Calendar No. 538

110TH CONGRESS
1st Session

SENATE

REPORT
110–245

PROTECTING CHILDREN IN THE 21ST CENTURY ACT

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 1965

DECEMBER 12, 2007.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
69–010 WASHINGTON : 2007

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

DANIEL K. INOUYE, Hawaii, *Chairman*
TED STEVENS, Alaska, *Vice-Chairman*

JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
THOMAS CARPER, Delaware
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota

JOHN MCCAIN, Arizona
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana
JOHN THUNE, South Dakota

MARGARET CUMMISKY, *Staff Director and Chief Counsel*
LILA HELMS, *Deputy Staff Director and Policy Director*
JEAN TOAL EISEN, *Senior Advisor and Deputy Policy Director*
CHRISTINE KURTH, *Republican Staff Director and General Counsel*
PAUL J. NAGLE, *Republican Chief Counsel*
MIMI BRANIFF, *Republican Deputy Chief Counsel*

Calendar No. 538

110TH CONGRESS *1st Session* | SENATE | REPORT 110–245

PROTECTING CHILDREN IN THE 21ST CENTURY ACT

DECEMBER 12, 2007.—Ordered to be printed

Mr. INOUYE, from the Committee on Commerce, Science, and Transportation, submitted the following

REPORT

[To accompany S. 1965]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 1965) to protect children from cybercrimes, including crimes by online predators, to enhance efforts to identify and eliminate child pornography, and to help parents shield their children from material that is inappropriate for minors, having considered the same, reports favorably thereon with amendments and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The purpose of S. 1965 is to assist parents in protecting their children from harmful content on the Internet and in educating children about potential dangers associated with inappropriate online communications. Toward these ends, the bill focuses on several strategies to improve online safety and to prevent the exploitation of children online. The bill would require the Federal Trade Commission to coordinate and implement a national public awareness and education campaign focused on strategies promoting the safe use of the Internet by children. The bill would also direct the Assistant Secretary of Commerce for Communications and Information to create a private sector working group to review and evaluate the status of industry efforts to promote online safety. The bill would require schools receiving universal service funds from the Federal "e-rate" program to ensure that their Internet safety policies include education about appropriate online behavior. Finally, the bill would increase maximum fines that may be assessed against certain Internet service providers for failing to report child pornography and would strengthen the ability of law enforcement

personnel and the National Center for Missing and Exploited Children (NCMEC) to share information with certain relevant parties.

BACKGROUND AND NEEDS

The Internet is a valuable educational and social resource for children. Used safely, it can offer children access to a wealth of information and material and can provide a means to exchange ideas with other social peers. However, this positive tool also includes hidden dangers. The wealth of information available on the Internet includes significant amounts of material that may not be suitable for children. Additionally, the anonymity of the Internet and the susceptibility of children raise particular dangers with respect to invasions of privacy and threats from online predators. These dangers have only become more pronounced as individuals use the Internet not only to find information, but increasingly to convey personal information about themselves on personal Web pages or though social networking sites like MySpace or Facebook.

According to a 2007 Pew Internet survey, 93 percent of all Americans between 12 and 17 years old use the Internet, demonstrating a steady rise from 87 percent in 2004 and 73 percent in 2000. Moreover, not only are more teens online, but they are also using the Internet more intensely now than in the past, with 89 percent percent of online teens using the Internet at least once a week and 61 percent using it daily.

Accordingly, efforts to promote a safe, online environment are critical components of ensuring that the promise of communications technologies can be fully embraced by parents and children alike. There is no single solution to protecting children on the Internet. Instead, protection requires a multi-layered approach that relies on social and educational strategies to teach responsible and safe use coupled with technology, public policy, and law enforcement to shape the online environment that children experience.

Child Pornography and the Internet. Unfortunately, the growth of broadband and the anonymity of the Internet have resulted in a significant increase in the distribution of illegal, child pornography. Commercial child pornography is a multi-billion dollar, worldwide industry. While the exact scope of the problem of child pornography is difficult to determine, it is clear that the problem has exploded with the advent of the Internet. NCMEC reported that it had received an increase of reports to its CyberTipline from more than 24,400 in 2001 to more than 340,000 by the beginning of 2006. Moreover, NCMEC found that 19 percent of identified sex offenders had images of children younger than 3 years old; 39 percent had images of children younger than 6 years old; and 83 percent had images of children younger than 12 years old.

Protecting Children from Inappropriate Content. Beyond concerns about the victimization of children in pornography parents are also concerned with shielding their children from adult pornography that may be easily accessible over the Internet. Easy access to pornography through the Internet threatens to dramatically reshape a child's perception about sex and body image.

According to a 2001 study by the Kaiser Family Foundation, 70 percent of the nation's 15 to 17 year olds have looked at Internet pornography, much of it graphically hardcore, with just under half (45 percent) saying that they were upset by the experience. While

filtering technologies and other methods to control children's access to pornography are available, parents' lack of familiarity with these tools and the rapid development of technologies to defeat such tools leave parents feeling as if they are fighting a losing battle to limit their children's exposure to sexually explicit content.

In May 2002, at the direction of Congress, the National Academy of Sciences issued a report reviewing computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet. This report, titled Youth, Pornography, and the Internet, was prepared by a committee chaired by former U.S. Attorney General Richard Thornburgh. According to the Thornburgh Report, the nature of the Internet posed particular challenges to parents seeking to protect their children from inappropriate material in that:

> "Compared to other media, the Internet has characteristics that make it harder for adults to exercise responsible supervision over children's use of it. A particularly worrisome aspect of the Internet is that inappropriate sexually explicit material can find its way onto children's computer screens without being actively sought. Further, it is easy to find on today's Internet not only images of naked people, but also graphically depicted acts of heterosexual and homosexual intercourse (including penetration), fellatio, cunnilingus, masturbation, bestiality, child pornography, sadomasochism, bondage, rape, incest, and so on. While some such material can be found in sexually explicit videos and print media that are readily available in hotels, video rental stores, and newsstands, other sexually explicit material on the Internet is arguably more extreme than material that is easily available through non-Internet media."

While acknowledging the additional risks arising from the ease of access and anonymity on the Internet, the Thornburgh Report was careful to conclude that:

> "[t]here is no single or simple answer to controlling the access of minors to inappropriate material on the Web. To date, most of the efforts to protect children from inappropriate sexually explicit material on the Internet have focused on technology-based tools such as filters and legal prohibitions or regulation. But the committee believes that neither technology nor policy can provide a complete—or even a nearly complete—solution. While both technology and public policy have important roles to play, social and educational strategies to develop in minors an ethic of responsible choice and the skills to effectuate these choices and to cope with exposure are foundational to protecting children from negative effects that may result from exposure to inappropriate material or experiences on the Internet. . .".

According to a recent 2007 Pew Internet survey, 54 percent of parents say that they have a filter installed on the computer that their child uses at home, and 45 percent of parents say that they have monitoring software installed on the computer that the teen uses at home. Similar data was revealed in a 2007 Kaiser Family Foundation report which found that among parents with children age 9 or older who use the Internet at home, 41 percent say they use parental controls to block access to certain websites.

Protecting Children from Inappropriate Communication. In addition to concerns arising from the availability of unsavory content, the anonymity of the Internet and the willingness of children to communicate and share information raise additional concerns related to privacy, harassment or "cyberbullying," and potential safety risks from online predators.

Much of the recent media coverage surrounding dangers faced by children online has focused on the increasing popularity of social networking sites like MySpace or Facebook. More basic social networking sites provide an online location where a user can create a profile and build a personal network that connects him or her to other users. In the past five years, such sites have rocketed from a niche activity into a phenomenon that engages tens of millions of Internet users. The explosive growth in the popularity of these sites has generated concerns among some parents, school officials, and government leaders about the potential risks posed when personal information is made available in such a public setting.

These fears are heightened by data reflecting attitudes among teens related to their willingness to post personal information. According to one recent survey sponsored by Cox Communications in partnership with NCMEC, a majority of teens (58 percent) do not think posting photos or other personal information on social networking sites is unsafe. According to this same study, 64 percent post photos or videos of themselves, while 58 percent post info about where they live, and 8 percent have posted their cell phone number online.

In April 2007, the Pew Internet & American Life Project released the results of a recent survey titled *Teens, Privacy and Online Social Networks* that examined teenage use of social networks and their understanding of the implications of sharing their personal information online. According to that survey, 32 percent of online teenagers (and 43 percent of social-networking teens) have been contacted online by complete strangers, and 17 percent of online teens (31 percent of social networking teens) have "friends" on their social network profile who they have never personally met.

SUMMARY OF PROVISIONS

S. 1965 focuses on a variety of measures designed to improve the safety of children online. The bill would direct the Federal Trade Commission to carry out a nationwide program to increase public awareness and provide education promoting the safe use of the Internet by children. It also would direct the Assistant Secretary of Commerce for Communications and Information to establish an Online Safety and Technology working group to review industry efforts to promote online safety for children. Further, S. 1965 would amend the Communications Act of 1934 to require schools to educate minors about appropriate online behavior and to impose a forfeiture penalty on certain Internet service providers who violate requirements to report online child pornography. Finally, the bill would strengthen existing enforcement strategies by tripling the maximum fines that may be levied on providers of electronic communication services or remote computing services who knowingly and willfully fail to report child pornography, by requiring reporting of online child pornography to foreign law enforcement agencies, and by authorizing the NCMEC to provide elements of images

relating to child pornography to electronic communication service providers for the purpose of stopping further transmission of such images and developing anti-child pornography technologies.

LEGISLATIVE HISTORY

The Protecting Children in the 21st Century Act (S. 1965) was introduced by Senator Ted Stevens on August 2, 2007, and referred to the Senate Committee on Commerce, Science, and Transportation. The bill is cosponsored by 16 Senators including Senators Inouye, Hutchinson, Nelson (FL), Pryor, Rockefeller, Kerry, Klobuchar, Smith, Snowe, and Thune. On July 24, 2007, the Committee held a hearing on "Protecting Children on the Internet." On September 27, 2007, the Committee considered the bill in an open Executive Session. Chairman Inouye and Vice-Chairman Stevens offered an amendment making minor technical changes. The amendment and bill were both adopted by voice vote. The Committee, by voice vote, ordered that S. 1965 be reported.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 18, 2007.

Hon. DANIEL K. INOUYE
Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 1965, the Protecting Children in the 21st Century Act.

If you wish further details on this estimate, we will be pleased to provide them.

The CBO staff contact is Susan Willie.

Sincerely,

ROBERT A. SUNSHINE
(For Peter R. Orszag, Director).

Enclosure.

S. 1965—Protecting Children in the 21st Century Act

Summary: S. 1965 would authorize the Federal Trade Commission (FTC) to develop a program to promote safe use of the Internet by children. The bill also would require the National Telecommunications and Information Administration (NTIA) to establish a working group to study and report to the Congress on actions taken by the telecommunications industry to promote a safe environment on the Internet for children. Finally, the bill would increase certain penalties on Internet service providers (ISPs) that fail to report child pornography to the appropriate federal authorities.

CBO estimates that implementing S. 1965 would increase spending subject to appropriation by $4 million in 2008 and $10 million over the 2008–2012 period, assuming that the authorized funds are

appropriated. CBO expects that enacting the bill would not have a significant effect on collections from penalties, which are recorded in the budget as revenues, and would not affect direct spending.

S. 1965 contains no intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

S. 1965 would impose a private-sector mandate as defined in UMRA on certain ISPs by requiring them to provide additional information when reporting suspected violations of child pornography laws to the National Center for Missing and Exploited Children (NCMEC). CBO expects that the cost to those providers of complying with this mandate would not be significant and would not exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

Estimated cost to the federal government: The estimated budgetary impact of S. 1965 is shown in the following table. The costs of this legislation fall within budget functions 370 (commerce and housing credit) and 750 (administration of justice).

	By fiscal year, in millions of dollars—				
	2008	2009	2010	2011	2012
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Authorization Level	5	5	0	0	0
Estimated Outlays	4	5	1	0	0

Basis of estimate: Section 103 would authorize the appropriation of $5 million in each of fiscal years 2008 and 2009 for the FTC to develop and carry out a campaign to promote ways of protecting children who use the Internet. The bill also would require the FTC to submit a report to the Congress detailing the activities undertaken in the campaign. Based on information from the FTC, CBO estimates that implementing this provision of S. 1965 would cost $4 million in 2008 and $10 million over the 2008–2012 period.

Section 105 would require the NTIA to establish a working group to evaluate efforts of the telecommunications industry to create a safe environment for children using the Internet. Based on information from the NTIA, CBO estimates that implementing this provision would not have a significant effect on spending subject to appropriation.

Other provisions of the bill would increase forfeiture and civil penalties for ISPs that fail to report certain information about child pornographers or the existence of child pornography on their sites. Thus, the federal government might collect additional forfeiture and civil fines if the legislation is enacted (collections of such fines are recorded in the budget as revenues). CBO estimates that any additional revenues would not be significant because of the relatively small number of cases likely to be affected.

Estimated impact on state, local, and tribal governments: S. 1965 contains no intergovernmental mandates as defined in UMRA and would impose no costs on state, local, or tribal governments.

Estimated impact on the private sector: S. 1965 would expand an existing reporting requirement on certain ISPs by requiring them to provide additional information when reporting suspected violations of child pornography to the NCMEC. ISPs are currently re-

quired to report any incident of child pornography to the NCMEC. Current law, however, does not specify what information should be included in such reports. The bill would require ISPs to include:

- User ID or other online identifier of the individual who appears to be violating the law;
- Time and date on which the incident occurred or was discovered;
- Geographic location of the individuals involved;
- Images of the apparent child pornography relating to the incident; and
- Contact information for the ISP reporting the incident.

Although such information is already requested in NCMEC's online report forms, compliance is voluntary.

CBO expects the additional cost of complying with the mandate would be minimal. The information required by the bill is usually captured and stored by ISP systems, and some ISPs already comply with the mandate when filing reports with the NCMEC. Further, the bill would require ISPs to provide the requested information only to the extent that such information is available. Consequently, CBO estimates that the incremental cost to ISPs of complying with this mandate would not exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

Estimate prepared by: Federal Costs: Susan Willie; Impact on State, Local, and Tribal Governments: Elizabeth Cove; Impact on the Private Sector: MarDestinee Perez.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

S. 1965 is intended to enhance current efforts to combat child pornography, to educate children about inappropriate online communications, and to assist parents in protecting their children from inappropriate material that is available via the Internet. The bill affects a number of parties involved in educating children about safe online behavior and in providing online services over the Internet.

ECONOMIC IMPACT

S. 1965 would not have an adverse economic impact on the Nation's economy.

PRIVACY

The reported bill would have no significant impact on the personal privacy of United States citizens.

PAPERWORK

The reported bill should not significantly increase paperwork requirements for individuals and businesses.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

Section 1 would establish the Act as the Protecting Children in the 21st Century Act.

Section 101. Internet safety

Section 101 would define the scope of Internet safety issues as addressed in the bill.

Section 102. Public Awareness Campaign

Section 102 would direct the Federal Trade Commission to carry out a national program to increase public awareness and provide education promoting the safe use of the Internet by children.

Section 103. Annual reports

Section 103 would require the Federal Trade Commission to submit an annual report to Congress on the activities of the public awareness campaign.

Section 104. Authorization of Appropriations

Section 104 would authorize $5,000,000 for each of fiscal years 2008 and 2009 for the public awareness campaign.

Section 105. Online Safety and Technology Working Group

Section 105 would direct the Assistant Secretary of Commerce for Communications and Information to establish an Online Safety and Technology working group comprised of representatives from the business community, public interest groups, and other appropriate groups and Federal agencies to review industry efforts to promote online safety for children. The working group would report its findings to the Senate Committee on Commerce, Science, and Transportation within one year of being convened.

Section 106. Promoting online safety in schools

Section 106 would amend the Communications Act of 1934 to require schools to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Section 107. Definitions

Section 107 would define the term "Commission" as the Federal Trade Commission and the term "Internet" as collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the inter-connected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor successor protocols to such protocol, to communicate information of all kinds by wire or radio.

Section 201. Child pornography prevention; forfeitures related to child pornography

Section 201 would amend the Communications Act of 1934 to provide a forfeiture penalty for carriers who violate requirements to report online child pornography.

Section 202. Additional child pornography amendmentsr

Section 202 (a) would amend the Crime Control Act of 1990 to triple the fines on providers of electronic communication services or remote computing services who knowingly and willfully fail to report child pornography and (b) would amend the Victims of Child Abuse Act of 1990 to require more specific reporting of online child pornography to foreign law enforcement agencies and authorize the NCMEC to provide elements of images relating to child pornography to electronic communication service providers for the purpose of stopping further transmission of such images and developing anti-child pornography technologies.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, 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 material is printed in italic, existing law in which no change is proposed is shown in roman):

COMMUNICATIONS ACT OF 1934

SEC. 254. UNIVERSAL SERVICE.

[47 U.S.C. 254]

(a) PROCEDURES TO REVIEW UNIVERSAL SERVICE REQUIREMENTS.—

(1) FEDERAL-STATE JOINT BOARD ON UNIVERSAL SERVICE.—Within one month after the date of enactment of the Telecommunications Act of 1996, the Commission shall institute and refer to a Federal-State Joint Board under section 410(c) a proceeding to recommend changes to any of its regulations in order to implement sections 214(e) and this section, including the definition of the services that are supported by Federal universal service support mechanisms and a specific timetable for completion of such recommendations. In addition to the members of the Joint Board required under section 410(c), one member of such Joint Board shall be a State-appointed utility consumer advocate nominated by a national organization of State utility consumer advocates. The Joint Board shall, after notice and opportunity for public comment, make its recommendations to the Commission 9 months after the date of enactment of the Telecommunications Act of 1996.

(2) COMMISSION ACTION.—The Commission shall initiate a single proceeding to implement the recommendations from the Joint Board required by paragraph (1) and shall complete such proceeding within 15 months after the date of enactment of the Telecommunications Act of 1996. The rules established by such proceeding shall include a definition of the services that are supported by Federal universal service support mechanisms and a specific timetable for implementation. Thereafter, the Commission shall complete any proceeding to implement sub-

sequent recommendations from any Joint Board on universal service within one year after receiving such recommendations.

(b) UNIVERSAL SERVICE PRINCIPLES.—The Joint Board and the Commission shall base policies for the preservation and advancement of universal service on the following principles:

(1) QUALITY AND RATES.—Quality services should be available at just, reasonable, and affordable rates.

(2) ACCESS TO ADVANCED SERVICES.—Access to advanced telecommunications and information services should be provided in all regions of the Nation.

(3) ACCESS IN RURAL AND HIGH COST AREAS.—Consumers in all regions of the Nation, including low-income consumers and those in rural, insular, and high cost areas, should have access to telecommunications and information services, including interexchange services and advanced telecommunications and information services, that are reasonably comparable to those services provided in urban areas and that are available at rates that are reasonably comparable to rates charged for similar services in urban areas.

(4) EQUITABLE AND NONDISCRIMINATORY CONTRIBUTIONS.—All providers of telecommunications services should make an equitable and nondiscriminatory contribution to the preservation and advancement of universal service.

(5) SPECIFIC AND PREDICTABLE SUPPORT MECHANISMS.—There should be specific, predictable and sufficient Federal and State mechanisms to preserve and advance universal service.

(6) ACCESS TO ADVANCED TELECOMMUNICATIONS SERVICES FOR SCHOOLS, HEALTH CARE, AND LIBRARIES.—Elementary and secondary schools and classrooms, health care providers, and libraries should have access to advanced telecommunications services as described in subsection (h).

(7) ADDITIONAL PRINCIPLES.—Such other principles as the Joint Board and the Commission determine are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with this Act.

(c) DEFINITION.—

(1) IN GENERAL.—Universal service is an evolving level of telecommunications services that the Commission shall establish periodically under this section, taking into account advances in telecommunications and information technologies and services. The Joint Board in recommending, and the Commission in establishing, the definition of the services that are supported by Federal universal service support mechanisms shall consider the extent to which such telecommunications services—

(A) are essential to education, public health, or public safety;

(B) have, through the operation of market choices by customers, been subscribed to by a substantial majority of residential customers;

(C) are being deployed in public telecommunications networks by telecommunications carriers; and

(D) are consistent with the public interest, convenience, and necessity.

(2) ALTERATIONS AND MODIFICATIONS.—The Joint Board may, from time to time, recommend to the Commission modifications in the definition of the services that are supported by Federal universal service support mechanisms.

(3) SPECIAL SERVICES.—In addition to the services included in the definition of universal service under paragraph (1), the Commission may designate additional services for such support mechanisms for schools, libraries, and health care providers for the purposes of subsection (h).

(d) TELECOMMUNICATIONS CARRIER CONTRIBUTION.—Every telecommunications carrier that provides interstate telecommunications services shall contribute, on an equitable and nondiscriminatory basis, to the specific, predictable, and sufficient mechanisms established by the Commission to preserve and advance universal service. The Commission may exempt a carrier or class of carriers from this requirement if the carrier's telecommunications activities are limited to such an extent that the level of such carrier's contribution to the preservation and advancement of universal service would be de minimis. Any other provider of interstate telecommunications may be required to contribute to the preservation and advancement of universal service if the public interest so requires.

(e) UNIVERSAL SERVICE SUPPORT.—After the date on which Commission regulations implementing this section take effect, only an eligible telecommunications carrier designated under section 214(e) shall be eligible to receive specific Federal universal service support. A carrier that receives such support shall use that support only for the provision, maintenance, and upgrading of facilities and services for which the support is intended. Any such support should be explicit and sufficient to achieve the purposes of this section.

(f) STATE AUTHORITY.—A State may adopt regulations not inconsistent with the Commission's rules to preserve and advance universal service. Every telecommunications carrier that provides intrastate telecommunications services shall contribute, on an equitable and nondiscriminatory basis, in a manner determined by the State to the preservation and advancement of universal service in that State. A State may adopt regulations to provide for additional definitions and standards to preserve and advance universal service within that State only to the extent that such regulations adopt additional specific, predictable, and sufficient mechanisms to support such definitions or standards that do not rely on or burden Federal universal service support mechanisms.

(g) INTEREXCHANGE AND INTERSTATE SERVICES.—Within 6 months after the date of enactment of the Telecommunications Act of 1996, the Commission shall adopt rules to require that the rates charged by providers of interexchange telecommunications services to subscribers in rural and high cost areas shall be no higher than the rates charged by each such provider to its subscribers in urban areas. Such rules shall also require that a provider of interstate interexchange telecommunications services shall provide such services to its subscribers in each State at rates no higher than the rates charged to its subscribers in any other State.

(h) TELECOMMUNICATIONS SERVICES FOR CERTAIN PROVIDERS.—

(1) IN GENERAL.—

(A) HEALTH CARE PROVIDERS FOR RURAL AREAS.—A telecommunications carrier shall, upon receiving a bona fide request, provide telecommunications services which are necessary for the provision of health care services in a State, including instruction relating to such services, to any public or nonprofit health care provider that serves persons who reside in rural areas in that State at rates that are reasonably comparable to rates charged for similar services in urban areas in that State. A telecommunications carrier providing service under this paragraph shall be entitled to have an amount equal to the difference, if any, between the rates for services provided to health care providers for rural areas in a State and the rates for similar services provided to other customers in comparable rural areas in that State treated as a service obligation as a part of its obligation to participate in the mechanisms to preserve and advance universal service.

(B) EDUCATIONAL PROVIDERS AND LIBRARIES.—All telecommunications carriers serving a geographic area shall, upon a bona fide request for any of its services that are within the definition of universal service under subsection (c)(3), provide such services to elementary schools, secondary schools, and libraries for educational purposes at rates less than the amounts charged for similar services to other parties. The discount shall be an amount that the Commission, with respect to interstate services, and the States, with respect to intrastate services, determine is appropriate and necessary to ensure affordable access to and use of such services by such entities. A telecommunications carrier providing service under this paragraph shall—

(i) have an amount equal to the amount of the discount treated as an offset to its obligation to contribute to the mechanisms to preserve and advance universal service, or

(ii) notwithstanding the provisions of subsection (e) of this section, receive reimbursement utilizing the support mechanisms to preserve and advance universal service.

(2) ADVANCED SERVICES.—The Commission shall establish competitively neutral rules—

(A) to enhance, to the extent technically feasible and economically reasonable, access to advanced telecommunications and information services for all public and nonprofit elementary and secondary school classrooms, health care providers, and libraries; and

(B) to define the circumstances under which a telecommunications carrier may be required to connect its network to such public institutional telecommunications users.

(3) TERMS AND CONDITIONS.—Telecommunications services and network capacity provided to a public institutional telecommunications user under this subsection may not be sold, resold, or otherwise transferred by such user in consideration for money or any other thing of value.

(4) ELIGIBILITY OF USERS.—No entity listed in this subsection shall be entitled to preferential rates or treatment as required by this subsection, if such entity operates as a for-profit business, is a school described in paragraph (7)(A) with an endowment of more than $50,000,000, or is a library or library consortium not eligible for assistance from a State library administrative agency under the Library Services and Technology Act.

(5) REQUIREMENTS FOR CERTAIN SCHOOLS WITH COMPUTERS HAVING INTERNET ACCESS.—

(A) INTERNET SAFETY.—

(i) IN GENERAL.— Except as provided in clause (ii), an elementary or secondary school having computers with Internet access may not receive services at discount rates under paragraph (1)(B) unless the school, school board, local educational agency, or other authority with responsibility for administration of the school—

(I) submits to the Commission the certifications described in subparagraphs (B) and (C);

(II) submits to the Commission a certification that an Internet safety policy has been adopted and implemented for the school under subsection (l); and

(III) ensures the use of such computers in accordance with the certifications.

(ii) APPLICABILITY.— The prohibition in clause (i) shall not apply with respect to a school that receives services at discount rates under paragraph (1)(B) only for purposes other than the provision of Internet access, Internet service, or internal connections.

(iii) PUBLIC NOTICE; HEARING.— An elementary or secondary school described in clause (i), or the school board, local educational agency, or other authority with responsibility for administration of the school, shall provide reasonable public notice and hold at least 1 public hearing or meeting to address the proposed Internet safety policy. In the case of an elementary or secondary school other than an elementary or secondary school as defined in section 14101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 8801), the notice and hearing required by this clause may be limited to those members of the public with a relationship to the school.

(B) CERTIFICATION WITH RESPECT TO MINORS.— A certification under this subparagraph is a certification that the school, school board, local educational agency, or other authority with responsibility for administration of the school—

(i) 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 of its computers with Internet access that protects against access through such computers to visual depictions that are—

(I) obscene;
(II) child pornography; or
(III) harmful to minors; [and]

(ii) is enforcing the operation of such technology protection measure during any use of such computers by [minors.] *minors; and*

(iii) as part of its Internet safety policy is educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

(C) CERTIFICATION WITH RESPECT TO ADULTS.—A certification under this paragraph is a certification that the school, school board, local educational agency, or other authority with responsibility for administration of the school—

(i) is enforcing a policy of Internet safety 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—

(I) obscene; or
(II) child pornography; and

(ii) is enforcing the operation of such technology protection measure during any use of such computers.

(D) DISABLING DURING ADULT USE.—An administrator, supervisor, or other person authorized by the certifying authority under subparagraph (A)(i) may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose.

(E) TIMING OF IMPLEMENTATION.—

(i) IN GENERAL.—Subject to clause (ii) in the case of any school covered by this paragraph as of the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certification under subparagraphs (B) and (C) shall be made—

(I) with respect to the first program funding year under this subsection following such effective date, not later than 120 days after the beginning of such program funding year; and

(II) with respect to any subsequent program funding year, as part of the application process for such program funding year.

(ii) PROCESS.—

(I) SCHOOLS WITH INTERNET SAFETY POLICY AND TECHNOLOGY PROTECTION MEASURES IN PLACE.—A school covered by clause (i) that has in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C) shall certify its compliance with subparagraphs (B) and (C) during each annual program application cycle under this subsection, except that with respect to the first program funding year after the

effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certifications shall be made not later than 120 days after the beginning of such first program funding year.

(II) SCHOOLS WITHOUT INTERNET SAFETY POLICY AND TECHNOLOGY PROTECTION MEASURES IN PLACE.—A school covered by clause (i) that does not have in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C)—

(aa) for the first program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is undertaking such actions, including any necessary procurement procedures, to put in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C); and

(bb) for the second program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is in compliance with subparagraphs (B) and (C).

Any school that is unable to certify compliance with such requirements in such second program year shall be ineligible for services at discount rates or funding in lieu of services at such rates under this subsection for such second year and all subsequent program years under this subsection, until such time as such school comes into compliance with this paragraph.

(III) WAIVERS.—Any school subject to subclause (II) that cannot come into compliance with subparagraphs (B) and (C) in such second year program may seek a waiver of subclause (II)(bb) if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by such subclause. A school, school board, local educational agency, or other authority with responsibility for administration of the school shall notify the Commission of the applicability of such subclause to the school. Such notice shall certify that the school in question will be brought into compliance before the start of the third program year after the effective date of this subsection in which the school is applying for funds under this subsection.

(F) NONCOMPLIANCE.—

(i) FAILURE TO SUBMIT CERTIFICATION.—Any school that knowingly fails to comply with the application guidelines regarding the annual submission of certifi-

cation required by this paragraph shall not be eligible for services at discount rates or funding in lieu of services at such rates under this subsection.

(ii) FAILURE TO COMPLY WITH CERTIFICATION.—Any school that knowingly fails to ensure the use of its computers in accordance with a certification under subparagraphs (B) and (C) shall reimburse any funds and discounts received under this subsection for the period covered by such certification.

(iii) REMEDY OF NONCOMPLIANCE.—

(I) FAILURE TO SUBMIT.—A school that has failed to submit a certification under clause (i) may remedy the failure by submitting the certification to which the failure relates. Upon submittal of such certification, the school shall be eligible for services at discount rates under this subsection.

(II) FAILURE TO COMPLY.—A school that has failed to comply with a certification as described in clause (ii) may remedy the failure by ensuring the use of its computers in accordance with such certification. Upon submittal to the Commission of a certification or other appropriate evidence of such remedy, the school shall be eligible for services at discount rates under this subsection.

(6) REQUIREMENTS FOR CERTAIN LIBRARIES WITH COMPUTERS HAVING INTERNET ACCESS.—

(A) INTERNET SAFETY.—

(i) IN GENERAL.—Except as provided in clause (ii), a library having one or more computers with Internet access may not receive services at discount rates under paragraph (1)(B) unless the library—

(I) submits to the Commission the certifications described in subparagraphs (B) and (C); and

(II) submits to the Commission a certification that an Internet safety policy has been adopted and implemented for the library under subsection (l); and

(III) ensures the use of such computers in accordance with the certifications.

(ii) APPLICABILITY.—The prohibition in clause (i) shall not apply with respect to a library that receives services at discount rates under paragraph (1)(B) only for purposes other than the provision of Internet access, Internet service, or internal connections.

(iii) PUBLIC NOTICE; HEARING.—A library described in clause (i) shall provide reasonable public notice and hold at least 1 public hearing or meeting to address the proposed Internet safety policy.

(B) CERTIFICATION WITH RESPECT TO MINORS.—A certification under this subparagraph is a certification that the library—

(i) is enforcing a policy of Internet safety 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—

(I) obscene;

(II) child pornography; or

(III) harmful to minors; and

(ii) is enforcing the operation of such technology protection measure during any use of such computers by minors.

(C) CERTIFICATION WITH RESPECT TO ADULTS.—A certification under this paragraph is a certification that the library—

(i) is enforcing a policy of Internet safety 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—

(I) obscene; or

(II) child pornography; and

(ii) is enforcing the operation of such technology protection measure during any use of such computers.

(D) DISABLING DURING ADULT USE.—An administrator, supervisor, or other person authorized by the certifying authority under subparagraph (A)(i) may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose.

(E) TIMING OF IMPLEMENTATION.—

(i) IN GENERAL.—Subject to clause (ii) in the case of any library covered by this paragraph as of the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act [note to this section], the certification under subparagraphs (B) and (C) shall be made—

(I) with respect to the first program funding year under this subsection following such effective date, not later than 120 days after the beginning of such program funding year; and

(II) with respect to any subsequent program funding year, as part of the application process for such program funding year.

(ii) PROCESS.—

(I) LIBRARIES WITH INTERNET SAFETY POLICY AND TECHNOLOGY PROTECTION MEASURES IN PLACE.—A library covered by clause (i) that has in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C) shall certify its compliance with subparagraphs (B) and (C) during each annual program application cycle under this subsection, except that with respect to the first program funding year after the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certifications shall be made not

later than 120 days after the beginning of such first program funding year.

(II) LIBRARIES WITHOUT INTERNET SAFETY POLICY AND TECHNOLOGY PROTECTION MEASURES IN PLACE.—A library covered by clause (i) that does not have in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C)—

(aa) for the first program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is undertaking such actions, including any necessary procurement procedures, to put in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C); and

(bb) for the second program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is in compliance with subparagraphs (B) and (C).

Any library that is unable to certify compliance with such requirements in such second program year shall be ineligible for services at discount rates or funding in lieu of services at such rates under this subsection for such second year and all subsequent program years under this subsection, until such time as such library comes into compliance with this paragraph.

(III) WAIVERS.—Any library subject to subclause (II) that cannot come into compliance with subparagraphs (B) and (C) in such second year may seek a waiver of subclause (II)(bb) if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by such subclause. A library, library board, or other authority with responsibility for administration of the library shall notify the Commission of the applicability of such subclause to the library. Such notice shall certify that the library in question will be brought into compliance before the start of the third program year after the effective date of this subsection in which the library is applying for funds under this subsection.

(F) NONCOMPLIANCE.—

(i) FAILURE TO SUBMIT CERTIFICATION.—Any library that knowingly fails to comply with the application guidelines regarding the annual submission of certification required by this paragraph shall not be eligible for services at discount rates or funding in lieu of services at such rates under this subsection.

(ii) FAILURE TO COMPLY WITH CERTIFICATION.—Any library that knowingly fails to ensure the use of its computers in accordance with a certification under subparagraphs (B) and (C) shall reimburse all funds and discounts received under this subsection for the period covered by such certification.

(iii) REMEDY OF NONCOMPLIANCE.—

(I) FAILURE TO SUBMIT.—A library that has failed to submit a certification under clause (i) may remedy the failure by submitting the certification to which the failure relates. Upon submittal of such certification, the library shall be eligible for services at discount rates under this subsection.

(II) FAILURE TO COMPLY.—A library that has failed to comply with a certification as described in clause (ii) may remedy the failure by ensuring the use of its computers in accordance with such certification. Upon submittal to the Commission of a certification or other appropriate evidence of such remedy, the library shall be eligible for services at discount rates under this subsection.

(7) DEFINITIONS.—For purposes of this subsection:

(A) ELEMENTARY AND SECONDARY SCHOOLS.—The term "elementary and secondary schools" means elementary schools and secondary schools, as defined in section 9101 of the Elementary and Secondary Education Act of 1965.

(B) HEALTH CARE PROVIDER.—The term "health care provider" means—

(i) post-secondary educational institutions offering health care instruction, teaching hospitals, and medical schools;

(ii) community health centers or health centers providing health care to migrants;

(iii) local health departments or agencies;

(iv) community mental health centers;

(v) not-for-profit hospitals;

(vi) rural health clinics; and

(vii) consortia of health care providers consisting of one or more entities described in clauses (i) through (vi).

(C) PUBLIC INSTITUTIONAL TELECOMMUNICATIONS USER.—The term "public institutional telecommunications user" means an elementary or secondary school, a library, or a health care provider as those terms are defined in this paragraph.

(D) MINOR.—The term "minor" means any individual who has not attained the age of 17 years.

(E) OBSCENE.—The term "obscene" has the meaning given such term in section 1460 of title 18, United States Code.

(F) CHILD PORNOGRAPHY.—The term "child pornography" has the meaning given such term in section 2256 of title 18, United States Code.

(G) HARMFUL TO MINORS.—The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that—

(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

(ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

(H) SEXUAL ACT; SEXUAL CONTACT.—The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

(I) TECHNOLOGY PROTECTION MEASURE.—The term "technology protection measure" means a specific technology that blocks or filters Internet access to the material covered by a certification under paragraph (5) or (6) to which such certification relates.

(i) CONSUMER PROTECTION.—The Commission and the States should ensure that universal service is available at rates that are just, reasonable, and affordable.

(j) LIFELINE ASSISTANCE.—Nothing in this section shall affect the collection, distribution, or administration of the Lifeline Assistance Program provided for by the Commission under regulations set forth in section 69.117 of title 47, Code of Federal Regulations, and other related sections of such title.

(k) SUBSIDY OF COMPETITIVE SERVICES PROHIBITED.—A telecommunications carrier may not use services that are not competitive to subsidize services that are subject to competition. The Commission, with respect to interstate services, and the States, with respect to intrastate services, shall establish any necessary cost allocation rules, accounting safeguards, and guidelines to ensure that services included in the definition of universal service bear no more than a reasonable share of the joint and common costs of facilities used to provide those services.

(l) INTERNET SAFETY POLICY REQUIREMENT FOR SCHOOLS AND LIBRARIES.—

(1) IN GENERAL.—In carrying out its responsibilities under subsection (h), each school or library to which subsection (h) applies shall—

(A) adopt and implement an Internet safety policy that addresses—

(i) access by minors to inappropriate matter on the Internet and World Wide Web;

(ii) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

(iii) unauthorized access, including so-called "hacking", and other unlawful activities by minors online;

(iv) unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and

(v) measures designed to restrict minors' access to materials harmful to minors; and

(B) provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy.

(2) LOCAL DETERMINATION OF CONTENT.—A determination regarding what matter is inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination. No agency or instrumentality of the United States Government may—

(A) establish criteria for making such determination;

(B) review the determination made by the certifying school, school board, local educational agency, library, or other authority; or

(C) consider the criteria employed by the certifying school, school board, local educational agency, library, or other authority in the administration of subsection (h)(1)(B).

(3) AVAILABILITY FOR REVIEW.—Each Internet safety policy adopted under this subsection shall be made available to the Commission, upon request of the Commission, by the school, school board, local educational agency, library, or other authority responsible for adopting such Internet safety policy for purposes of the review of such Internet safety policy by the Commission.

(4) EFFECTIVE DATE.—This subsection shall apply with respect to schools and libraries on or after the date that is 120 days after the date of the enactment of the Children's Internet Protection Act.

* * * * * * *

SEC. 503. FORFEITURES

[47 U.S.C. 503]

(a) REBATES AND OFFSETS.—Any person who shall deliver messages for interstate or foreign transmission to any carrier, or for whom as sender or receiver, any such carrier shall transmit any interstate or foreign wire or radio communication, who shall knowingly by employee, agent, officer, or otherwise, directly or indirectly, by or through any means or device whatsoever, receive or accept from such common carrier any sum of money or any other valuable consideration as a rebate or offset against the regular charges for transmission of such messages as fixed by the schedules of charges provided for in this Act, shall in addition to any other penalty provided by this Act forfeit to the United States a sum of money three times the value of any other consideration so received or accepted, to be ascertained by the trial court; and in the trial of said action all such rebates or other considerations so received or accepted for a period of six years prior to the commencement of the action, may be included therein, and the amount recovered shall be three times the total amount of money, or three times the total value of such consideration, so received or accepted, or both, as the case may be.

(b) ACTIVITIES CONSTITUTING VIOLATIONS AUTHORIZING IMPOSITION OF FORFEITURE PENALTY; AMOUNT OF PENALTY; PROCEDURES

APPLICABLE; PERSONS SUBJECT TO PENALTY; LIABILITY EXEMPTION PERIOD.—

(1) Any person who is determined by the Commission, in accordance with paragraph (3) or (4) of this subsection, to have—

(A) willfully or repeatedly failed to comply substantially with the terms and conditions of any license, permit, certificate, or other instrument or authorization issued by the Commission;

(B) willfully or repeatedly failed to comply with any of the provisions of this Act or of any rule, regulation, or order issued by the Commission under this Act or under any treaty, convention, or other agreement to which the United States is a party and which is binding upon the United States;

(C) violated any provision of section 317(c) or 508(a) of this Act; **[**or**]**

(D) violated any provision of section 1304, 1343, **[**or 1464**]** *1464, or 2252* of title 18, United States Code; *or*

(E) violated any provision of section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

shall be liable to the United States for a forfeiture penalty. A forfeiture penalty under this subsection shall be in addition to any other penalty provided for by this Act; except that this subsection shall not apply to any conduct which is subject to forfeiture under title II, part II or III of title III, or section 506 of this Act.

(2)(A) If the violator is (i) a broadcast station licensee or permittee, (ii) a cable television operator, or (iii) an applicant for any broadcast or cable television operator license, permit, certificate, or other instrument or authorization issued by the Commission, the amount of any forfeiture penalty determined under this section shall not exceed $25,000 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $250,000 for any single act or failure to act described in paragraph (1) of this subsection.

(B) If the violator is a common carrier subject to the provisions of this Act or an applicant for any common carrier license, permit, certificate, or other instrument of authorization issued by the Commission, the amount of any forfeiture penalty determined under this subsection shall not exceed $100,000 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,000,000 for any single act or failure to act described in paragraph (1) of this subsection.

(C) Notwithstanding subparagraph (A), if the violator is—

(i) (I) a broadcast station licensee or permittee; or

(II) an applicant for any broadcast license, permit, certificate, or other instrument or authorization issued by the Commission; and

(ii) determined by the Commission under paragraph (1) to have broadcast obscene, indecent, or profane language, the amount of any forfeiture penalty determined under this subsection shall not exceed $325,000

for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $3,000,000 for any single act or failure to act.

(D) In any case not covered in subparagraph (A), (B), or (C), the amount of any forfeiture penalty determined under this subsection shall not exceed $10,000 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $75,000 for any single act or failure to act described in paragraph (1) of this subsection.

(E) The amount of such forfeiture penalty shall be assessed by the Commission, or its designee, by written notice. In determining the amount of such a forfeiture penalty, the Commission or its designee shall take into account the nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require.

(3)(A) At the discretion of the Commission, a forfeiture penalty may be determined against a person under this subsection after notice and an opportunity for a hearing before the Commission or an administrative law judge thereof in accordance with section 554 of title 5, United States Code. Any person against whom a forfeiture penalty is determined under this paragraph may obtain review thereof pursuant to section 402(a).

(B) If any person fails to pay an assessment of a forfeiture penalty determined under subparagraph (A) of this paragraph, after it has become a final and unappealable order or after the appropriate court has entered final judgment in favor of the Commission, the Commission shall refer the matter to the Attorney General of the United States, who shall recover the amount assessed in any appropriate district court of the United States. In such action, the validity and appropriateness of the final order imposing the forfeiture penalty shall not be subject to review.

(4) Except as provided in paragraph (3) of this subsection, no forfeiture penalty shall be imposed under this subsection against any person unless and until—

(A) the Commission issues a notice of apparent liability, in writing, with respect to such person;

(B) such notice has been received by such person, or until the Commission has sent such notice to the last known address of such person, by registered or certified mail; and

(C) such person is granted an opportunity to show, in writing, within such reasonable period of time as the Commission prescribes by rule or regulation, why no such forfeiture penalty should be imposed.

Such a notice shall (i) identify each specific provision, term, and condition of any Act, rule, regulation, order, treaty, convention, or other agreement, license, permit, certificate, instrument, or authorization which such person apparently violated or with which such person apparently failed to comply; (ii) set

forth the nature of the act or omission charged against such person and the facts upon which such charge is based; and (iii) state the date on which such conduct occurred. Any forfeiture penalty determined under this paragraph shall be recoverable pursuant to section 504(a) of this Act.

(5) No forfeiture liability shall be determined under this subsection against any person, if such person does not hold a license, permit, certificate, or other authorization issued by the Commission, and if such person is not an applicant for a license, permit, certificate, or other authorization issued by the Commission, unless, prior to the notice required by paragraph (3) of this subsection or the notice of apparent liability required by paragraph (4) of this subsection, such person (A) is sent a citation of the violation charged; (B) is given a reasonable opportunity for a personal interview with an official of the Commission, at the field office of the Commission which is nearest to such person's place of residence; and (C) subsequently engages in conduct of the type described in such citation. The provisions of this paragraph shall not apply, however, if the person involved is engaging in activities for which a license, permit, certificate, or other authorization is required, or is a cable television system operator, if the person involved is transmitting on frequencies assigned for use in a service in which individual station operation is authorized by rule pursuant to section 307(e), or in the case of violations of section 303(q), if the person involved is a nonlicensee tower owner who has previously received notice of the obligations imposed by section 303(q) from the Commission or the permittee or licensee who uses that tower. Whenever the requirements of this paragraph are satisfied with respect to a particular person, such person shall not be entitled to receive any additional citation of the violation charged, with respect to any conduct of the type described in the citation sent under this paragraph.

(6) No forfeiture penalty shall be determined or imposed against any person under this subsection if—

(A) such person holds a broadcast station license issued under title III of this Act and if the violation charged occurred—

(i) more than 1 year prior to the date of issuance of the required notice or notice of apparent liability; or

(ii) prior to the date of commencement of the current term of such license, whichever is earlier; or

(B) such person does not hold a broadcast station license issued under title III of this Act and if the violation charged occurred more than 1 year prior to the date of issuance of the required notice or notice of apparent liability.

For purposes of this paragraph, "date of commencement of the current term of such license" means the date of commencement of the last term of license for which the licensee has been granted a license by the Commission. A separate license term shall not be deemed to have commenced as a result of continuing a license in effect under section 307(c) pending decision on an application for renewal of the license.

[42 U.S.C. 13032]

SEC. 227. REPORTING OF CHILD PORNOGRAPHY BY ELECTRONIC COMMUNICATION SERVICE PROVIDERS.

(a) DEFINITIONS.—In this section—

(1) the term "electronic communication service" has the meaning given the term in section 2510 of title 18, United States Code; and

(2) the term "remote computing service" has the meaning given the term in section 2711 of title 18, United States Code.

(b) REQUIREMENTS.—

(1) DUTY TO REPORT.—Whoever, while engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce, obtains knowledge of facts or circumstances from which a violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 of title 18, United States Code, involving child pornography (as defined in section 2256 of that title), or a violation of section 1466A of that title, is apparent, shall, as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children, which shall forward that report to ⟦a law enforcement agency⟧ *appropriate Federal, State, or foreign law enforcement agencies* or agencies designated by the Attorney General.

(2) DESIGNATION OF AGENCIES.—Not later than 180 days after the date of enactment of this section, the Attorney General shall designate the *Federal, State, or foreign* law enforcement agency or agencies to which a report shall be forwarded under paragraph (1).

(3) CONTENTS OF REPORT.—To the extent this information is reasonably available to an electronic communication service provider or a remote computing service provider, each report under paragraph (1) shall include—

(A) information relating to the Internet identity of any individual who appears to have violated any section of title 18, United States Code, referenced in paragraph (1), including any relevant user ID or other online identifier, electronic mail addresses, website address, uniform resource locator, or other identifying information;

(B) information relating to when any apparent child pornography was uploaded, transmitted, reported to, or discovered by the electronic communication service provider or a remote computing service provider, as the case may be, including a date and time stamp and time zone.

(C) information relating to geographic location of the involved individual or reported content, including the hosting website, uniform resource locator, street address, zip code, area code, telephone number, or Internet Protocol address;

(D) any image of any apparent child pornography relating to the incident, and any images commingled with images of apparent child pornography, such report is regarding; and

(E) accurate contact information for the electronic communication service provider or remote computing service provider making the report, including the address, telephone number, facsimile number, electronic mail address of, and individual point of contact for such electronic communication service provider or remote computing service provider.

[(3)] (4) In addition to forwarding such reports to those agencies designated in subsection (b)(2), the National Center for Missing and Exploited Children is authorized to forward any such report to an appropriate official of a state or subdivision of a state for the purpose of enforcing state criminal [law.] law, or appropriate officials of foreign law enforcement agencies designated by the Attorney General for the purpose of enforcing State or Federal laws of the United States.

[(4)] (5) FAILURE TO REPORT.—A provider of electronic communication services or remote computing services described in paragraph (1) who knowingly and willfully fails to make a report under that paragraph shall be fined—

(A) in the case of an initial failure to make a report, not more than [$50,000;] $150,000; and

(B) in the case of any second or subsequent failure to make a report, not more than [$100,000.] $300,000.

(c) CIVIL LIABILITY.—No provider or user of an electronic communication service or a remote computing service to the public shall be held liable on account of any action taken in good faith to comply with or pursuant to this section.

(d) LIMITATION OF INFORMATION OR MATERIAL REQUIRED IN REPORT.—A report under subsection (b)(1) may include additional information or material developed by an electronic communication service or remote computing service, except that the Federal Government may not require the production of such information or material in that report.

(e) MONITORING NOT REQUIRED.—Nothing in this section may be construed to require a provider of electronic communication services or remote computing services to engage in the monitoring of any user, subscriber, or customer of that provider, or the content of any communication of any such person.

(f) CONDITIONS OF DISCLOSURE OF INFORMATION CONTAINED WITHIN REPORT.—

(1) IN GENERAL.—No law enforcement agency that receives a report under subsection (b)(1) shall disclose any information contained in that report, except that disclosure of such information may be made—

(A) to an attorney for the government for use in the performance of the official duties of the attorney;

(B) to such officers and employees of the law enforcement agency, as may be necessary in the performance of their investigative and recordkeeping functions;

(C) to such other government personnel (including personnel of a State or subdivision of a State) as are determined to be necessary by an attorney for the government to assist the attorney in the performance of the official duties of the attorney in enforcing Federal criminal law; or

(D) where the report discloses a violation of State criminal law, to an appropriate official of a State or subdivision of a State for the purpose of enforcing such State law.

(2) DEFINITIONS.—In this subsection, the terms "attorney for the government" and "State" have the meanings given those terms in Rule 54 of the Federal Rules of Criminal Procedure.

(g) LIMITATION ON LIABILITY.—

(1) IN GENERAL.—Except as provided in paragraphs (2) and (3), the National Center for Missing and Exploited Children, including any of its directors, officers, employees, or agents, is not liable in any civil or criminal action arising from the performance of its CyberTipline responsibilities and functions, as defined by this section, section 404 of the Missing Children's Assistance Act (42 U.S.C. 5773), or from its efforts to identify child victims.

(2) INTENTIONAL, RECKLESS, OR OTHER MISCONDUCT.—Paragraph (1) does not apply in an action in which a party proves that the National Center for Missing and Exploited Children, or its officer, employee, or agent as the case may be, engaged in intentional misconduct or acted, or failed to act, with actual malice, with reckless disregard to a substantial risk of causing injury without legal justification, or for a purpose unrelated to the performance of responsibilities or functions under this section.

(3) ORDINARY BUSINESS ACTIVITIES.—Paragraph (1) does not apply to an act or omission related to an ordinary business activity, such as an activity involving general administration or operations, the use of motor vehicles, or personnel management.

(h) USE OF INFORMATION TO COMBAT CHILD PORNOGRAPHY.—The National Center for Missing and Exploited Children is authorized to provide elements relating to any image or other relevant information reported to its Cyber Tip Line to an electronic communication service provider or a remote computing service provider for the sole and exclusive purpose of permitting that electronic communication service provider or remote computing service provider to stop the further transmission of images and develop anti-child pornography technologies and related industry best practices. Any electronic communication service provider or remote computing service provider that receives information from the National Center for Missing and Exploited Children under this subsection may use such information only for the purposes described in this subsection.

○