

INTERNET ACCESS, FILTERING, AND LIBRARIES

The Internet is a recent phenomenon, which, even in its infant state, has transformed society. Anyone can share pictures, text, and sound files with the rest of the world. Through email and chat people around the world can communicate. Unfortunately, this includes those who would use this technology in ways that may harm others. In response to concerns that there is material on the Internet that is inappropriate for children, Congress has made several attempts to control content on the Internet and to shield children from harmful materials.

So far, none of their efforts at crafting legislation have succeeded in passing a Constitutional test. All have been declared unconstitutional for various reasons, which are explained below. But it is worthwhile to have the language being debated in front of us:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Our responsibility at Winnefox is to provide professional leadership to the member libraries of Winnefox. The Library profession has historically supported the principle of free speech and its derivative rights – freedom to read and freedom of access to information.

The responsibility of libraries is to abide by the law. The supreme law of the land is the Constitution of the United States. Laws developed by government at all levels must not violate the Constitution. This is obviously not an easy task given the lack of success of Congress cited above. Affirming this responsibility has gotten many libraries in trouble since it is usually in response to a controversy that we find ourselves defending the principle of free speech.

THE COMMUNICATIONS DECENCY ACT (CDA)

In February of 1996, the CDA was enacted as part of the Telecommunications Act of 1996. CDA sought to protect minors from harmful material online by criminalizing Internet transmission of "indecent" materials to minors.

In 1997, the Supreme Court ruled 9-0 that CDA was an unconstitutional restriction on the Internet. Because only obscenity is regulable, the regulations would effectively reduce the constitutionally protected material available to adults "to only what is fit for children." The unique characteristics of Internet communications (its ready availability and ease of use) were integral to the decision. Because it is possible to warn viewers about incipient indecent content (unlike radio, where warnings fail to protect all potential

listeners), and because alternatives exist, the CDA's provisions cast a "far darker shadow over free speech which threatened to torch a larger segment of the Internet community than [any] speech restrictions previously encountered."

THE CHILD ONLINE PROTECTION ACT (COPA)

In October 1998, Congress passed and President Clinton signed into law the Child Online Protection Act (COPA), the "sequel" to CDA. COPA establishes criminal penalties for any commercial distribution of material harmful to minors.

In February 1999, the Federal District Court in Philadelphia issued an injunction preventing the government from enforcing COPA. That court held that COPA was invalid because there is no way for Web speakers to prevent minors from harmful material on the Web without also burdening adults from access to protected speech. The Third Circuit Court of Appeals affirmed on June 22, 2000, finding that COPA was unconstitutional on a different ground. "Because of the peculiar geography-free nature of cyberspace, [COPA's] community standards test would essentially require every web communication to abide by the most restrictive community's standards." On May 13, 2002 the Supreme Court issued a decision, which did not decide any of the core legal questions, but ordered a lower court to decide the case on a wider range of First Amendment issues. Meanwhile, a majority of justices appeared to have grave doubts about the law's ultimate constitutionality, and the Court left in place an injunction barring enforcement of the law.

THE CHILDREN'S INTERNET PROTECTION ACT (CIPA) AND THE NEIGHBORHOOD CHILDREN'S INTERNET PROTECTION ACT (NCIPA)

In December 2000 Congress passed two laws designed to protect children from Internet pornography. The Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA) were part of a large federal appropriations measure (PL 106-554).

CIPA requires libraries to install blocking or filtering technology on all computers connected to the Internet if they receive E-Rate or LSTA funds for Internet access or purchasing computers to be used for Internet access. The law requires filtering of visual depictions of obscenity, child pornography, and materials harmful to minors. The law does not require the filtering of text.

NCIPA requires that libraries participating in the E-Rate program adopt and implement an Internet safety policy that addresses:

1. Access by minors to inappropriate matter on the Internet and the Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;

4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors;
 5. Measures designed to restrict minors' access to materials harmful to minors.
- The Internet Safety Policy must be adopted after holding at least one public hearing or meeting.

On May 31, 2002, a Federal district court declared the CIPA filtering mandate for public libraries unconstitutional. The Supreme Court is currently reviewing this decision. This decision addressed only CIPA, not NCIPA.

CONSTITUTIONAL ISSUES

In all three cases, the U.S. Supreme Court and other federal courts have repeatedly ruled that filtering Internet access in public libraries is unconstitutional on First Amendment grounds.

- **Use of filters blocks Constitutionally protected speech** In addition to pornography, filters routinely “overblock” and prevent access to legally protected sites. Examples include sites dealing with health and medical issues; political sites, including those of political candidates; sports teams; religious organizations; and charities. “Many erroneously blocked pages contain content that is completely innocuous for both adults and minors, and that no rational person could conclude matches the filtering companies' category definitions”
- **Filters do not block visual images** CIPA requires libraries to block visual depictions of pornography. No existing filter has the ability to do this.
- **There are other, less restrictive ways to achieve the goal of protecting children.** To protect children from harmful material, libraries could grant minors unfiltered access only if accompanied by a parent, or upon parental consent, or could require minors to use unfiltered terminals in view of library staff. To prevent patrons from being unwillingly exposed to offensive, sexually explicit content, libraries can offer patrons the option of using blocking software, can place unfiltered terminals outside of patrons' sight lines, and can use privacy screens and recessed monitors.
- **The library is a public forum.** Libraries have been established as forums where information on a wide and contrasting variety of topics and opinions is available. “...we believe that where the state designates a forum for expressive activity and opens the forum for speech by the public at large on a wide range of topics, strict scrutiny applies to restrictions that single out for exclusion from the forum particular speech whose content is disfavored. Laws designed or intended to suppress or restrict the expression of *specific* speakers contradict basic First Amendment principles.”

- **There are other ways to prevent objectionable behavior on the part of adults.** Libraries can adopt policies prohibiting access to illegal content. Libraries can ensure that their patrons are aware of such policies by posting them in prominent places in the library, requiring patrons to sign forms agreeing to comply with the policy, and by presenting patrons, when they log on to one of the library's Internet terminals, with a screen that requires the user to agree to comply with the library's policy before allowing access to the Internet. Libraries can detect violations of their Internet use policies either through direct observation or through review of the library's Internet use logs. "The proper method for a library to deter unlawful or inappropriate patron conduct, such as harassment or assault of other patrons, is to impose sanctions on such conduct, such as either removing the patron from the library, revoking the patron's library privileges, or, in the appropriate case, calling the police."
- **The constantly changing Internet** Internet sites, unlike printed books, do not stay the same. Webmasters can easily change the content on their sites at any time. An Internet address (URL) can be abandoned by one owner and acquired by another who will change the content. Filtering companies do not regularly go back and review sites already categorized. Indeed, because of the size of the Internet and the speed at which it changes they cannot do this.
- **The lack of community standards** The Internet is a worldwide phenomenon, fully available to people in almost every country. As the Court pointed out in the COPA case, it is not possible for one community's standards to be imposed on such a medium.

HOW FILTERS WORK

Filters (also known as content filters or blocking software) are software programs that block the transmission of data over the Internet. Filters employ two primary methods for blocking data: *word blocking* and *site blocking*.

Word blocking (also known as keyword blocking) matches web pages against a list of keywords. If the web pages match the keywords, the web pages are blocked. Unfortunately, filtering software is not sophisticated enough to evaluate context and the user will be unable to reach sites with phrases such as "chicken breast" and "Dick Cheney".

Site blocking matches web pages on the Internet against a list of predetermined sites. When the user attempts to access one of these sites, the filter's stoplist prevents them from reaching it. Most site-blocking stoplists are created in part or entirely by human review; employees of the filtering companies select sites to be included on the stoplist. Site blocking has several major drawbacks.

- A single Internet service provider will host the websites of many businesses and individuals; one person's objectionable site may cause all sites on that ISP to be blocked.
- The Internet is always changing; sites with objectionable content today may be free of it tomorrow, and vice versa.
- These filters represent the opinions of the people who select their content. What one person finds offensive another will find harmless.

For more information

Information on CIPA and NCIPA from the Wisconsin DPI.

<http://www.dpi.state.wi.us/dlcl/pld/cipafaq.html>

Libraries & the Internet Toolkit from the American Library Association

<http://www.ala.org/alaorg/oif/internettoolkit.html>

Effectiveness of Internet Filtering Software Products A report prepared by Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO).

<http://www.aba.gov.au/internet/research/filtering/filtereffectiveness.pdf>

Filtering Software: The Religious Connection. A report reviewing the relationship between eight filtering software companies with conservative religious organizations.

<http://responsiblenetizen.org/documents/religious2.html>

Plain Facts About Internet Filtering Software. A report from the Public Library Association. http://www.pla.org/publications/technotes/technotes_filtering.html