Order Code RS20036
Updated January 16, 2001

Internet—Protecting Children from Unsuitable Material and Sexual Predators: Overview and Pending Legislation

Marcia S. Smith
Specialist in Aerospace and Telecommunications Policy
Resources, Science, and Industry Division

Summary

Protecting children from unsuitable material and sexual predators on the Internet has been a major concern for Congress and the Clinton Administration. Congress passed three laws concerning protecting children from certain content on the Web. The major provisions of the first, the Communications Decency Act (P.L. 104-104), were overturned by the Supreme Court. The Child Online Protection Act (P.L. 105-277) is currently under review in the courts. The Children's Internet Protection Act (P.L. 106-554), which would require most schools and libraries to use filtering technologies to block certain Web sites, is expected to be challenged as well. Since the arena for debate on this issue is expected to shift from Congress to the courts, this report will not be updated. See CRS Report 98-670 for information on the status of court action.

Overview

What children are encountering on the Internet, particularly in terms of indecent or otherwise unsuitable material or contacts with strangers who intend to do them harm, is an issue of major concern.

Congress passed the Communications Decency Act (CDA) as part of the 1996 Telecommunications Act (P.L. 104-104). Among other things, CDA would have made it illegal to send indecent material to children via the Internet. In June 1997, the Supreme Court overturned the portions of the CDA dealing with indecency and the Internet. (Existing law permits criminal prosecutions for transmitting obscenity or child pornography over the Internet.) Congress passed a replacement law, the Child Online Protection Act, in 1998 (see next section) and other legislation to protect children as they use the Internet.

The Child Online Protection Act (P.L. 105-277): Prohibiting Access by Children to Material That is "Harmful to Minors"

The 105th Congress passed the Child Online Protection Act (COPA) as part of the Omnibus Appropriations Act (P.L. 105-277, Title XIV of Division C). The law prohibits commercial distribution of material over the Web to children under 17 that is "harmful to minors." Web site operators must ask for a means of age verification such as a credit card number before displaying such material. It replaces provisions of the 1996 Communications Decency Act that were overturned by the Supreme Court. By limiting the language to commercial activities and using "harmful to minors" instead of "indecent" as was used in the 1996 Act, the sponsors hoped they had drafted a law that would survive court challenges.

The American Civil Liberties Union (ACLU) and others filed suit against the part of COPA dealing with commercial distribution of material harmful to minors over the Internet in the U.S. District Court for the Eastern District of Pennsylvania on October 22, 1998. Judge Lowell A. Reed, Jr. issued a preliminary injunction against enforcement of that part of the Act on February 1, 1999. The Justice Department appealed the ruling. The U.S. Court of Appeals for the Third Circuit let stand the injunction on June 22, 2000. (See also CRS Report 98-670, *Obscenity, Child Pornography, and Indecency: Recent Developments and Pending Issues*.)

COPA established a Commission on Online Child Protection to study technologies and methods to help reduce access by children to material on the Web that is harmful to minors. (This part of the Act was not affected by the injunction.) The Commission, composed of 16 industry members appointed by the Republican and Democratic congressional leaders plus one ex officio representative each from the Federal Trade Commission (FTC) and Departments of Commerce and Justice, issued its report on October 20, 2000 [available at http://www.copacommission.org]. The report did not make recommendations for new legislation. It surveyed various technologies and other means by which children's access to certain materials on the Internet can be restricted, concluding that no single solution exists. Recommendations focused on the need for public education, consumer empowerment efforts, vigorous enforcement of existing laws, and voluntary industry actions. Separately, P.L. 105-314 (see next section) requires the Attorney General to contract with the National Research Council (NRC) to conduct a two-year study on the capabilities of computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet. NRC anticipates that the study will be completed in late 2001.

Sexual Predators on the Internet (P.L. 105-314 and P.L. 105-277)

The 105th Congress also was concerned about sexual predators using the Internet to approach children. Because conversations can take place anonymously on the Internet, a child may not know that (s)he is talking with an adult. The adult may persuade the child to agree to a meeting, with tragic results. Congress passed H.R. 3494 (P.L. 105-314), the Protection of Children from Sexual Predators Act, to address those and other non computer-related issues related to protecting children from sexual predators. The law: prohibits using the mail or any facility or means of interstate or foreign commerce (a) to initiate the transmission of the name, address, telephone number, social security number, or electronic mail address of an individual under 16 with the intent to entice, encourage,

offer, or solicit any person to engage in any sexual activity for which any person can be charged with a criminal offense, or (b) to persuade, induce, entice, or coerce any individual under 18 to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense; makes it a crime to transfer obscene matter by mail or any facility or means of interstate or foreign commerce to anyone under 16; calls for the U.S. Sentencing Commission to recommend appropriate changes to Federal Sentencing Guidelines if a defendant used a computer with the intent to persuade, induce, entice, coerce, or facilitate the transport of a child to engage in any prohibited sexual activity; requires electronic communication or remote computing services that have knowledge of violations of child pornography laws to report it to law enforcement officials; prohibits federal prisoners from having unsupervised access to the Internet and recommends that states do the same with their prisoners; and requires a study of technologies to control the electronic transmission of pornography (discussed earlier).

The Children's Internet Protection Act: Requiring Schools and Libraries to Use Filtering Technologies (Title XVII of the FY2001 Labor-HHS Appropriations Act, H.R. 4577)

Background. Software products to filter or block access to Web sites or e-mail addresses has existed for many years. Links to information about these and other products and other tools for protecting children on the Web are available at [http://www.GetNetWise.org]. Some filtering products screen sites based on keywords, while others use ratings systems based on ratings either by the software vendor or the Web site itself.

Existing filtering software products have received mixed reviews because they cannot effectively screen out all objectionable sites on the ever-changing Web, or because they inadvertently screen out useful material. The Electronic Privacy Information Center (EPIC) released a report on filtering software in November 1997 entitled *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* [http://www2.epic.org/reports/filter-report.html]. EPIC tested a filtering program called Net Shepard, searching the Web for sites it expected to be useful to and suitable for children. For example, EPIC searched for Web sites about the "American Red Cross" with and without Net Shepard activated. EPIC reported that Net Shepard prevented access to 99.8% of the sites. From this and other examples, EPIC concluded that in the effort to protect children from a small amount of unsuitable material, they were being denied access to a large amount of suitable information.

Congress and the Clinton Administration debated for several years whether to require schools and libraries to use filtering technology when children are using computers with Internet access, or to require Internet Service Providers (ISPs) to offer such technology to subscribers in general. A section of COPA requires interactive computer services to advise customers that parental control protections are commercially available.

On May 5, 1999, Vice President Gore held a press conference with representatives of the Internet industry to announce that by July 1999 a "Parents' Protection Page" would appear automatically on most Web sites to help parents identify tools already available for them to guide their children in using the Internet, including filtering software. The Vice President stated: "The best protection is an involved parent, taking time to pass on the right values to children. But government and industry do have a responsibility to make it

easier and simpler for parents to do so." (White House press release 1999-05-05, *Remarks by the Vice President on the Internet*). The GetNetWise Web site mentioned above, sponsored by the Internet industry and public interest groups, debuted in August 1999 providing "one click" tools for parents to guide their children when using the Internet and to report trouble. Many ISPs already were providing parents with tools and information voluntarily. The Internet industry had created another Web site [http://www.americalinksup.org] following a December 1997 "Kids Online Summit" to offer filtering software to parents and implement an outreach campaign to increase its use.

Despite these efforts at industry-sponsored solutions, debate continued over whether schools and libraries should be required by law to use filtering technology on computers that have Internet access when children are using them. Policies adopted by local communities reflect the spectrum of attitudes on this topic. Some allow children to use computers at local libraries only with parental permission, some use filtering software, and others impose no restrictions. Quality Education Data reported in October 1999 (*Communications Daily*, October 25, 1999, p. 2-3) that 58.3% of schools use filtering software and 90.5% have "acceptable use" policies where adults and children have an agreement regarding how the children should behave when using the Internet.

Supporters of attempts to pass a law requiring schools and libraries to use filtering technology argue that children must be protected from inappropriate material, particularly when their parents are not present to supervise them. Critics assert that it is censorship, prevents access to appropriate sites, and that such decisions should be left to the local community. Some believe "acceptable use" or "Internet use" policies are preferable.

Passage of the Act. The 106th Congress ultimately passed legislation requiring schools and libraries that receive federal funds to use filtering or blocking technology. The Children's Internet Protection Act, Title XVII of the FY2001 Labor-HHS Appropriations Act (H.R. 4577 as cleared for the White House on December 15, 2000, *Congressional Record*, December 15, 2000, p. H12302-12307), requires most schools and libraries to use "technology protection measures" to filter or block unsuitable Web sites. The Act blends approaches to this issue championed by Representative Istook, Senator McCain, and Senator Santorum.

Representative Istook's approach was that if a school received funds under Title III of the Elementary and Secondary Education Act (ESEA) to buy computers used to access the Internet or to pay for access to the Internet, it must use filtering or blocking technologies on computers accessible to minors. The filtering or blocking technologies would screen out Web sites with material that was obscene, child pornography, or harmful to minors. Senator McCain's approach was similar except that he would have applied it to schools and libraries receiving federally-provided "E-rate" subsidies through the universal service fund. (For information on universal service and the E-rate, see CRS Issue Brief IB98040, *Telecommunications Discounts for Schools and Libraries: the "E-Rate" Program and Controversies*.) Also, library computers used by adults would have been subject to similar requirements. The filtering or blocking technology could be disabled by an authorized person for bona fide research or other lawful purposes. Senator Santorum took a different approach in which schools and libraries receiving E-rate funds would be required to adopt and implement "Internet use" policies instead of using filtering technology.

Congress resolved these different approaches in the Children's Internet Protection Act. The Act refers to "technology protection measures," defined in the Act as specific technologies that block or filter Internet access to visual depictions that are obscene, child pornography, or harmful to minors. Other important definitions in the Act include: a "minor" is under 17; "obscene" has the meaning given in 18 U.S.C. 1460; "child pornography" has the meaning given in 18 U.S.C. 2256; and "harmful to minors" means any picture, image, graphic image file, or other visual depiction that, taken as a whole and with respect to minors appeals to a prurient interest in nudity, sex, or excretion; depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or contact, actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals; and taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. Schools and libraries may block other content if they wish. Nothing in the Act requires tracking of Internet use by any identifiable minor or adult. The Act provides that:

NTIA Notice and Comment Proceeding. The National Telecommunications and Information Administration must initiate a notice and comment proceeding no later than 18 months after the date of enactment of the Act to evaluate whether or not currently available technology protection measures, including commercial Internet blocking and filtering software, adequately addresses the needs of educational institutions; make recommendations on how to foster the development of measures that meet such needs; and evaluate the development and effectiveness of local Internet safety policies that are currently in operation after community input.

Schools and Libraries That Do Not Receive E-Rate Funds. Funds made available to schools under Title III of ESEA, and funds made available to libraries under section 224 of the Museum and Library Services Act, to schools or libraries that do not receive E-rate funds, may not be used to purchase computers used to access the Internet or to pay for direct costs of accessing the Internet, unless the school, school board, local educational agency, or other authority, or library, has an Internet safety policy for minors that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors. A similar requirement is made to protect against access by other users to visual depictions that are obscene or are child pornography. The technology protection measure may be disabled by an administrator, supervisor, or other authorized person to enable access for bona fide research or other lawful purposes.

Timetables are established for schools to be certified by the local educational agency responsible for that school, and libraries to self-certify as part of the application process for the next program funding year. Waivers may be granted if state or local procurement rules or regulations or competitive bidding requirements prevent making the certification. If a school does not comply, the Secretary of Education may withhold further funding under Title III, issue a cease and desist order, or enter into a compliance agreement. If a library does not comply, the Director of the Institute of Museum and Library Services has the same options. No recovery of funds is permitted in either case.

Schools and Libraries That Do Receive E-Rate Funds. Elementary and secondary schools and libraries that receive E-rate funding must be certified by the Federal Communications Commission (FCC) that they have adopted and implemented an Internet safety policy for computers with Internet access and are using those computers in

accordance with the certifications. This requirement does not apply to schools and libraries that receive E-rate funds only for purposes other than the provision of Internet access, Internet service, or internal connections.

Each school, school board, or other authority responsible for administering the school, or library, shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy. If a school does not meet the definition of an elementary or secondary school under ESEA, the notice and hearing may be limited to members of the public with a relationship to the school.

The certification must certify that the school or library is enforcing a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with respect to any computer with Internet access that protects against access to visual depictions that are obscene, child pornography, or harmful to minors, and is enforcing operation of the technology protection measure. A similar requirement is made for adult users against access to material that is obscene or child pornography. The technology protection measure may be disabled during adult use to enable access for bone fide research or other lawful purpose.

Timetables and waivers are similar to what is provided for schools that do not receive E-rate funds. Schools and libraries that do not submit certifications may not receive E-rate funds. If they do not comply, they must reimburse any funds or discounts they received during the period covered by the certification. The FCC is required to prescribe regulations to implement this section within 120 days of enactment.

Funds for Acquiring Technology Protection Measures. Funding available under Title VI of ESEA or section 231 of the Library Services and Technology Act may be used to obtain necessary technology protection measures.

Neighborhood Children's Internet Protection Act. Each school or library receiving E-rate funds shall adopt and implement an Internet safety policy that addresses access by minors to inappropriate matter on the Internet and World Wide Web, the safety and security of minors when using e-mail, chatrooms, and other forms of direct electronic communications; unauthorized access and other unlawful activities by minors online; unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors, and provide reasonable public notice and hold at least one public hearing or meeting to address the proposal Internet safety policy. Determining what is inappropriate for minors shall be made locally. The FCC shall prescribe regulations for purposes of this section no later than 120 days after the date of enactment.

Expedited judicial review. Any civil action challenging the constitutionality, on its face, of the Act would be heard first by a district court of three judges convened pursuant to 28 U.S.C. 2284. Appellate review would be by direct appeal to the Supreme Court.

Expected Challenges to the Law. According to the Washington Times (December 20, 2000, p. B7), the American Library Association and the American Civil Liberties Union have indicated that they will challenge the law in court, as will the Free Congress Foundation, which opposes the Act because it overrides local laws. The Electronic Privacy Information Center (EPIC) and the Center for Democracy and Technology (CDT) also have criticized passage of the Act.