WHEN THE INTERNET BECOMES X-RATED: CREATING AN ETHICAL CLIMATE FOR TECHNOLOGY IN CATHOLIC SCHOOLS

SUSAN HANLEY KOSSE
Louis D. Brandeis School of Law

Pornography is the number-one business on the Internet, yet the very same Internet can be a valuable source of knowledge for all students. Educational leaders face many challenges in bringing the Internet into classrooms. This article reviews recent and relevant case law on Internet access in schools, offers guidance about the writing of effective acceptable use policies, and concludes with advice to Catholic school teachers and administrators on creating an ethical climate while fully using available technology.

As of 1999, the Internet was made up of more than 200 million users worldwide. There are now more than 100 countries linked to the Internet. The Internet works by connecting computers together by various means so instantaneous communication can occur. The World Wide Web is "a system of Internet servers that support specially formatted documents" written in a language called Hypertext Markup Language (HTML) (*Webopedia,* 2001). Web browsers such as Netscape Navigator and Microsoft's Internet Explorer allow us to access the World Wide Web. The Internet has often been compared to a multilane highway with the World Wide Web comprising just one of those lanes. This technology allows people next door and around the world to share information via video, sounds, and pictures, which has a profound impact on our daily living. We now get our news from it, shop and do business by it, and stay in touch with friends through e-mail.

It is difficult to imagine anything that has changed students' access to information more than the Internet and the World Wide Web. With just a few keystrokes and a click of the mouse, students can find information on virtually any subject. This technology has enabled our students to have worldwide connections to other schools and cultures, specialized instruction, technolog-

Catholic Education: A Journal of Inquiry and Practice, Vol. 4, No. 4, June 2001, 514-529

ical proficiency, and exposure to new topics and knowledge that the student may not have had an opportunity to learn (Pool, Blanchard, & Hale, 1995). Students are able to retrieve more information at greater speeds than by traditional methods of learning. "Book learning" is enhanced instantaneously with websites that provide pictures, information, and interactive exercises.

Realizing the benefits of this technology, communities have placed a high priority on getting their students and schools connected. In 1994, the White House's National Information Infrastructure initiative challenged the nation's schools to be 100% connected by the year 2000 (National Center For Education Statistics, 2000b). By 1999 it was estimated that 95% of the public schools had Internet access. Private schools, in contrast, are less likely to have Internet access (National Center For Education Statistics, 2000a). In fact, in 1998, 33% of private schools were still not connected. In general, Catholic schools (83%) are more likely than nonsectarian schools (66%) or those with other religious affiliations (54%) to have access. It is also interesting to note that of the schools still without access, Catholic schools are most likely to have plans to connect to the Internet in the future (74%) compared to nonsectarian schools (38%) or other religious schools (41%).

Yet for all the benefits the Internet provides to school children, it has the potential to expose them to sexually explicit material. Unfortunately, sexually explicit or pornographic sites are on the World Wide Web in greater and greater numbers (Miller, 1999). Although it would be nearly impossible to specify the number of such sites, there is evidence that they are increasing. According to a recent law review article, in 1997 there were 10,000 sites containing sexually explicit material on the Internet. By 1999 this number had grown to between 30,000 and 60,000 sites. Since these sites are very profitable and the fastest growing, there is no reason to think the upward trend will end soon.

The issue for many concerned parents is how to keep our children from accessing these inappropriate sites. Unfortunately, many of them can be found inadvertently through what would seem harmless searches. For example, a child who typed in "Sleeping Beauty," "Little Women," or "Girls.com" may retrieve some appropriate material but also sexually explicit material (Miller, 1999). The author indicates that Girls.com "features '125,000 hardcore pics' and Pam Anderson [and] Tommy Lee uncensored videos"' (p. 161). Typing WhiteHouse.com instead of WhiteHouse.gov would lead children to a site containing pornographic material and claiming to be the number-one adult website.

With this in mind, Congress has attempted for the last few years to pass legislation that will protect our children from inappropriate and harmful material found on the Internet. Although that goal is commendable, it has proven difficult to achieve without violating the First Amendment. This article will first examine the recent federal legislation including the lawsuits

those laws spawned. Next, the article will discuss alternatives to legislation, in particular, acceptable use policies. Finally, the article will conclude with concerns specific to Catholic schools.

CONGRESSIONAL RESPONSE

COMMUNICATIONS DECENCY ACT

Passed as part of the Telecommunications Act of 1996, the Communications Decency Act (CDA) prohibited Internet users from using the Internet to communicate material that is obscene or indecent to minors under the age of 18. Specifically, 47 U.S.C. Sec. 223(a) provided:

> Whoever—
> (1) in interstate or foreign communications—
> (B) by means of a telecommunications device knowingly—
> (i) makes, creates, or solicits, and
> (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication....
> (2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under title 18, or imprisoned not more than two years or both.

The second provision, section 223(d), prohibited the sending or displaying of messages that would be deemed, under contemporary community standards, patently offensive to a person under 18 years of age. It provided:

> Whoever—
> (1) in interstate or foreign communications knowingly—
> (A) uses an interactive computer service to send a specific person or persons under 18 years of age, or
> (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or
> (2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under Title 18, or imprisoned not more than two years, or both.

These two provisions were limited by two affirmative defenses. One protected individuals from liability if the person had taken "in good faith, reasonable, effective, and appropriate actions under the circumstances" to keep minors from the harmful material (section 223(e)(5)(A)). The other covered individuals who restrict access by requiring certain forms of age proof such as a verified credit card or an adult identification number.

Despite these limiting defenses, the statute was struck down by the Supreme Court in *Reno v. ACLU* (1997) on the grounds that it was unconstitutionally vague and too broad, violating the First Amendment. The Court used a strict scrutiny standard which requires the government to show not only a compelling interest for the law but also that the law is a necessary means to achieving the goal. In striking down CDA, the Court was particularly troubled over undefined key terms such as "indecent" and "patently offensive." The failure of Congress to define these, among other words, made the statute unconstitutionally vague because an individual would not have a clear understanding of what material was to be included by those terms.

Perhaps even more troubling for the Court was the statute's "wholly unprecedented" breadth since it was "not limited to commercial speech or commercial entities...[but rather] [i]ts opened prohibitions embrace[d] all nonprofit entities and individuals posting indecent messages or displaying them on their own computers" (*Reno*, 1997, p. 877). Although the statute would further the government's interest in protecting children from harmful Internet material, the CDA would result in the suppression of legitimate material that adults have a constitutional right to send and receive. Therefore the court opined that the government was required to use less restrictive means to achieve its goals of protecting minors.

Moreover the statute was void of any guidance on which community standards in particular would be applied to determine whether material was harmful to minors. Since the Internet is available to the world, it is conceivable that a community standards criterion under this law could be interpreted to mean the community that has the most restrictive views about what is offensive (*Reno*, 1997).

Finally, the defenses provided in the statute were unworkable and did not "constitute the 'narrow tailoring' necessary to save an unconstitutional provision" (*Reno*, 1997, p. 882). Although the age verification was a legitimate option for commercial sites, the court found that it was not economically feasible for noncommercial sites. In addition, the Court was skeptical whether the current technology used by commercial pornographers actually kept children from gaining access. In light of the statute's criminal sanctions, the Court agreed with the District Court that the government had failed to prove that the defense would reduce the heavy burden on adult speech.

CHILD ONLINE PROTECTION ACT

In 1998, Congress attempted to correct the problems of the Communications Decency Act and address the concerns raised by the Supreme Court by enacting the Child Online Protection Act (COPA). Specifically COPA prohibits an individual or entity from:

> Knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, mak[ing] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors. (47 U.S.C. 231(a)(1))

This second attempt was noticeably narrower than CDA in three respects. First, COPA only applied to commercial pornographers, unlike CDA, which affected all communications. Second, COPA only applied to Web communications. Finally, the standard was changed from the ambiguous "indecent and patently offensive" standards to a "harmful to minors" standard.

Congress also defined some of the essential key terms including "by means of the World Wide Web," "minor," "commercial purposes," and "engaged in the business." In addition, to give the "harmful to minors" standard criterion more clarity, Congress adopted a three-prong test, set out first in *Miller v. California* (1973), which would give guidance in determining what is actually harmful to minors. For liability to attach, it must be proven that the material:

> a) [judged by] the average person, applying contemporary community standards,...taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, prurient interest;
> b) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted act, or a lewd exhibition of the genitals or post-pubescent female breast; and
> c) taken as a whole, lacks serious, literary, artistic, political, or scientific value for minors. (p. 24)

The day after the statute became effective, the American Civil Liberties Union (ACLU) filed suit once again, claiming that the statute violated the First and Fifth Amendments because it was vague and infringed upon the protected speech of adults (*ACLU v. Reno*, 2000). The United States District Court issued a preliminary injunction preventing COPA's enforcement. The government appealed to the Third Circuit, which affirmed the District Court's order, holding that the District Court properly exercised its discretion in granting the injunction (*ACLU,* 2000). Although the Court did not rule on the statute's constitutionality per se, its opinion gives a clear indication that this statute too would be found to be overbroad and thus unconstitutional.

Specifically, the court concluded its opinion by stating, "Due to current technological limitations, COPA—Congress' laudatory attempt to achieve its compelling objective of protecting minors from harmful material on the World Wide Web—is more likely than not to be found unconstitutional as overbroad on the merits" (ACLU, 2000, p. 180).

To determine whether the preliminary injunction was properly granted, the Third Circuit applied a four-prong test (*ACLU*, 2000). The four prongs were: 1) whether the movant had shown a reasonable probability of success on the merits; 2) whether the movant will be irreparably harmed by denial of the relief; 3) whether granting preliminary relief will result in even greater harm to the nonmoving party; and 4) whether granting the preliminary relief will be in the public interest. The most important prong is whether there is a reasonable probability that the party seeking the injunction will succeed on the merits if the case is taken to trial. In analyzing this prong the Court recognized that the government did have a compelling interest in protecting children from harmful material. This objective, however, must be met in the least restrictive means available. In surmising that the statute was unconstitutional, the Court focused on COPA's definition of "harmful to minors," applying a "contemporary community standards" clause. It did so while recognizing that the District Court had identified several other grounds for declaring the statute unconstitutional. For example, the District Court found that the economic costs and burdens of the age verification requirement were too great of a burden on publishers, forcing them to stop publishing or more heavily censor what they published. The Third Circuit acknowledged that this may be true but opined that the even greater problem with the statute was that the Supreme Court's concern regarding the "community standards" test in the unconstitutional CDA was still not adequately remedied by this new statute (*ACLU*, 2000).

In response, the government argued that Congress had effectively dealt with this issue by including the *Miller* (1973) three-prong test within the statute's text. The Court, however, was not persuaded that this cured the problem since the facts in *Miller* differed drastically from the current situation. *Miller* involved the mailing of sexually explicit material, which was in violation of California law. The publisher of the information could control to which geographic locations the material was sent. But because the Internet has no geographic boundaries and publishers have no means of even knowing what locale their material goes to, the Court reasoned that a community standards test would be particularly troublesome and not appropriate. In essence, the publisher would be forced to censor material that may be accessed from extremely puritan communities or implement costly age verification systems. This would effectively block material from all minors even if it were not deemed harmful in their own communities. In addition, adults would be unconstitutionally deprived of their rights.

Based on this decision, the government had three options. It could appeal the ruling to the Supreme Court, ask for the entire United States Third Circuit Court of Appeals to reconsider, or go back to the lower court and request a full trial. As of the time of this writing, none of these options had been pursued, indicating the government probably surmised any challenge they made would be unsuccessful. Because of the injunction prohibiting the statute's enforcement, COPA is virtually useless.

BLOCKING SOFTWARE BILLS

An alternative way to limit minors' access to harmful Internet material is to use filtering software. Filtering software falls into two general categories: predetermined blocking filters and ratings-based filters (Semitsu, 2000). The predetermined filters block access by one of five methods: blacklists, allow lists, word blocking, image-blocking, and the blocking of entire categories (p. 513). Most common is the use of blacklists, which block sites that have been predetermined to be inappropriate. Many of the programs use some form of word blocking, which often can lead to the overinclusive blocking of constitutionally protected material. For example, there are reports that certain programs banned the word *breast,* unintentionally blocking all websites dealing with breast cancer. Critics of filtering software argue that this technology can be underinclusive as well. A recent report testing one software blocking product found that thousands of unbanned porn sites were not properly blocked mainly because it was too difficult for any manufacturer to keep up with all the new material added daily to the Internet.

More sophisticated rating-based filters (PICS) allow individuals, webmasters, or third-party groups to rate sites by creating descriptive labels (Semitsu, 2000). PICS can then read the labels and use their own filtering criteria to decide whether to block the site. This technology makes it much easier to tailor what will and will not be blocked based on the policies and concerns of the library or school using it. Ideally, each community library could create its own criteria for blocking sites. Realistically, however, this would be too burdensome for the libraries and they will be forced to adopt criteria designed by third-party organizations. This, critics argue, will result in these third-party organizations' subjective value judgments being implemented by the libraries (Semitsu, 2000).

Despite the debate over the technology, legislation that would require schools and libraries with Internet access to install blocking software on their computers has been on the legislative agenda for several years. The first proposed act to address the issue was the Safe Schools Internet Act of 1998. Senator John S. McCain introduced the bill to the Senate on February 9, 1998, while Representative Bob Franks introduced H.R. 3177 two days later. Both those acts proposed amending 47 U.S.C. 254 to require that elementary

and secondary schools and libraries receiving federal Internet access subsidies install blocking software. Specifically the act provided that "no services may be provided...to any elementary or secondary school, or any library, unless it provides the certification...that it has...selected a system for computers with Internet access to filter or block matter deemed to be inappropriate for minors" (Safe Schools, 1998).

The Senate version of the bill was referred to the Committee on Commerce, and hearings were held. On June 25, 1998, Senator McCain reported to the Senate and the bill was placed on the Senate Legislative Calendar. It was attached to the FY 1999 Commerce, Justice, State Appropriations bill on July 21, 1998, and passed by the Senate on July 23. H.R. 3177 (Safe Schools, 1998) on the House side was referred to the House Commerce Committee, where it was not acted upon.

Not to be discouraged, in January 1999 Senators McCain and Ernest F. Hollings tried again. This time they introduced the Children's Internet Protection Act (Title XVII, 1999). This bill was then reintroduced by McCain as Amendment No. 3610 to the Labor, Health and Human Services Appropriations Bill (H.R. 4577). This amendment was approved by a vote of 95-3 on June 29, 2000.

The House passed a similar but not identical bill on June 8, 2000. The legislation was referred to a conference committee to reconcile the House and Senate versions. Currently it is an amendment to the HHS Appropriations Bill, which was passed by Congress on Friday, December 15, 2000 (Internet Filtering Law, 2000), and was signed by President Clinton on December 21, 2000.

Fierce opposition to the bill has come from the American Library Association (ALA) and free speech groups. The ALA's website had multiple entries urging its members to lodge their disapproval with their elected representatives. They advised their members that

> Federal filtering mandates are not the answer to the very complex question of objectionable Internet material because:
> - Federal filtering mandates are unfunded mandates. They will require my library to take on the onerous burden of paying to install and maintain filters or be stripped of key federal funding.
> - Federal mandates trample on the decision-making responsibilities and capabilities of my local library board. Mandates do not allow us to articulate our own community values because they force us to turn over our community decisions to corporate entities.
> - Federal filtering mandates are a one-size-fits-all, overly broad solution to a complex and local problem. Around 95% of public libraries already have in place a formal policy to regulate use of the Internet. But the Labor-HHS-Ed amendments prescribe broad, unfunded federal government control in my library.

> • Federal mandates will have the most profound effect on those libraries that most need E-rate discounts and other funding. Low-income, poverty-stricken libraries will not have the resources to implement filtering and comply with the certification requirement. (American Library Association, 2000)

Even the *New York Times* (A Misguided Pornography Bill, 2000) published an editorial urging Congress not to pass the amendment. The writer called federally mandated filters "absurd" and most likely "unconstitutional" (p. 4-14). Since filtering software is often ineffective, the author urged more closely monitoring students was a better solution.

In contrast, parent groups praised Senator McCain's relentless efforts to protect children from the negative aspects of the Internet. The American Family Association strongly supported the bill, stating that it would "provide a very effective solution to the growing problem of pornography accessible on the Internet by computers in schools and public libraries" (Senate Approves Amendment, 2000, p. 2028).

Before the bill was even signed into law, the ACLU announced plans to sue (Internet Filtering Law, 2000). ACLU lawyer Chris Hansen called the filtering requirement "a mandated censorship system by the federal government" (p. A4). Hansen took particular offense since even the bill's supporters recognize that there are multiple problems with filters but argue that overall filters are better than having nothing at all. Hansen stated that

> The First Amendment doesn't have a 'good enough' requirement.... Suppose we said it would be better than nothing for someone to go into Barnes and Noble and burn every 10th book. That sort of casual insensitivity to censorship is disturbing. (p. A4)

A lawsuit over the constitutionality of filters is nothing new. In fact, there have already been lawsuits filed testing the First Amendment's limitations on the use of Internet filtering in public libraries. In 1997, 10 individual plaintiffs, all adult patrons of their local library, brought a suit to enjoin the library from installing filtering software on the library's computers (*Mainstream Loudoun v. Board of Trustees of Loudoun County Library I,* 1998a). Earlier that year the library board had voted to adopt a policy on Internet sexual harassment. The policy required that "site-blocking software…be installed on all [library] computers" so as to

> a. block child pornography and obscene material (hard core pornography);
> b. block material deemed Harmful to Juveniles under applicable Virginia statutes and legal precedents (soft core pornography) (p. 556).

The commercial product X-Stop was chosen to limit access to sites that violated the library policy.

The plaintiffs alleged a violation of their freedom of speech. Specifically they argued that the policy impermissibly blocked their access to protected speech and chilled their receipt of constitutionally protected materials. For instance, they could no longer gain access to the Quaker Home Page, the Zero Population Growth website, and the site for the American Association of University Women—Maryland because they had been blocked. Moreover, they claimed there were no clear criteria for determining which sites would be blocked (*Mainstream,* 1998a).

Since the libraries at issue were determined to be limited public forums, any content-based restriction had to be "narrowly drawn to effectuate a compelling state interest" (*Mainstream*, 1998a, p. 795). The court held protecting minors from harmful Internet material and avoiding a sexually hostile environment were compelling government objectives. But because the filtering policy was too broad (it was not limited to minors and there were not adequate standards for restricting speech), it was not the least restrictive means nor reasonably necessary to achieve the government's goals. The Court noted that lesser restrictive options were available including library staff monitoring, filters for minors only, and privacy screens (*Mainstream*, 1998b).

Just the threat of lawsuits has made some libraries change their plans to install filters. For example, on August 16, 2000, the Nashua Public Library Board of Trustees voted to reverse its decision to install Surfwatch software on all their computers. This reversal came after local citizens opposed to the policy contacted the People for the American Way Foundation and some New England attorneys. And when the ACLU threatened legal action, the public libraries of Kern County, California, changed their policy of requiring filters on their computers (Ontario Consultants on Religious Tolerance, 2001).

Conversely, there has also been litigation for a library's failure to restrict children's access to harmful Internet material, although the lawsuits have been unsuccessful. It is not surprising that many libraries choose not to use filters, considering the American Library's Association position that any efforts to block access violate the Library Bill of Rights (American Library Association, 1997). Perhaps the most publicized suit filed concerning this matter was *Kathleen R. v. City of Livermore* (1998), in which a mother filed suit hoping to force her local library to install filters. The impetus for the legal battle came after her 12-year-old son downloaded pornographic pictures off the library's computer. The case was dismissed in January 1999 in a one-sentence ruling.

This issue has not been limited to public libraries. In 1998 in Palm Beach, Florida, a mother sued the Broward County School Board for failing to install filters on public school computers (*Hoffman v. The School Board of Broward County, Florida*). The case was dismissed on January 14, 1999.

Whether a federal statute mandating filters for schools and libraries could survive constitutional scrutiny is doubtful. Perhaps the biggest obstacle for

such legislation is drafting it so it is not deemed a prior restraint. First, the legislation must be narrowly tailored, including specific guidelines as to what could be blocked. One of the major problems in the *Loudoun* case was the complete lack of guidance as to the criterion used to block the sites. Lack of guidance would surely bring cries of vagueness and overbreadth again. For example, the "inappropriate to minors" standard may be too unclearly defined to give a person the necessary guidance to know what to block. Also, plaintiffs could argue that the law would also regulate speech that was constitutionally protected.

At least one commentator on the use of filters by libraries and schools proposes that a librarian's exclusion of Internet material can be constitutional as long as the libraries do not favor any one viewpoint over another (Nadel, 2000). The author compares the use of filters to the librarian's discretion in purchasing books. He says the First Amendment does not prohibit librarians from purchasing multiple books of the same title, which necessarily will limit access to other titles due to the practicalities of library budgets. Therefore, the same rationale should justify librarians using filters even if they will result in denying patrons access to other constitutionally protected material.

Nadel (2000) takes issue with some of the findings in the *Mainstream Loudoun* opinions. (See also written testimony of Jay A. Sekulow, Esq., who also believes *Mainstream Loudoun* was incorrectly decided.) Specifically, he disagrees with the Court's view that financial constraints do not impact Internet access as they do with traditional book acquisitions (Nadel, 2000). He argues that financial considerations apply equally to the Internet because they essentially drive how many terminals and Internet accounts a library can afford as well as the speed of access links. These all have an impact on how many websites a patron can ultimately view. The solution, Nadel argues, is to allow filters that will help librarians manage the Internet resource by preventing the domination of terminals by patrons wanting to view pornography or play games and thus tying up the terminals from more desirable uses such as research.

Critics of this approach argue that sign up sheets could be an effective remedy for the budgetary resource problem. However, Nadel (2000) argues that this is not a favorable approach, noting that libraries do not purchase only one copy of a popular book to lend on a first-come first-serve basis. This is so even if purchasing multiple copies of the book will deny access by patrons to other books because of limited purchasing resources or shelf space. Thus, Nadel concludes that since this purchasing decision would not be considered a prior restraint, the same logic should uphold the use of filters if they are utilized to maximize the access of "preferred" categories of Internet content.

Nadel (2000) recognizes that libraries could get into constitutional trouble if they do not guarantee that they are making the exclusions themselves instead of some software producer of filters. Delegating full control to an out-

sider is unquestionably unconstitutional. To avoid this, Nadel proposes that libraries "1) retain final say over selection decisions, 2) understand the criteria that the filter software uses to exclude content, and 3) have the resources to correct the viewpoint discrimination that the filters are likely to generate" (p. 1118). These recommendations are particularly relevant in light of the flawed quality of existing filters, which sometimes create errors. Therefore, it is essential that librarians be able to "tweak" the filters to rectify any impermissible exclusions.

Not everyone, however, agrees with Nadel's (2000) comparison of filtering to that of purchasing books. In fact some legal scholars think filtering software is more like removing a book already in the library's collection (Semitsu, 2000). Semitsu quotes attorney Jonathan Wallace, author of *Sex, Laws and Cyberspace,* who stated:

> A library installing computers with full Internet access has, in effect, acquired the entire contents of the Internet. Blocking software which screens out sites based on their inclusion in a database of impermissible sites, or blocks them based on the occurrence of banned words or phrases, is effectively removing these resources from the library. Just as the board of education did in *Pico* [the Supreme Court case which held that local school boards could not remove books simply based on a dislike of a book's ideas], someone has gone through a thought process which resulted in the removal of materials based on their disfavored content. (p. 527)

The ultimate resolution of whether any mandate requiring filters is constitutional or not may very well turn on this distinction between removing or selecting information for a library. As noted above, courts are much more reluctant to uphold a library's actions of removing books. Equally as important will be the court's designation of the library as either a limited public forum or a nonpublic forum. If a court were to hold that *Mainstream Loudoun* incorrectly classified the library as a limited public forum, the library must only show that its content-based restrictions are reasonable and viewpoint neutral. This would be a much easier burden than having to show that the restriction has been narrowly drawn to effectuate a compelling state interest.

ACCEPTABLE USE POLICIES

One way for schools to avoid lawsuits is to adopt and enforce acceptable use policies (AUP). An AUP is "a written agreement signed by students, their parents, and their teachers, outlining the terms and conditions of Internet use for the safety and educational benefit of the students" (Horizon, 2001). These agreements not only deal with the issues of pornography and obscenity but also such matters as copyright and intellectual property laws, defamation, and commercial use of the school-provided Internet access.

When designing AUPs, schools should remember that the AUP is a legal document and should be reviewed by an attorney. An AUP should contain:

- An overview of what the Internet is, how it will be used in the school, and why access to it is beneficial to the educational process
- Usage policies and guidelines including what constitutes acceptable and unacceptable uses of the Internet
- Penalties for violating the policies and guidelines
- A description of the rights of individuals using the networks in the school/district
- A disclaimer absolving the school district, under specific circumstances, from responsibility
- A clear indication that Internet access is a privilege, not a right, and may be withdrawn. (Horizon, 2001)

There are many Web resources that can aid a school or district in drafting an AUP. Two are: www.netizen.uoregon.edu and www.gsn.org/web/tutorial/issues/aupsampl.htm#begin/. Taking advantage of the various templates and suggestions listed on the Web is most helpful; however, they should not be adopted without tailoring them to the needs and philosophies of each individual school or district.

Although designing an AUP would appear to be fairly easy and straightforward, there are many issues districts or schools should consider before drafting an AUP. If these concerns are ignored, the AUP may be challenged in court much like the federal statutes discussed previously. Perhaps the biggest challenge could be based on vagueness. In other words, does the AUP clearly inform students about what is appropriate and inappropriate behavior that could possibly lead to discipline? If a court determines it does not, the AUP could be ruled unconstitutional.

Many common phrases found in AUPs regarding inappropriate actions may in fact be vague and subject to court challenges. For example, phrases such as "Students shall not access any objectionable material or inappropriate material" or "Students shall not post defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, or illegal material" do not clearly indicate to students what they can and cannot access or post (Willard, 1997). In addition, these phrases are too broad. Their current wording impermissibly prohibits some speech that is considered protected speech. This unclear speech very likely has First Amendment ramifications if courts find it chills students' free speech since they will not fully understand what they can and cannot do (Willard, 1997).

CATHOLIC SCHOOLS' CONCERNS

Catholic schools are governed by different rules than public schools or independent schools. Public schools are considered to be governmental agencies and therefore must comply with constitutional requirements. In contrast, a Catholic school is a private agency and therefore does not have to enforce constitutional protections (Shaughnessy, 1995). The Constitution was designed to be a guarantee by the government that it will respect certain rights contained within it. Since Catholic schools are not part of the government, they make no guarantee concerning these constitutional rights.

This does not intend to imply that Catholic school students or their parents have no rights (Shaughnessy, 1991). Although they have no rights under the Constitution because a Catholic school is not a governmental agency, they do have rights grounded in both state and federal statutory and common law. For example, both state and federal statutes prohibit racial discrimination. This law is not enacted by the Constitution and therefore can bind both governmental and private agencies including Catholic schools. In addition, parents and children of Catholic schools may have certain rights originating from contract law. The terms of the contract between the Catholic schools and its pupils are often contained in a printed handbook.

If the state is significantly involved in the private school or the contested activity, courts will find state action and as a result constitutional rights to exist (Shaughnessy, 1991). Courts have identified four sources for state action in a private school: state funding, state control, tax-exempt status, and the public benefit or function theory. A review of the case law indicates that the definition of substantial presence of state action is somewhat difficult to define (*Bright v. Isenbarger*, 1970; *Geraci v. St. Xavier High School*, 1978; *Wisch v. Sanford School, Inc.*, 1976). From these three cases it would appear that the court finds it very important whether the state is involved in the challenged action. In fact it must be "so entwined with the contested activity that a symbiotic relationship could be held to exist between the state and the action" (Shaughnessy, 1991, p. 9). This is so even where the school obtains 90% of its funds from the state (*Rendell-Baker v. Kohn*, 1982).

If a federal law makes filters mandatory in the Catholic schools, the contested activity (denial of Internet access) may be intertwined with the state action especially if the state action is based on funding for the computers. Although generally Catholic students would not have a cause of action against their school or school boards based on denial of free speech, they may in fact bring such an action if they are able to establish substantial state action.

Perhaps the better option for the Catholic student is to bring an action against the federal agency directly. This avoids the state action dilemma altogether since the suit would be brought against the government itself.

Therefore, if a federal law mandates filters on Catholic school computers, the student may have a valid First Amendment claim against the government.

The drafting of AUPs may be an area in which the Catholic schools will have more latitude than their public school counterparts. It would no doubt be unconstitutional for a public school to prohibit material because officials disagreed with its viewpoint. However, if this same material was in conflict with the Church's teachings (i.e., abortion or homosexual activity), Catholic schools would be free to prohibit access to it.

CONCLUSION

In this unsettled area of law the goal of keeping children protected from indecent and sexually explicit material on the Internet is shared by virtually all those concerned. How to achieve that universal goal is subject to intense debate. Legislation to this point has failed based on "vagueness" and "overbreadth" challenges. Courts have agreed that the laws violated the First Amendment since they chilled protected speech.

Perhaps the only way to protect students is to require them to sign and abide by properly drafted acceptable use policies. In addition, more supervision by parents, teachers, and librarians would aid in ensuring that children are not viewing improper material on the Internet. Even that becomes somewhat of a burden on a teacher or librarian who deals with many children daily. One day this may all be resolved if technology advances to cure the defects that currently exist in the filtering software programs. Until then the debate will continue about how best to protect our children without violating the First Amendment.

On March 20, 2001, the ACLU and the ALA filed a lawsuit in federal court in Philadelphia contesting the constitutionality of the new filter law. At present, only the part of the law that mandates filters in libraries is challenged, not the part that mandates Internet filters on school computers.

REFERENCES

ACLU v. Reno, 31 F. Supp.2d 473 (E.D. PA. 1999) rev'd 217 F.3d 162 (3d. Cir. 2000).

American Library Association. (1997). *Resolution on the use of Internet filtering software in libraries*. Retrieved February 12, 2001 from the World Wide Web: http://www.ala.org/alaorg/oif/filt_res.html

American Library Association. (2000). Education spending with filtering mandates, still in play. *Washington Office Newsline, 9*(86). Retrieved January 12, 2001 from the World Wide Web: www.ala.org/wasoff/alawon

Bright v. Isenbarger, 314 F. Supp. 1382 (1970).

Child Online Protection Act, 47 U.S.C. Sec. 231 (1998).

Communications Decency Act, 47 U.S.C. Sec. 223 (1996).

Geraci v. St. Xavier High School, 13 Ohio Op. 3d 146 (1978).

Hoffman v. The School Board of Broward County, Case No. 98-6290-CIV-HURLEY (S.D. Fla. 1999).

Horizon. (2001). *Internet 101 acceptable use policies (aup's).* Retrieved January 12, 2001 on the World Wide Web: www.horizon.nmsu.edu/101/aup.html

Internet filtering law faces lawsuit by ACLU. (2000, December 20). *Courier Journal,* p. A4.

Kathleen R. v. City of Livermore, Case No. V-015266-4 (Superior Court of California 1998).

Labor, Health and Human Services Appropriations Bill (H.R. 4577) Amendment 3610 (2000).

Mainstream Loudoun v. Board of Trustees of Loudoun County Library I, 2 F.Supp.2d 783 (E.D. Va. 1998a).

Mainstream Loudoun v. Board of Trustees of Loudoun County Library II, 24 F. Supp.2d. 552 (E.D. Va. 1998b).

Miller v. California, 413 U.S. 15 (1973).

Miller, H. L. (1999). Strike two: An analysis of the Child Online Protection Act's constitutional failure. *Federal Communications Law Journal, 52,* 155-188.

A misguided pornography bill. (2000, November 12). *New York Times,* p. 4-14.

Nadel, M. S. (2000). The First Amendment's limitations on the use of Internet filtering in public and school libraries: What content can librarians exclude? *Texas Law Review, 78,* 1117-1157.

National Center for Education Statistics. (2000a). *Stats in brief, February 2000: Internet access in U.S. private schools and classrooms: 1994-99.* Washington, DC: Author.

National Center for Education Statistics. (2000b). *Stats in brief, February 2000: Internet access in U.S. public schools and classrooms: 1994-99.* Washington, DC: Author.

Ontario Consultants on Religious Tolerance. *Internet Censorship Software Programs.* Retrieved January 12, 2001 from the World Wide Web: http://www.religioustolerance.org/cyberpat.htm

Pool, T. S., Blanchard, S. M., & Hale, S. A. (1995). From over the Internet, users discuss a new direction for learning. *Techtrends, 40*(1), 24-28.

Rendell-Baker v. Kohn, 102s. Ct. 2764 (1982).

Reno vs. ACLU, 521 U.S. 844 (1997).

Safe Schools Internet Act of 1988, S. 1619 and H.R. 3177 (1998).

Sekulow, J. A. (2000). *Written testimony on the Constitutionality of S. 97—a bill to require the installation and use by schools and libraries of Internet filtering software.* Retrieved December 4, 2000 from the World Wide Web: http://www.aclj.org/issues/filtering%20testimony.asp

Semitsu, J. P. (2000). Burning cyberbooks in public libraries: Internet filtering software vs. the First Amendment. *Stanford Law Review, 52*(2), 509-545.

Senate approves amendment requiring filters for web surfing in libraries, schools. (2000, July 11). *United States Law Week,* p. 2028.

Shaughnessy, M. A. (1991). *The law and Catholic schools: Approaching the new millennium.* Washington, DC: National Catholic Educational Association.

Shaughnessy, M. A. (1995). *Home and school working together: Catholic school parents' rights and responsibilities.* Washington, DC: National Catholic Educational Association.

Title XVII, Children's Internet Protection Act, Section 1701, PL 106-554 2000 HR 4577 (1999).

Webopedia. (2001). Retrieved February 12, 2001 on World Wide Web: www.webopedia.com.

Willard, N. (1997). *A legal and educational analysis of k-12 Internet acceptable use policies.* Retrieved February 12, 2001 from the World Wide Web: http://www.netizen.uoregon.edu

Wisch v. Sanford School, Inc., 420 F. Supp. 1310 (1976).

Susan Hanley Kosse is assistant professor at Louis D. Brandeis School of Law. Correspondence concerning this article should be addressed to Susan Hanley Kosse, J.D., Assistant Professor, Louis D. Brandeis School of Law, University of Louisville, 2301 South Third Street, Louisville, KY 40292.