 231(e)(7) defines minor as any person under 17 years of age.

*Section 4. Notice requirement*

Section 4 amends Section 230 of the Communications Act by requiring a provider of interactive computer service to notify each customer, at the time it enters into an agreement to sign up the customer, that parental control protections (such as computer hardware, software, and filtering service) are commercially available that may assist the customer in limiting access to material that is harmful to minors.

The Committee believes that such a requirement will help inform parents and educators on the availability of filtering software and services that may assist with the shielding of harmful material. The Committee also believes that this requirement is a necessary supplement to the general prohibition in Section 3 and allows for marketplace solutions to develop to address the difficult technical and legal questions surrounding restricting a minor's access to harmful material with respect to all communications that take place on the Internet.

*Section 5. Study by commission on online child protection*

Section 5 establishes a temporary Commission on Online Child Protection for purposes of conducting a study regarding methods to help reduce access by minors to material that is harmful to minors

on the Internet. The Commission will be composed of industry and government representatives and is required to report its findings within one year from the date of enactment of H.R. 3783. The Committee intends that the Commission's findings may be used to make legislative recommendations to Congress on additional ways to reduce access by minors to harmful material and as an evidentiary basis for good faith defenses under Section 3 of the bill. The Committee notes that the Commission is required to study alternative ways to reduce material that is harmful to minors on the Internet, which should include ways to reduce such harmful material with respect to one-to-one messaging (e-mail), one-to-many messaging (listserv), distributed message databases (USENET newsgroups); real time communications (Internet relay chat); real time remote utilization (telnet) and remote information retrieval systems. The Commission is also free to comment on the approach taken in H.R. 3783 and on whether other legislative recommendations would be helpful, such as a proposal to prohibit the distribution of unsolicited commercial e-mail that contains material harmful to minors.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

**COMMUNICATIONS ACT OF 1934**

* * * * * * *

# TITLE II—COMMON CARRIERS

## PART I—COMMON CARRIER REGULATION

* * * * * * *

**SEC. 223. OBSCENE OR HARASSING TELEPHONE CALLS IN THE DISTRICT OF COLUMBIA OR IN INTERSTATE OR FOREIGN COMMUNICATIONS.**

(a) * * *

* * * * * * *

(h) For purposes of this section—

(1) * * *

(2) The term "interactive computer service" has the meaning provided in section [230(e)(2)] *230(f)(2)*.

* * * * * * *

**SEC. 230. PROTECTION FOR PRIVATE BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.**

(a) * * *

* * * * * * *

*(d) OBLIGATIONS OF INTERACTIVE COMPUTER SERVICE.—A provider of interactive computer service shall, at the time of entering*

*an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.*

[(d)] *(e)* EFFECT ON OTHER LAWS.—

(1) * * *

* * * * * * *

[(e)] *(f)* DEFINITIONS.—As used in this section:

(1) * * *

* * * * * * *

***SEC. 231. RESTRICTION OF ACCESS BY MINORS TO MATERIALS SOLD BY MEANS OF WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.***

*(a) REQUIREMENT TO RESTRICT ACCESS.—*

*(1) PROHIBITED CONDUCT.—Whoever, in interstate or foreign commerce, by means of the World Wide Web, knowingly makes any communication for commercial purposes that includes any material that is harmful to minors, without restricting access to such material by minors pursuant to subsection (c), shall be fined not more than $50,000, imprisoned not more than 6 months, or both.*

*(2) INTENTIONAL VIOLATIONS.—In addition to the penalties under paragraph (1), whoever intentionally violates such paragraph shall be subject to a fine of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.*

*(3) CIVIL PENALTY.—In addition to the penalties under paragraphs (1) and (2), whoever violates paragraph (1) shall be subject to a civil penalty of not more than $50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.*

*(b) INAPPLICABILITY OF CARRIERS AND OTHER SERVICE PROVIDERS.—For purposes of subsection (a), a person shall not be considered to make any communication for commercial purposes to the extent that such person is—*

*(1) a telecommunications carrier engaged in the provision of a telecommunications service;*

*(2) a person engaged in the business of providing an Internet access service;*

*(3) a person engaged in the business of providing an Internet information location tool; or*

*(4) similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication made by another person, without selection or alteration of the content of the communication, except that such person's deletion of a particular communication or material made by another person in a manner consistent with subsection (c) or section 230 shall not constitute such selection or alteration of the content of the communication.*

*(c) AFFIRMATIVE DEFENSE.—*

*(1) DEFENSE.—It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors—*

*(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; or*

*(B) by any other reasonable measures that are feasible under available technology.*

*(2) PROTECTION FOR USE OF DEFENSES.—No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this subsection or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.*

*(d) PRIVACY PROTECTION REQUIREMENTS.—*

*(1) DISCLOSURE OF INFORMATION LIMITED.—A person making a communication described in subsection (a)—*

*(A) shall not disclose any information collected for the purposes of restricting access to such communications to individuals 17 years of age or older without the prior written or electronic consent of—*

*(i) the individual concerned, if the individual is an adult; or*

*(ii) the individual's parent or guardian, if the individual is under 17 years of age; and*

*(B) shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the person making such communication and the recipient of such communication.*

*(2) EXCEPTIONS.—A person making a communication described in subsection (a) may disclose such information if the disclosure is—*

*(A) necessary to make the communication or conduct a legitimate business activity related to making the communication; or*

*(B) made pursuant to a court order authorizing such disclosure.*

*(e) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:*

*(1) BY MEANS OF THE WORLD WIDE WEB.—The term "by means of the World Wide Web" means by placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol.*

*(2) COMMERCIAL PURPOSES; ENGAGED IN THE BUSINESS.—*

*(A) COMMERCIAL PURPOSES.—A person shall be considered to make a communication for commercial purposes only if such person is engaged in the business of making such communications.*

*(B) ENGAGED IN THE BUSINESS.—The term "engaged in the business" means that the person who makes a commu-*

*nication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income). A person may be considered to be engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to minors, only if the person knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web.*

*(3) INTERNET.—The term "Internet" means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit information.*

*(4) INTERNET ACCESS SERVICE.—The term "Internet access service" means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services.*

*(5) INTERNET INFORMATION LOCATION TOOL.—The term "Internet information location tool" means a service that refers or links users to an online location on the World Wide Web. Such term includes directories, indices, references, pointers, and hypertext links.*

*(6) MATERIAL THAT IS HARMFUL TO MINORS.—The term "material that is harmful to minors" means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that—*

*(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, that such material is designed to appeal to or panders to the prurient interest;*

*(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or female breast; and*

*(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.*

*(7) MINOR.—The term "minor" means any person under 17 years of age.*

* * * * * * *

○