



Internet Filters In Schools And Libraries

©2009 eNotes.com, Inc. or its Licensors. Please see [copyright information](#) at the end of this document.

- [Background](#)
- [Filtering Restrictions](#)
- [State and Local Restrictions](#)
- [Additional Resources](#)
- [Organizations](#)

Background

Internet filters are software programs that control what is shown while a computer user is viewing pages on the World Wide Web. Emerging on the commercial market for home use in the mid-to-late 1990s, the filters are designed to protect minors from viewing [PORNOGRAPHY](#), hate speech, and other controversial online content. They work by intercepting and blocking attempts to view particular web pages and their controls cannot be disabled except by an administrator. Marketed primarily toward parents who wish to allow their children to surf the Internet without constant adult supervision, filters currently available include Cyber Patrol, Net Nanny, and Cyber Snoop.

Government interest in filters emerged after early, unsuccessful attempts to directly regulate Internet content. Prompted by the explosion of popularity in Internet usage in the early 1990s, lawmakers responded to public complaints about the accessibility of pornography. While such imagery represented only a small percentage of web sites, studies have shown it amounts to as little as 2%, Internet search engines made locating the material easy even for young people. Thus, unlike with printed material controlled at the point of sale in newsstands and bookstores, minors using the Internet could obtain or accidentally suffer exposure to hard core pornography. In an effort to combat this problem, Congress first sought to control what could be shown on web pages.

- The Communications Decency Act of 1996 (CDA) was passed to prohibit Internet users from communicating material that would be deemed offensive to minors under contemporary community standards. The controversial law carried fines and [IMPRISONMENT](#) for offenders, but enforcement was immediately blocked by a federal court. Attacked by critics as [CENSORSHIP](#), the law was later over-turned unanimously by the Supreme Court as an unconstitutional violation of the First Amendment in *Reno v. ACLU* in 1997.
- The Child Online Protection Act of 1998 (COPA) was passed to meet the objections of the Supreme Court to the CDA. The new law attempted to be more specific in order to overcome constitutional problems, this time targeting commercial purveyors of material deemed harmful to minors. However, in 1999, it, too, was immediately blocked by a court injunction, and subsequently a district court and federal appeals court both found the law unconstitutional because it would require every Web page to abide by the most restrictive community standards. The Supreme Court agreed to hear an appeal, *ACLU v. Ashcroft*, scheduled for 2002.
- When the courts proved unwilling to allow federal control of what was communicated, lawmakers pursued a new avenue. Internet filtering offered a mechanism by which the law could control what was received on publicly-funded computers connected to the Internet. In December 2000, Congress passed both the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection

Encyclopedia of Everyday Law: Internet Filters In Schools And Libraries

Act (Neighborhood Act), highly similar bills that were added to an appropriations measure, signed by President William J. Clinton and enacted as **PUBLIC LAW 106-554**. Together, the two acts place restrictions on Internet usage in public libraries and public schools that receive federal funding. For enforcement, the law employs a carrot and stick approach: continued computer and Internet funding depends upon libraries and schools using filtering software and, in some cases, establishing broader controls as part of a new, comprehensive Internet safety policy.

Federally-required Internet filtering in schools and libraries immediately proved as controversial as earlier congressional measures. In particular, critics argued that Internet filtering software is highly imprecise; it has the tendency to erroneously block harmless, non-pornographic material as well because it cannot determine the context in which the material it filters appears. As the law went into effect in Spring 2001, [LITIGATION](#) promptly followed. Separate lawsuits brought by the American Library Association (ALA) and another by a coalition including publishers and civil liberties groups challenged the law on First Amendment grounds similar to those brought successfully against the CDA and COPA. After a court found that both challenges have valid legal grounds to continue, trial was scheduled to begin in February 2002.

Filtering Restrictions

Institutions Affected

Public elementary and secondary schools and public libraries are required to certify annual compliance with the law if they wish to maintain eligibility for federal funding for computers and/or Internet access. The extent to which they are regulated depends upon what types of federal funding they already receive. There are three distinct federal programs that provide subsidies to institutions for Internet access, service, internal connections, and personal computers:

- Universal Service (E-rate) discounts for Internet access, Internet service, or internal connections.
- Library Services and Technology Act (LSTA) state grant funding to buy computers used to access the Internet or to pay direct Internet access costs.
- Title III funding under the Elementary and Secondary Education Act (ESEA) to buy computers used to access the Internet or to pay direct Internet access costs.

The libraries and schools that receive E-rate funding face the broadest range of new requirements, including installation of filters, public notification and participation, and other measures. The law governs all such federal funding, whether it is disbursed directly or through a state intermediary agency. However, it does not apply to academic or college libraries, which do not qualify for the types of federal funding in question.

Compliance

Lawmakers gave the Federal Communications Commission (FCC) regulatory authority over the law. In the broadest possible application of the rules for eligibility, institutions must meet three requirements:

- Adopt an Internet safety policy.
- Provide notice and hold at least one public meeting on the proposed Internet safety policy.
- Certify that they have adopted and implemented the policy, which must include Internet filters.

For eligibility for E-rate funding, institutions must meet all three requirements. However, those institutions receiving only LSTA or ESEA funding must only meet the filter requirement.

Internet Safety Policy

The Internet safety policy requirement covers five areas. It is designed to be a comprehensive policy governing Internet usage by minors in public schools and libraries and, as such, goes beyond the issue of filtering web pages. More broadly, libraries and schools must monitor several types of Internet usage. Under FCC rules, the policy must address five key areas.

- Access by minors to "inappropriate matter" on the Internet and the World Wide Web.
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
- Unauthorized access, including so-called "hacking," and other unlawful online activities by minors.
- Unauthorized disclosure, use, and dissemination of personal information regarding minors.
- Measures designed to restrict minors' access to materials harmful to minors.

Prior to adopting an Internet safety policy, schools and libraries must provide public notice of the process and hold at least one public [HEARING](#) or meeting on the proposed policy. The actual adopted policy must be available for review by the FCC.

Filtering

The Internet safety policy must include what the law defines as a "technology protection measure," i.e., a software filter or blocker that prevents the display of certain visual depictions, photographs, and illustrations. No particular brand of filter is required, however, but the filter must perform specific duties. It must govern Internet access by both adults and minors and block three types of visual depictions.

- **OBSCENITY.**
- Child pornography.
- Material that is "harmful to minors."

The law does not provide an express definition of obscenity. Under *Miller v. California* in 1973, the Supreme Court laid out its famous three-part "community standards" test now typically used to determine what is obscene. The test requires a court determination of three parts:

- 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.
- Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

The Internet law goes into some specific detail as to what constitutes material "harmful to minors," who are defined as anyone under the age of 17. It states that the term "means any picture, image, graphic image file, or other visual depiction" that has the following characteristics:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion.
- Depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals.
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Adults are not subject to the restrictions on material harmful to minors. Text on web pages is not regulated under the law like visual depictions are.

Encyclopedia of Everyday Law: Internet Filters In Schools And Libraries

The law makes a further distinction between what is "harmful" to minors and what is merely "inappropriate" for minors. While it carefully defines harmful material, it leaves the definition of inappropriate material up to local community control. The FCC declined to be more specific in this area in its rule-making capacity, instead leaving such definitions up to school boards, library boards, and other local authorities.

Disabling Filters

Under some circumstances, Internet filters may be legally disabled. While forbidding Internet users to disable the filters themselves, the law permits a school or library administrator to disable filtering software in order to allow bona fide research or other lawful use by an adult. However, the law does not specify what constitutes such usage. In its April 2001 rules, the FCC acknowledged criticism of this measure: libraries complained that the law's vagueness meant they would be required to spend considerable time determining the validity of each adult request for filter disabling. Nevertheless, the FCC here, too, declined to be more specific. The commission noted that prescribing rules would "have a chilling effect" on adults' Internet usage and "significantly impinge" on library staff time and resources. As such all libraries must develop their own policies.

Timetable

Congress and the FCC do not expect these changes to occur overnight. In each affected federal program, the law phases in its requirements over two years. For the first year, the deadline of October 28, 2001, was established for schools and libraries to certify that they are taking steps to put in place their Internet safety policy. In the second year, these institutions must demonstrate that their policies and the required filtering technology is in place. As such, some library patrons may not encounter filtering software until 2002 or later.

Enforcement

The law prescribes different types of enforcement. In each case, the responsible funding agencies must make determinations about compliance. For institutions receiving E-rate funding, failure to submit certification annually will result in ineligibility, and failure to comply with the law can result in institutions being suspended or required to reimburse funding. For those receiving funds under ESEA or LSTA programs, the responsible funding agency may withhold further payments, suspend the funding, or issue a complaint to compel compliance; recovery of funding is, however, specifically prohibited.

Complaints about an institution could lead to an agency finding that it is out of compliance. However, legal analysts are in doubt as to whether the law creates a cause of action—legal grounds that may serve as the basis for litigation—for citizens to sue institutions over failure to comply.

Expedited Legal Review

Foreseeing likely legal challenges to the law, Congress provided for any litigation contesting its constitutionality to receive expedited [JUDICIAL REVIEW](#) first by a three-judge federal appeals panel and, if necessary, by the Supreme Court.

State and Local Restrictions

Even before enactment of the 2000 federal law, five states had passed their own statutes. Nearly 20 states had some form of legislation under consideration in 2001. Most of these laws are directed at libraries, some at schools, and at least one mandates that no filters be used at all in public libraries.

Encyclopedia of Everyday Law: Internet Filters In Schools And Libraries

During the late 1990s, cities, counties, and library boards began enacting Internet usage policies that varied widely and often differed from community to community in the same state. Michigan demonstrates this variety. In Holland, Michigan, where the nation's first ballot measure on library Internet filters was held in February 2000, residents of the 32,000-strong city voted 55 percent to 45 percent against the proposal, despite heavy spending by proponents such as the American Family Association in a controversial political battle that attracted national attention. Nearby Georgetown Township, which is slightly larger, installed filters. And then later in the year, the state enacted a law requiring filters, rendering local differences moot.

For the nation's nearly 9,000 public libraries, the issue is still clearly unsettled. Some had already begun installing filters independently in the late 1990s, and the American Library Association estimated that as many as 25 percent had done so by 2001. However, most had resisted filtering. The ALA reported that many had adopted resolutions similar to its 1997 anti-filtering declaration, which holds that federally-mandated filtering is unconstitutional and violates the organization's Library **BILL OF RIGHTS**. For thousands of libraries, the ALA's pending litigation against the federal filtering law is closely watched and will ultimately shape future policies.

In two cases, filtering advocates have lost legal challenges. In 1998, in *Mainstream Loudoun V. Board of Trustees of Loudoun County*, a federal district court in Virginia ruled that a library violated the First Amendment by using filtering software. In 2001, a California federal appeals court upheld a ruling that rejected a parent's lawsuit against a library where her 12-year-old son downloaded sexually-explicit photos on the library's Internet connection. The court in *Kathleen R. v. City of Livermore* held that the city is not subject to suit for damages, nor could it be forced to censor the Internet usage of its library patrons.

Not all legal action on library filtering has focused upon the needs of library patrons. In a Minneapolis, Minnesota dispute that attracted national attention, twelve librarians filed [SEXUAL HARASSMENT](#) claims based on unwanted exposure to patrons viewing pornography on the library's Internet computers. They argued that such exposure subjected them to a so-called "hostile work environment," one of the legal standards commonly pursued under sexual harassment law. In June 2001, the U. S. Equal Employment Opportunity Commission agreed with their complaint.

More broadly than public libraries, a majority of schools have adopted restrictive Internet policies. In 2000, a national survey by Quality Education Data Inc. found that more than 90 percent of teachers reported that schools had established acceptable use policies for Internet usage. Often these policies have involved installing software solutions, whether fitting each computer with off-the-shelf filters, blocking data at the school server level, or monitoring student Internet activity with so-called "sniffing" software that inspects their communication for behavior such as illegally downloading copyrighted music or seeking weapons information.

The following states and cities have enacted specific filtering legislation. However, other state and local laws may also apply to Internet usage on public computers. Concerned individuals can check with their school or library for a copy of its Internet usage policy.

ARIZONA: Public schools are required to filter Internet services to prevent minors from accessing harmful material, with each school district prescribing its own standards and rules. Public libraries must equip computers with Internet filters, implement policies, and follow statewide library rules. Schools and libraries in compliance with the law are protected from criminal liability and liability for damages.

KENTUCKY: Public schools are required to be filtered via so-called proxy software installed on Internet servers. However, schools and districts are free to exercise control over what they consider inappropriate.

Encyclopedia of Everyday Law: Internet Filters In Schools And Libraries

MICHIGAN: Public libraries are required to choose from three options for preventing children from accessing inappropriate Internet sites. They may install filters, monitor children's behavior, or require adult supervision.

MINNESOTA: Public and school libraries are required to block Internet access for obscenity and child pornography for both adults and children. They may choose between using either filtering software or "other effective methods."

SAN FRANCISCO: The city banned the use of Internet filters on most public-access library computers, thus codifying a 1999 San Francisco Public Library policy in opposition to filters.

SOUTH CAROLINA: Public and school libraries must filter computers for pornographic pictures or text; those not in compliance face losing half their state funding.

TENNESSEE: All public school computers have Internet web pages filtered system wide, making the state the first in the nation to employ this approach.

Additional Resources

Children's Internet Protection Act and the Neighborhood Internet Protection Act, as contained in Public Law. 106-554 Available at: <http://www.ala.org/cipa/Law.PDF>

"CIPA's Internet Filter Software Mandate Takes Effect." Brian Matross. [InternetLawJournal.com](http://www.tilj.com). June 3, 2001. Available at: <http://www.tilj.com/content/ecomheadline06030101.htm>

"Digital Chaperones for Kids: Which Internet Filters Protect the Best? Which Get in the Way?" Consumer Reports Online. March 2001. Available at: <http://www.consumerreports.org>

"Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet." Ann Beeson, et al. American Civil Liberties Union. 1997 Available at: <http://www.aclu.org/issues/cyber/burning.html>

"Filth, Filtering, and the First Amendment: Ruminations on Public Libraries' Use of Internet Filtering Software." Bernard Bell. Federal Communications Law Journal. March, 2001.

"The Internet Filter Farce." Geoffrey Nunberg. The American Prospect. Volume 12, Issue 1. January 1-15, 2001.

Organizations

American Civil Liberties Union (ACLU)

125 Broad Street, 18th Floor
New York, New York 10004 USA
Phone: (212) 549-2500
URL: <http://www.aclu.org>
Primary Contact: Nadine Strossen, President

American Family Association

Encyclopedia of Everyday Law: Internet Filters In Schools And Libraries

P.O. Box 2440
Tupelo, MS 38803 USA
Phone: (662) 844-5036
Fax: (662) 842-7798
URL: <http://www.afa.net>
Primary Contact: Donald E. Wildmon, President

American Library Association (ALA)

1301 Pennsylvania Avenue NW, Ste. 403
Washington, DC 20004 USA
Phone: (202) 628-8410
Fax: (202) 628-8419
URL: <http://www.ala.org/cipa/>
Primary Contact: Emily Sheketoff, Executive
Director Washington Office

Electronic Frontier Foundation

454 Shotwell Street
San Francisco, CA 94110 USA
Phone: (415) 436-9333
Fax: (415) 436-9993
URL: <http://www.eff.org>
Primary Contact: Brad Templeton, Chairman

Copyright Notice

©2009 eNotes.com, Inc.

ALL RIGHTS RESERVED.

No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution or information storage retrieval systems without the written permission of the publisher.

For complete copyright information, please see the online version of this work:
<http://www.enotes.com/everyday-law-encyclopedia>