Section 2 Preface

The Electronic Frontier Foundation (EFF) and the Online Policy Group (OPG) are studying Internet blocking software for the following reasons:

- No organization has studied effectively and quantitatively the issue of student Internet access within public schools that operate Internet blocking software. [10]
- The Children's Internet Protection Act (CIPA) requires use of a "technology protection measure" such as Internet blocking software in all schools that receive certain federal funds or discounts. [24]
- Inappropriate censorship negatively impacts educational opportunities. [13]
- Safety of educational communities and individuals online is critical to a productive educational environment.

Since their inception, EFF and OPG have made clear and deliberate strides to preserve civil liberties despite clashes between technological advancements and legal developments. Both these organizations strive to establish policy that best serves the community by careful analysis of the legal and technical landscape.

The percentage of children who use the Internet has increased steadily in the recent past, and various organizations and members of the public have expressed concern about illegal obscene, child pornographic, or harmful to minors materials. Congress passed a series of legislation, including the Communications Decency Act (CDA), the Child Online Protection Act (COPA), and the Children's Internet Protection Act (CIPA), which attempted to address this concern. [24] [23] [22] CIPA is particularly relevant since it focuses on blocking of Internet use in schools and because, while U.S. courts have struck the relevant portions of CDA and COPA, they have not yet ruled CIPA unconstitutional in the context of schools. [26] [27] [28]

The Children's Internet Protection Act

The Children's Internet Protection Act of 2000, was passed by Congress and signed by President Clinton:

> To require the installation and use by schools and libraries of a technology for filtering or blocking material on the Internet on computers with Internet access to be eligible to receive or retain universal service assistance

CIPA Provisions

This section outlines the parts of CIPA particularly relevant to Internet blocking in schools, that is, CIPA §1702, §1711, and §1721.

Disclaimers

CIPA §1702 provides the following disclaimers related to effects of the law on Internet blocking beyond what is required by CIPA and on privacy concerns related to monitoring of Internet use:

> SEC. 1702. DISCLAIMERS.
>
> DISCLAIMER REGARDING CONTENT.--Nothing in this title or the amendments made by this title shall be construed to prohibit a local educational agency, elementary or secondary school, or library from blocking access on the Internet on computers owned or operated by that agency, school, or library to any content other than content covered by this title or the amendments made by this title.
>
> (b) DISCLAIMER REGARDING PRIVACY.--Nothing in this title or the amendments made by this title shall be construed to require the tracking of Internet use by any identifiable minor or adult user.

Internet Safety Policy and Technology Protection Measure

CIPA §1711 amends Title III of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 6801 et seq.) to require schools receiving certain federal funds or discounts to adopt and enforce an Internet use policy and technology protection measure preventing access to visual depictions that are obscene, child pornography or harmful to minors:

> SEC. 3601. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS.
>
> (a) INTERNET SAFETY.—
>
> (1) IN GENERAL.--No funds made available under this title to a local educational agency for an elementary or secondary school that does not receive services at discount rates under section 254(h)(5) of the Communications Act of 1934, as added by section 1721 of Children's Internet Protection Act, may be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet, for such school unless the school, school board, local educational agency, or other authority with responsibility for administration of such school both—
>
> (A)(i) has in place a policy of Internet safety 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—
>
> (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; and

(B)(i) has in place 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) MINOR.--The term 'minor' means an individual who has not attained the age of 17.

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

(F) 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.

(G) OBSCENE.--The term 'obscene' has the meaning given such term in section 1460 of title 18, United States Code.

(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.

CIPA §1721 amends the Communications Act of 1934 (47 U.S.C. 254(h)(5)) to require schools receiving certain federal funds or discounts to adopt and enforce an Internet use policy and technology protection measure preventing access to visual depictions that are obscene, child pornography or harmful to minors:

(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.

(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.

CIPA Litigation

On May 31, 2002, the U.S District Court for the Eastern District of Pennsylvania ruled in *United States of America v. American Library Assocation* (2002) against CIPA as it applied to public libraries because the court held the law violates the First Amendment [28]. The ruling concluded that Internet blocking software products operate as "blunt instruments" that are unable to block obscenity, child pornography, and other materials that are harmful to minors and still preserve access to constitutionally protected content. The court ruled that:

> …the library plaintiffs must prevail in their contention that CIPA requires them to violate the First Amendment rights of their patrons, and accordingly is facially invalid… In view of the limitations inherent in the filtering technology mandated by CIPA, any public library that adheres to CIPA's conditions will necessarily restrict patrons' access to a substantial amount of protected speech, in violation of the First Amendment.

Though providing relief for public libraries, the plaintiffs did not request and the court did not remove the requirement for public schools to install Internet blocking software in order to receive certain federal funding or discounts. The U.S government has already appealed even the library-related decision to the Supreme Court.

In the library case, the court relied on the constitutional limitations to Congress' spending clause power, citing *South Dakota v. Dole*, 483 U.S. 203 (1987) on violation of the constitutional rights of those receiving federal funding or discounts. The court concluded that restrictions on such funding and discounts for public libraries are subject to strict scrutiny, rather than just rational basis review because, as in *Reno v. ACLU*, 521 U.S 844, 868 (1997):

> …the more widely the state facilitates the dissemination of private speech in a given forum, the more vulnerable the state's decision is to restrict access to speech in that forum.

The court explains that:

> …provision of Internet access uniquely promotes First Amendment values in a manner analogous to traditional public for a such as streets, sidewalks, and parks, in which content-based restrictions are always subject to strict scrutiny.
>
> Under strict scrutiny, a public library's use of filtering software is permissible only if it is narrowly tailored to further a compelling government interest and no less restrictive alternative would serve that interest.

While acknowledging the government's legitimate interest in preventing access to visual depictions of obscenity, child pornography, or in the case of minors, material harmful to minors, the court found that there exist less restrictive alternatives, such as implementation and enforcement of Internet use policies, as well as optional Internet blocking, privacy screens, recessed monitors, and placement of unfiltered Internet terminals out of sight-lines for adults and "requiring parental consent to or presence during unfiltered access or restricting minors' unfiltered access to terminals within view of library staff."

Basically, the court declared CIPA unconstitutional for libraries because of the underblocking of visual depictions of obscenity, child pornography, or in the case of minors, material harmful to minors, and because of the overblocking of materials protected under the First Amendment of the U.S. Constitution.

It is unclear what effect such a ruling, if upheld by the U.S. Supreme Court, would have on a similar legal challenge brought in the school rather than the library setting.

Related Litigation and Legal Definitions

As interpreted by the U.S. judiciary system, the First Amendment of the U.S. Constitution does not protect illegal obscenity, child pornography, or—in the case of minors—harmful to minors content.

There is sometimes confusion over the legal definitions of illegally obscenity, child pornography, and harmful to minors materials.

Obscenity

CIPA uses the constitutional definition of obscenity set forth in *Miller v. California*, 413 U.S. 15 (1973), and codified at 18 U.S.C. 1460:

- Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;
- Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state or federal law to be obscene; and
- Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Child Pornography

CIPA uses the statutory definition of "child pornography" found in 18 U.S.C. 2256:

- "Any visual depiction" of a minor under 18 years old engaging in "sexually explicit conduct," which includes "actual or simulated" sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or "lascivious exhibition of the genitals or pubic area."

The U.S. Supreme Court has ruled in *Ashcroft v. Free Speech Coalition*, 122 S.Ct. 1389 (2002) that any activity not actually involving a minor cannot be child pornography.

Harmful to Minors

CIPA defines "harmful to minors" as:

> …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.

This harmful to minors definition is similar to the definition provided by *Ginsberg v. New York*, 390 U.S. 629 (1968).

As with CIPA, the *Ginsberg* case also defined a minor as under 17 years of age. *Ginsberg* also provided that parents may provide harmful to minors speech to their children, although according to the court that struck the library portions of CIPA, CIPA provides no such exception for parents to provide such materials to minors. [28] [21]

Other Content

The legal definitions provided in CIPA do not cover other types of content, such as chat, criminal skills, drugs, alcohol, or tobacco, electronic commerce, free pages, gambling, hacking, hate speech, violence, weapons, web-based email, and so on, which are blocking codes often used by Internet blocking software manufacturers in their products.

Students have a right to speak, even at school. In a case affirming the right of students to wear black armbands protesting the Vietnam War, the U.S. Supreme Court found that students who are minors "are 'persons' under our Constitution possessed of fundamental rights which the State must respect." *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503, 511 (1969). In another case, the Court found that minors have the right to receive information in public school libraries. *Board of Education, Island Trees Union Free School District No. 26 v. Pico*, 457 U.S. 853, 867, 872 (1982).

While minors' constitutional rights are weaker than adults' rights, minors' rights become stronger as they grow older. In a case involving minors' right to abortion, the Court said that "constitutional rights do not mature and come into being magically only when one

attains the state-defined age of majority." *Planned Parenthood of Central Missouri v. Danforth*, 428 U.S. 52, 74 (1976); see *Bellotti v. Baird*, 443 U.S. 622, 648 (1979) ("parental consent" abortion statute must contain procedure for minor to get abortion without parental consent or notice).

Indeed, "mature minors" arguably have a right to information despite their parents' wishes in the areas of reproductive health, sexually-transmitted diseases, contraception, and abortion. See *Doe v. Irwin*, 615 F.2d 1162, 1166 (6th Cir. 1980).

The courts also recognize the rights of parents and guardians to control much of their childrens' experience at schools. As EFF Senior Staff Attorney Lee Tien has written:

> …schools traditionally, and sometimes by statue, accommodate parental wishes as to their children's exposure to material in school. EFF therefore argues that parents enjoy at least as much right to insist that their children not be blocked from objectionable speech. Indeed, parents may have more right to opt out of blocking.

In recent years, school administrators have exerted greater control over speech in schools. For example, the U.S. Supreme Court decided to curtail student free speech rights and allow high school administrators greater liberty to censor student newspapers in *Hazelwood v. Kuhlmeier*, 484 U.S. 260 (1988). Nonetheless, Tien cites *Linmark Association v. Township of Willingsboro*, 431 U.S. 85, 96 (1977) and *Griswold v. Connecticut*, 381 U.S. 479, 482 (1965) which said that "the State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge." He also quotes the Ninth Circuit observation in *Monteiro v. Tempe Union High School District*, 158 F.3d 1022, 1031 (9th Cir. 1998):

> …that a student is required to read a book does not mean that he is being asked to agree with what is in it.…a necessary component of any education is learning to think critically about offensive ideas—without that ability one can do little to respond to them.

Board of Education, Island Trees Union Free School District No. 26 v. Pico, 457 U.S. 874 (1982) apparently indicates a requirement that schools have a First Amendment duty to inform parents about what books are banned in order to maintain censorship within constitutional limits. Suppression of information in school libraries must be based on "established, regular and facially unbiased procedures for the review of controversial materials." Any technological solution for blocking Internet content "must respect parental determinations of what their children may see or read, without subjecting either parent or child to undue burdens." [21] *Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965) suggests that schools may not put the burden on parents to opt out of blocking since the government may not impose affirmative obligations on one to receive information.

Impact on Schools

Parents, teachers, school administrators, and school boards can protect students from potentially harmful material more effectively if they implement Internet access in the schools with an understanding of the relevant law, research, and social and cultural implications of their decisions about whether and how to install Internet blocking software.