November 2002

ATG Special Report: Part II -- Libraries In The Cyberage

Mark Y. Herring

Winthrop University, herringm@winthrop.edu

Follow this and additional works at: <https://docs.lib.purdue.edu/atg>

Part of the [Library and Information Science Commons](#)

Recommended Citation

Herring, Mark Y. (2002) "ATG Special Report: Part II -- Libraries In The Cyberage," *Against the Grain*: Vol. 14: Iss. 5, Article 10.
DOI: <https://doi.org/10.7771/2380-176X.3759>

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.

What I write here may be seen as conservative. And if it were true that library users are habit-driven, conservative, and fearful of change, it might well be the case. No such stereotype, however, accurately captures the real variety of extremely intelligent and resourceful people who make up our communities. Comparatively few users are as conservative as even we at 300-year old academic libraries like to say that they are.

But — the most traditional thing about library management is the thing that offers the antidote to any excess conservatism. That is, librarians are custodians of the past, but they think constantly about the future. For custodianship is worthless unless it anticipates future developments — opportunities as well as risks. Librarians have always bought for their collections with one eye to the present readers' needs and a second eye to the future needs of readers who will come in place of the ones now here. It is our — librarians' — job to make sure we find a sustainable and responsible level of collecting that will make our collection valuable twenty or fifty years from today. There is no science to implementing that sense of responsibility; it is an art we have long ago mastered.

In a world of transition from all-analog to a blend of analog and digital materials, it is exactly that same *conservative* sense of responsibility that will keep librarians most alert to creating collections of future as well as present value. The art of building collections that serve the present and the future: that is the art we need to transfer, apply, reinvigorate, and cherish. If serving our present and future readers is the most difficult thing about dealing with digital resources, it is also the one that our traditional library skills leave us feeling most qualified to handle.

And there in my two a.m. reverie is where I can finally fall asleep. 🐼

Rumors from page 28

As we go to press, **Edna Laughrey** <elaughrey@aol.com> has told me about the death of one of her mentors and a man who inspired many of us throughout his life, **Frank Clasquin**. See this issue p.8.

Y'all — Who would have ever believed that *ATG* would grow into such a big, substantial publication! I was recently reading **Bill Katz'** *Magazines for Libraries* (2002 edition) glowing review of *ATG* and, well, it brought a smile of pride to my eyes for all of us crazy acquisitions and collection development and serials librarians who work to put this together all the time. Thank you all! And, there's so much held over this time, for which we apologize, but watch for it in the next exciting issue ... Coming soon ... 🐼

ATG Special Report: Part II — Libraries In The Cyberage

by **Mark Y. Herring** (Dean of Library Services,
Dacus Library, Winthrop University)
<herringm@winthrop.edu>

The forums covered here include the conclusion of **Clancy's** article favoring library filters. Essentially, **Clancy's** argument is that the disadvantages of filtering are far fewer than those of not filtering. **Clancy** claims, first of all, that filtering does

not impinge upon the First Amendment because it has never protected obscenity and/or pornography. Secondly, she argues that the dangers of unfiltered Internet access pose such grave risks to others that the unfiltered choice is unconscionable.

Libraries In The Cyberage — Filtering, Censorship and the First Amendment: Libraries at the Crossroads

by **Carol A. Clancy, Esq.** (Senior Counsel, National Law Center for
Children and Families) <http://www.NationalLawCenter.org>

Filtering Adult Internet Access Closes Library Door to Sexual Exploitation.

In *New York v. Ferber*,⁶⁸ the United States Supreme Court stated that:

[T]he distribution network for child pornography must be closed if the production of material which requires the sexual exploitation of children is to be effectively controlled.

Today, the Internet constitutes a major part of the "distribution network" for child pornography. The Library should use filtering technology to close access *by adults* to all Internet based child pornography distribution networks.

After a rash of incidents involving individuals using public libraries to download child pornography, the pedophile-monitoring group "**PedoWatch.org**" made allegations that "on-line pedophiles" were telling each other to use public libraries to download child pornography. **PedoWatch** director **Julie Posey** stated:

Basically what happens out there is that pedophiles on the Internet "network" together. It is much like just about any other interest that a person may have. There are mailing lists, message boards, chat rooms and multitudes of other resources that they use. When a particular pedophile finds that the Library is a safe secure place to view and download pornography, he shares this information with others with his same interests that he comes in contact with. Some libraries won't allow downloading so that information is passed on too. Remember that before there can be child pornography in the first place, there has to be a perpetrator and a vic-

tim. I have seen cases where pedophiles on the Internet use the Library to talk with children and eventually lure them to have a face-to-face meeting. These children are then molested, photos taken and further exploited when he sends the child's pictures to masses on the Internet.⁶⁹

The development of computer technology has made the instant, electronic transfer of child pornography in many cases virtually undetectable by present law enforcement techniques, and made it invisible to Library management and staff. Today the entire contents of an illegal adult bookstore can be stored in and transmitted through computer networks. The technical expertise and resources of Internet-based criminals currently far surpasses that of federal and state law enforcement, and that of any Public Library. Internet filters used to screen and block adult access to proscribed materials, can help close the doors of the Public Library to the distribution network for child pornography, and can help deter the creation of "secondary effects" related to the regular and continuous dissemination of sexually explicit pornographic materials. In order for the law to be effective, law enforcement agencies need the support of all public entities — including the Public Library.

Internet Filter Use Advances Important Library Goals.

The "effectiveness" of filter technology has vastly improved since the United States Supreme Court first discussed and indicated support for "user-based software technology" in rendering the *Reno v. ACLU* decision.⁷⁰ The implementation of user-based Internet filtering technology directly and materially advances:

- (1) the goal of preventing minors from

continued on page 34

gaining access to pornographic materials that are harmful to minors.

(2) the goal of preventing adults from accessing and disseminating illegal pornography, such as obscenity or child pornography;

(3) the goal of preventing the creation or maintenance of a sexually hostile work environment in the Public Library, and preventing discriminatory conduct;

(4) the goal of preventing Public Libraries from becoming places that attract a variety of negative "secondary effects" that are commonly associated with establishments that disseminate sexually explicit pornographic materials primarily designed for an adult audience, as a substantial, continuous, regular course of conduct;

(5) the goal of aiding and supporting parents and/or the guardians of children in the discharge of their primary responsibility for their children's well-being;

(6) the goal of maintaining discipline and order, and limiting disruptions in the study or work environment of the Library;

(7) the goal of the minimization of providing access to illegal pornography;

(8) the goal of aiding and supporting federal and state criminal and civil laws designed to deter and punish trafficking in obscenity, child pornography, stalking, and harassment by means of computer;

(9) with respect to minors, the goal of excluding material which is "pervasively vulgar" or "educationally unsuitable" for the respective recipient age group;⁷¹

(10) the goal of preserving the "right of the Nation and the States to maintain a decent society," as has been discussed and explained in United States Supreme Court case law;⁷²

(11) the goal of conserving, properly allocating, and expediting management of limited library resources (including minimizing burdens on both staff and equipment); and

(12) the goal of effectuating and supporting Library Internet Use Policies that prohibit the use of Library property to access pornography.

Library Internet Filter Use is Expanding.

A thorough discussion of the propriety of Internet filter use is especially appropriate, in light of the fact that the number of Libraries offering public Internet access, as well as those implementing some type of Internet filter use, is rapidly expanding. A new study⁷³ by the U.S. National Commission on Libraries and

Information Science shows a dramatic increase in the number of Public Libraries using Internet filters. In 1998, just 1,679 public libraries offering public Internet access filtered some or all Internet access.⁷⁴ In 2000, that number more than doubled to 3,711,⁷⁵ representing an increase of 121%. One in four Public Libraries offering public Internet access now use filters.

Overall, 24.6% of Public Libraries offering public Internet access use filtering on some or all terminals.⁷⁶ This percentage represents an increase from 14.6% in 1998.⁷⁷ The fact that the number of Libraries filtering has more than doubled, while the overall percentage of Libraries filtering has not doubled is explained by the fact that the total population of Libraries offering public Internet access has increased from 11,519 in 1998⁷⁸ to 15,128 in 2000.⁷⁹

The most dramatic gains came in Libraries filtering some Internet access, which increased from 801 or 7.0% in 1998,⁸⁰ to 2,265 or 15.0% in 2000.⁸¹ Data from this study indicate that there has been a 65% increase in Public Libraries filtering all public Internet access since 1998. The number of Libraries that filter all access has climbed from 878 or 7.6% in 1998,⁸² to 1,446 or 9.6%.⁸³ Nearly 1,500 libraries (one out of every ten) filter all access today.

Issues Involved in Library Filter Debate

The Internet provides access to an enormous collection of data files. Some of the content of these data files is extremely useful, but some of it may be confusing, false, misleading, or illegal. There are foreseeable dangers associated with offering unfiltered Internet access in a Public Library setting that filtering software can help avert, so that Public Library facilities are preserved as an important educational resource to all members of the community.

Although federal law and many state laws specifically authorize Public Libraries to use Internet filters, a heated debate continues to rage over whether, and under what circumstances, Public Libraries that provide public Internet access may legally use filtering technology to block or screen access to certain types of materials that might be deemed objectionable for Library usage. This article examines in more detail some of the prominent issues involved, under the following sections:

1. What constitutes filtering?
2. Are filters reliable?
3. Is filtering of pornographic content within First Amendment boundaries?
4. If libraries do not filter out pornographic sites, are they subject to pornographic distribution laws?
5. Do parents have a right to expect libraries to exercise modest in loco parentis restraints with respect to the Internet?
6. What role should parents play in the

restriction of their children's reading materials?

7. What impact does filtering have on the library's ability to serve the public?

§ 1. What constitutes filtering?

Today, many public libraries provide access to the Internet as a service to their patrons. The Internet can be viewed as one vast network of computers, linked together to share information or resources, although it has been suggested that it is probably more useful to conceptualize it as merely a huge number of smaller computer networks connected in an arbitrary and self-organizing manner.⁸⁴

Many of the software applications that are needed to help Library patrons both efficiently utilize the Internet and protect Library property use some type of "filter." For example, filtering technology is employed by the search engines routinely used by all Internet users and **Internet Service Providers (ISPs)** to "find information about content." Filtering technology is also used by software designed to "block access" to objectionable content. The major difference between the two types of software products revolves around *what each program does with the information about content, once identified*. One product is designed to "grant" access, while the other is designed to specifically "deny" access.

Whether used for the purpose of granting or denying access to data files, present generation filtering technology is fairly robust. It has vastly improved since the mid-1990's—the era of the *Reno v. ACLU*⁸⁵ case, in which the *Reno* plaintiffs (including the **American Library Association** and the **American Civil Liberties Union**) forcefully argued that user-based software filtering technology was "effective" when used by parents to protect their children from Internet dangers. Today, as a technological tool Internet filters remain an *effective* protective measure that can *legally* be used to identify pornographic content on Websites, usenet newsgroups, and elsewhere on the Internet, as well as to block Library access to data files containing such content.

§ 1.1. Filters Described

A "Filter" is a program (or part of a program) that "examines a message for specified criteria and then processes it accordingly."⁸⁶ Filtering is used extensively by Blocking Software programs (sometimes referred to as "filtering software"). These devices prevent access to parts of the Internet that have been characterized as objectionable, based upon specified criteria. Internet filters have a wide range of uses. They can be designed to block specific Internet addresses, known as a "URLs" (uniform resource locators),⁸⁷ and can stop individuals from accessing particular Websites, newsgroups, mailing lists and chat lines, and can prevent the transmission of names, addresses, or offensive words.⁸⁸ Software can also be designed to block only the display of images, so that text is always available and no Website is ever completely blocked.⁸⁹ Some Browsers (the software for

continued on page 36

viewing Web pages) contain facilities for controlling access to Websites that meet set criteria.⁹⁰

Most Internet filters incorporate one or more of the following basic techniques:

1. Blacklists:⁹¹ Filters based on blacklists block access to a specific list of "inappropriate" sites, as compiled by individuals who evaluate them based on a specific standard, leaving access open to everything else.

2. Whitelists (also known as "go lists" or "greenspaces"):⁹² Filters based on whitelists permit access only to a selected list of "appropriate" sites, blocking entry to all else.

3. Word-rule blocking:⁹³ Filters based on a "word-rule" block sites that fit some rule (such as "block all sites that display the letter combinations "sex," "breast," or "xxx") leaving all other sites unblocked. The Word-rule filters may also sort a site based on the site's self-ratings according to the industry's "PICS" standard or based on "fuzzy logic."

(a) The **PICs standard (Platform for Internet Content Selection)**⁹⁴ is a method for rating the content of Websites. Originally designed to give parents, schools, and companies control over accessing content on the Internet (such as "pornography"), **PICs** can be used to rate a range of content. Although the primary responsibility for rating sites rests with owners, it is possible for third parties to rate sites. In order to use **PICs**, it is necessary to install special software on the user's computer, which then must be configured to "check the list" before allowing access to any of the listed sites. Many software companies have built support for **PICs** into their browsers and blocking software products. This would enable parents or network administrators to rate content on several different levels and allow access accordingly. Another similar method for rating the content of Websites is **RSAC (Recreational Software Advisory Council)**, which was originally created to rate computer games, and was meant to help parents shield children from excessive violence, obscene language and other "adult" content.⁹⁵ Both **PICs** and **RSAC** have been subjected to the following criticism:

[D]espite their elegant design and relative ease of implementation, almost nobody uses them. Site owners have not shown the hoped-for public-spiritedness, and the Web is just too big for third parties to rate it reliably. **PICs** will probably not go away, but its proponents may have to look for more dependable means of governing access to undesirable material.⁹⁶

(b) "Fuzzy Logic" is a method that relies on "artificial intelligence" to categorize objectionable material:

The computer looks at phrases, not just words, and uses an algorithm to assess the language in context. It also scans pictures and assesses the colors and tones of the pixels. Algorithms for such video searches are not yet mature, but an active and robust discipline of "video content analysis" or "object-based video coding" seeks to provide tools for this kind of query.⁹⁷

4. Image detection and analysis technology:⁹⁸ Filters based on image detection and analysis technology rely on the use of artificial intelligence software (similar to that developed by **NASA** in the 1980). Filters using this approach are designed to hunt and intercept actual images (such as **JPEG** and **GIF** files), and then evaluate them for objectionable content. Unlike other filtering products that surf the texts of **HTML** looking for pornographic words, the browser of this software embarks on an instantaneous search, intercepting the actual images (**JPEG** and **GIF** files), and then checks them to see if they are pornographic in content. The software is programmed to hunt for "tones of flesh and curves." One of the creators of filters employing this technique suggested that this type of approach could eventually result in the use of an algorithm that can be used to create a "plug-in" for **Netscape** or **Explorer**, and thereby make it possible to eliminate full-frontal nudity viewed in inappropriate places, such as the office workplace.

These basic filtering methods can be used separately or in combination. For example, in order to avoid "overblocking," software can be designed to block out sites according to one method, and can also provide an automatic override that unblocks any site that are on a specific whitelist.⁹⁹

§ 1.2. Technical Overview of Filters by COPA Commission.

When Congress enacted **The Child Online Protection Act**,¹⁰⁰ it created a Commissionally appointed panel (**The COPA Commission**) to study and "identify technological or other methods that will help reduce access by minors to material that is harmful to minors on the Internet." On July 20-21, 2000, the **COPA Commission** held public hearings on the topic: "Filtering, Labeling and Rating," at Richmond, Virginia. Speakers provided a technical overview of Filtering technologies, and described the use of various methods based upon the location of the blocking filter (e.g., either "client side" or "server side"¹⁰¹), and offered comments on their effectiveness.¹⁰²

Dr. Lorrie Faith Cranor, Senior Technical Staff Member in the Secure Systems Research Department at **AT&T Labs-Research Shannon Laboratory** in Florham Park, New Jersey,¹⁰³ provided an overview of available

technologies that promote safe and appropriate online experiences for children. According to her study of these devices (which appear to have included, but were not necessarily limited to filters), all generally provided mechanisms for:

- (1) Identifying or describing content of a particular type; and
- (2) Taking an action based on the type of content.¹⁰⁴

She stated that classification of content can be done by a variety of different parties, such as:

- (1) Third-party experts;
- (2) Automated tools (which can be used to classify content, or used only to assist human classifiers in finding "suspect sites");
- (3) Local Administrators (who may personally decide what content should be accessible). Some tools allow the person who configures the software to provide their own lists of "acceptable/unacceptable" content by URL or by providing a list of key words or phrases to be searched for automatically;
- (4) Content providers (who may rate or label themselves);
- (5) Surveys or votes (this technique has seen limited use for rating online content).¹⁰⁵

Dr. Cranor testified that various classification schemes maybe designed to identify content, based upon such factors as:

- (1) Age suitability;
- (2) Specific characteristics or elements of content, such as the language in which it is written, or whether it contains nudity or violence;
- (3) The entity that created the content (e.g., government or non-government sources).¹⁰⁶

Dr. Cranor stated that because Internet content is provided through a variety of protocols, including **HTTP** (Websites), **FTP**, **gopher**, **chat**, **Telnet**, instant messaging, and email, there are a variety of products on the market. Some products and services focus on one protocol, or a small number of these protocols, while others provide more comprehensive solutions. Some monitor only incoming communications, which others monitor both incoming and outgoing communications.¹⁰⁷

In studying filter tools, **Dr. Cranor** stated that filter tools can perform a range of action, based on content labels or characteristics of online content. For example, these tools can be designed to:

- (1) Suggest (recommend appropriate content);
- (2) Search (select content that is appropriate, and matches a query);
- (3) Inform (provide information about the content);
- (4) Monitor (record for later inspection a list of the content accessed or attempted to be accessed by a user);

continued on page 38

(5) Warn (provide information about content and recommend against accessing that content before it is displayed); and

(6) Block (prevent viewer from accessing content).¹⁰⁸

Dr. Cranor testified:

Tools for selecting content can be implemented in a variety of ways, through a number of different technical mechanisms and with a wide variety of user interfaces. Some of the important differentiators between tools include where the tool is located, how it can be updated, and how customizable it is.¹⁰⁹

She stated that the mechanisms for implementing content selection might be located in a variety of places in a computer system, such as on:

(1) The user's personal computer;

(2) LAN or local proxy server (for networked PCs). She observed that centralized configuration is easier for system administrators, and harder for individuals to tamper with;

(3) Internet Service Provider (some ISPs offer filtered Internet access, or may restrict or limit access to chat rooms, newsgroups, or other types of services);

(4) Remote proxy server (subscribers configure their browser software to pass all requests through the proxy server, which can offer filtering mechanisms as part of its service);

(5) Search engines (some return only pointers to content that has been designated as "appropriate");

(6) Website (some sites self-label certain content as "appropriate for children").¹¹⁰

Dr. Cranor explained that as new content appears, it must be continually classified so that tools that make use of classification information can stay "up to date" (noting, however, that there are tools that classify content "on-the-fly," for which this is not an issue). Some products and services are continuously updated, and include mechanisms for users to automatically update material, while others require users to manually download updates.¹¹¹

§ 2. Are filters reliable?

It is a statistical fact that all software contains "bugs" (i.e., hidden defects). Therefore, "reliability" of software can never be measured by evaluating the technology against a "zero-tolerance for mistakes" standard. Unintended results are an unfortunate, but accepted part of the nature of software.

The question of software reliability therefore becomes a comparison of "correct responses" versus "incorrect responses." The testing of software must include a statistically large enough test sample (i.e., computers can

easily test sites numbering thousands or hundreds of thousands) and be conducted under normal operational conditions, before any assessment can be considered an accurate appraisal of "reliability." With respect to the testing of Library filters for "reliability," actual logs of library access should be obtained,¹¹² and then "filtered" by the test software under normal operational conditions for a Library. This would remove the personal bias that has been exhibited in many so-called "tests" of filter reliability. The most recent example of an inadequately designed "test" appeared in the widely-publicized March 2001 *Consumer Reports*. This study has been subjected to legitimate criticism:

What a terribly superficial report on computer filters (*CR*, March 2001). Leaving aside some pretty shaky methodology (like a non-random sample of 86 sites used to test a population of maybe 40 million "inappropriate" pages - 2% of the Web by your own estimate), you extended your opinions to products you did not test. Your sidebar on current legislation drew no distinction between the institutional-grade filters used in schools and libraries and the household (non-server-based) products that you reviewed.¹¹³

A review of the language contained in two recent United States Supreme Court cases indicate that *user-based* Internet filters must be regarded as legally "reliable," given the guidance provided by *Reno v. ACLU*¹¹⁴ and *United States v. Playboy Entertainment Group, Inc.*¹¹⁵ These cases indicate that the United States Supreme Court accepted, at least in part, the arguments of the *Reno* plaintiffs that *user-based* software filtering technology was a viable and "effective" alternative that protected children from exposure to non-obscene pornographic materials that could be harmful to them.

Moreover, with the passage of 47 U.S.C. § 230(c)(2)(A), Congress has made the legal determination that in controlling and managing access to the Internet, the good faith use of filters is to be regarded as sufficiently "reliable for use," and is controlling with respect to whether filters can *legally* be used by Public Libraries in providing interactive computer services.

Internet filters are reliable and legally "effective," even if under the current "State of the Art" and using the "Best Available Technology," filtering software may not be "perfect," and even though various products chosen in good faith, may either "over" or "under" block. A range of malfunction is to be expected with any software product, which can be based upon oversights in software development or implementation.

Even where Internet filter use may occasionally result in unintended outcomes, this does not mean that from a legal standpoint filters cannot be relied upon or used by Public Libraries. As to the "actual effectiveness" of *user-based* filtering software to protect children, see the arguments made by the *Reno* Plaintiffs to the United States Supreme Court,

portraying such filter technology as a legally "effective" tool that can help shield children from exposure to sexually explicit pornography.¹¹⁶

§ 2.1. *Reno v. ACLU* (1997): User Based Filters Are Effective

*Reno v. ACLU*¹¹⁷ was the first Supreme Court case to discuss the nature and contours of "cyberspace." It was also the first time the Court addressed the legal potential for *user-based* screening technologies, as well as their legal "effectiveness."

Prior to *Reno*, it was not clear whether the Internet should be regulated as a "Broadcast medium" (such as radio or television) or a "Print medium" (such as a book or movie).¹¹⁸ *Reno* involved a challenge to several provisions of the 1996 **Communications Decency Act (CDA)**, which had banned the Internet transmission and display to minors of "indecent" or "patently offensive" material, using language that had been held constitutionally permissible for regulating a "Broadcast medium." The Court focused on this factor, expressing concern that the CDA had not used a "Print medium" approach.

The *Reno* Plaintiffs challenged the CDA provisions, asserting that they violated the First and Fifth Amendment by being overly broad and vague in their definition of "indecent" Internet communication (the transmission and display of which was made subject to the statute's criminal penalties). Presented with a question of first impression, the *Reno* Court held that the Internet must be governed by "Print medium" standards. The Court therefore struck the challenged provisions of the CDA, holding them to be overbroad when applied to the Internet in a "Print context."

To bolster their argument that the CDA provisions should be struck, the *Reno* Plaintiffs made an unusual argument regarding the "effectiveness" of *user-based* Internet filters. Plaintiffs urged that *user-based screening technology* designed to filter pornographic content on the Internet was *currently in existence* and legally constituted a "less restrictive, equally as effective" solution to the problem of protecting children from exposure to Internet pornography. In invalidating the challenged CDA provisions, the *Reno* Court relied in part on these representations of Plaintiffs relating to the "effectiveness" of *user-based* filters.

With respect to the effectiveness of *user-based* Internet filters, the Government had taken the opposite position in *Reno*, and had asserted that:

(1) because of the proliferation of Internet pornography and the difficulty of "keeping up" with the addition of new sites, the state of Internet filters as of 1996-1997 had not sufficiently advanced to be capable of addressing the magnitude of the problem, and therefore "user-based" filtering software was an "ineffective" tool for protecting children from Internet pornography. In

continued on page 40

order to protect children from exposure to harmful pornographic materials, the criminal provisions of the CDA, regulating sexually explicit content, presented the only "effective" solution; and (2) the District Court below had reached this same conclusion.

The *Reno* Plaintiffs forcefully disagreed (both in their written Briefs and at Oral Argument) with the position of the Government on both points, and urged that:

(1) *user-based* screening technology designed to filter pornographic content was already available and was legally "effective;" and

(2) the District Court below had reached this same conclusion, when it had summarized that there was a broad range of technologies and software programs that were effective and that they would soon be more widely available.

In *Reno* Plaintiffs told the United States Supreme Court that at least 30% of all indecent content posted on Websites originated from abroad. The *Reno* Plaintiffs asserted that because of the substantial presence of foreign pornography, as a practical matter it would be difficult, if not impossible, to effectively use the American criminal process to contain the dissemination of this type of harmful foreign Website material. They argued that criminal penalties for the dissemination of non-obscene indecent materials had to be regarded as completely ineffective in protecting children, and they affirmatively advocated that *user-based filtering technology* was a presently available, legally acceptable alternative, and was a more "effective" method of vindicating the compelling interest Government had in *completely* protecting children from exposure to such harmful material. The *Reno* Plaintiffs argued that (at least when it came to protecting children) any limitations in the technology (with respect to unintended malfunctions or oversights, that resulted in overblocking or underblocking) was "not a First Amendment issue," but was "a parental judgment issue."¹¹⁹

Since the *Reno* case, the market in illegal pornography has expanded.

As was observed by the *Reno* Plaintiffs, **American Library Association**, et al., in their United States Supreme Court Brief, in support of user-based Internet filters:

It is no answer to say that the CDA would initially reduce, perhaps by half, the volume of sexually oriented material available over the Internet by suppressing all domestic speakers. Because of the nature of Internet searching, such a reduction would have no effect on the ability of children — acting without supervision and using computers with no screening or blocking — to access sexually oriented images. It would be the equivalent of al-

lowing children to browse in "adult" bookstores after half the adult books or videos had been removed. Such a law would not "directly and materially" advance the goal of preventing minors from gaining access to indecent materials. See, e.g., *Church of Lukumi Babalu Aye v. City of Hialeah*, 508 U.S. 520, 113 S. Ct. 2217, 2234 (1993) ("It is established in our strict scrutiny jurisprudence that 'a law cannot be regarded as protecting an interest 'of the highest order' ... when it leaves appreciable damage to that supposedly vital interest unprohibited.'" (quoting *Florida Star v. B.J.F.*, 491 U.S. 524, 541-42 (1989)) (Scalia, J., concurring in part and concurring in the judgment); *Florida Star v. B.J.F.*, 491 U.S. at 540-41 (holding that law prohibiting disclosure of rape victims's name in any "instrument of mass communication" but not by other means did not directly and substantially further the law's stated purpose); *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97, 104-05 (1979) (invalidating a law that barred newspapers, but not other media, from publishing names of juvenile offenders). [FN45]

[FN45. See also *Denver Area*, 116 S. Ct. at 2416 ("Partial service of a compelling interest is not narrow tailoring.") (Kennedy, J., joined by Ginsburg, J.)] Had Congress inquired into how the Internet works, it would have learned that it is impossible to prevent minors from gaining access to a substantial volume of "indecent" material by regulating speakers. The solution to that problem must focus on the only place where effective measures can be taken—at the recipient end. [FN46]

[FN46. See Cannon, *supra*, at 83 ("Government regulation can do nothing to stop [offshore offensive material]. Software can effectively block sites regardless of location.").]¹²⁰

The *Reno* Court ultimately was persuaded in part by Plaintiffs' arguments concerning *user-based software filters*, when it consequently struck the challenged CDA provisions as overbroad. In its opinion, the *Reno* Court identified the following as a controlling "Finding of Fact" issued by the District Court, as to which there was no dispute:

[T]he evidence indicates that "a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available."¹²¹

The *Reno* Court repeated this conclusion, as forming a basis for its legal analysis:

[T]he District Court found that "[d]espite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their chil-

dren from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available." Id., at 842 (Finding 73).¹²²

At the time *Reno* was decided (in 1997), *user-based* filtering technology was a more limited tool than it is today. Nevertheless, it is important to note that the *Reno* Court accepted *user-based* Internet Screening software (even in its more primitive state) as constituting a reasonably effective, legally acceptable alternative that could protect minors from exposure to sexually explicit material. Subsequently, in *United States v. Playboy Entertainment Group, Inc.*,¹²³ the majority clarified the *Reno* Court's position with respect to its reliance on *user-based* Internet screening software, and indicated that this had definitely had some impact on the ultimate disposition of the *Reno* case:

[T]he mere possibility that user-based Internet screening software would 'soon be widely available' was relevant to our rejection of an overbroad restriction of indecent cyberspeech. *Reno v. U.S.* 521 U.S. 844 (1997), at 876-877.¹²⁴

§ 2.2. The COPA Commission Hearing on Filtering Technology

The **Child Online Protection Act**¹²⁵ created a Congressionally appointed panel (**The COPA Commission**) to study and "identify technological or other methods that will help reduce access by minors to material that is harmful to minors on the Internet." According to testimony before this **Commission**, the range of filters available with which to choose online content has greatly expanded in recent years. For example, **Susan Getgood**, Vice President and General Manager of **Cyber Patrol**, an Internet filtering software company, stated that:

Internet filtering is widely used, very effective and improving in response to demand from an increasingly sophisticated audience of parents and educators.¹²⁶

At the same hearing, **Dr. Lorrie Faith Cranor**, Senior Technical Staff Member in the Secure Systems Research Department at **AT&T Labs-Research Shannon Laboratory** in Florham Park, New Jersey, testified before the **COPA Commission** Hearing on Filtering, Labeling and Rating:

I have outlined the range of tools that support parents' ability to choose online content appropriate for their children. When I first inventoried these tools in 1997, I found about three dozen tools that were available at that time. At last check, *GetNetWise.org* had found over 120 tools that are currently available. The proliferation of tools in this area has led to increased innovation and the availability of tools to meet a wide variety of needs.¹²⁷

The issue of filters and "reliability" often evokes a range of responses, as observed by **Gordon Ross**, President and CEO, **Net**

continued on page 42

Nanny Software International, Inc., in his testimony¹²⁸ before the **COPA Commission**:

Few technologies have been given as much attention, generated such controversy and caused so much confusion. This is largely due to conflicting views about how they actually work versus how people think they work. One thing is certain — according to the **Annenburg Public Policy Center**, three-quarters of parents in the U.S. are concerned about what their kids are doing online and want to do something about it. There is clearly a need for filtering technology. Why is it that only one-third has chosen to use them?

Some argue that consumers don't think filters are necessary while others argue that consumers don't know enough about online dangers to recognize the need for filters. Still others claim that consumers are paralyzed by mixed messages. And it's no wonder. On one hand, filters are supported as effective alternatives to Internet legislation and, on the other, they are dismissed, as ineffective tools that threaten our right to free speech — at different times these opinions have even come from the same source! Given this discrepancy, it is understandable why filters have been slow to gain widespread adoption.¹²⁹

Mr. Ross emphasized that filters are becoming more effective, but operate within certain natural limitations:

Whichever option a parent chooses, the importance of parental or caregiver responsibility must not be underestimated. Using a filter doesn't mean that parents shouldn't continue parenting, it simply makes their lives a little easier and offers some peace-of-mind, by serving as an electronic extension of their own values system. It is crucial that parents ALWAYS pay attention to what their kids are doing online. They need to make sure that the filtering program is operational and hasn't been bypassed by their young "technical wizard." They also need to consider accessing a filter's logs and a browser's history file to see if their rules or instructions have been violated. By paying attention to their child's behavior and going online themselves to learn what their children are doing, parents and caregivers have the means to step in when necessary.

Client-side filters are often accused of failing to be 100% effective. Those of us, who have been in the industry for several years, understand that it is impossible to please 100% of the people 100% of the time. We do, however, listen closely to our supporters and our detractors so that we can adapt our tech-

nology to address their concerns. New tools are emerging that will allow the filtering programs to do a better job of keeping up with the massive growth of Internet content, however, it is impossible to capture every site that may be considered inappropriate for children. Innovation is a constant in the technology industry and filters continue to benefit greatly from constant feedback.¹³⁰

Mr. Ross expressed the opinion that like most things, filters are not perfect, but they will reach their potential if built with constructive input from those who are charged with their implementation:

It is my hope that people involved in protecting children and the integrity of the Internet will seek to find a middle ground where both goals can be met through accurate product and issue analysis, sharing of constructive ideas and a willingness to look beyond individual agendas to achieve a workable solution. The alternative is more confusion for consumers and the danger that both child safety and our constitutional rights will fall through the cracks. Like most things, client-side filters are not perfect, but they will reach their potential if they are built with constructive input from people who care. Ideally, their potential will be reached when people understand that filtering tools should never replace parenting in the digital age, but rather assist it. With the proper combination of technology, education and policies, we will succeed in protecting children online and preserving the integrity and openness of the Internet.¹³¹

Experts expressed continued confidence in the ability of filtering technology to reliably meet the needs of the Public Library, both now and in the future. This was forcefully stated in the concluding remarks of **Kevin Fink**, co-founder and Chief Technology Officer of **N2H2**, an Internet filtering software company. Regarding future advances in the filtering industry, he testified before the **COPA Commission**:

Internet filtering has progressed significantly since its introduction in the early days of the World Wide Web. The first filtering was implemented entirely on client computers, which limited the sophistication of the filtering and the security of the solution. The next wave of products moved to a server-based approach, which offered significantly more sophisticated, and thus accurate, filtering and an extremely secure solution. By centralizing control, however, some individual control was lost.

The next wave of filtering solutions, which are just coming on the market today, will diverge into two paths, depending on the network's requirements. Solutions geared towards ISPs, libraries, and other networks used by large

numbers of individuals with specific access needs will use a hybrid approach which will offer the power and security of server-based filtering along with the customizability of client software.

Solutions geared towards corporations, government agencies, schools, and other networks used by groups of users will continue to use a server-based approach, and will become more integrated into overall network architectures. They will work closely with routers, switches, firewalls, and other network hardware components. They will also become integrated with network management systems, so that network policy will be managed at a single point. In both cases, filtering systems will continue to rely more and more heavily on hybrid approaches, leveraging the intelligence and perception of human reviewers with the speed and tirelessness of computers. These solutions will use artificial intelligence for the tasks which humans aren't well suited to, like individually reviewing every product in an e-commerce database, and human intelligence for tasks which computers aren't well suited to, like differentiating between pictures of the **Mona Lisa** and pictures of "Mona's Mountains."

URL databases will also continue to become larger, more targeted, and more accurate. When **N2H2** began assembling our URL database in 1995, we had two categories: "naughty" and "nice," which were used for all of our customers, whether they were kindergarten classes or 12th-grade libraries. We added additional lists to accommodate different types of users, then moved to a category-based approach where our customers could build exactly the lists they needed. We continually add categories as our customers indicate the need for additional precision, as well as adding additional customization features such as local override databases and per-user category selection.

In general, filtering systems will become easier to manage and more accurate in their implementation of network policies. They will continue to evolve to keep pace with the evolution of the content they seek to categorize and the access they seek to control. They will also extend beyond "blocking" to offer more direction and help to users who are trying to find particular pieces of content. Now and in the future, these systems will help to encourage safe, knowledgeable, confident, and productive use of the World Wide Web. **N2H2** is working hard to ensure that we remain focused on satisfying our customer's needs, staying on the forefront of technology and service to allow them to take full advantage of all the Internet has to offer.¹³²

continued on page 44

Cyberage Endnotes

(continued from *ATG*, v.14#4, p.58)

Please Note: Because of the length of *Ms. Clancy's* article (about 60 pages) it was necessary to break it into two parts. The first part appears in *Against the Grain*, v.14#4, June 2002, p.58. Forums 3 and 4 in this series of forums, will appear in the next two issues of *Against the Grain*. The entire proceedings will also be available online at www.charlestonco.com.

68. 458 U.S. 747, 759 (1982).

69. See FilteringFacts, Press Release, dated March 6, 2000, "On-line Pedophiles Telling Each Other to use Libraries" (visited August 3, 2000) <http://www.filteringfacts.org/pedolib.htm>.

70. 521 U.S. 844 (1997). See *infra* discussion at '2. Are filters reliable?

71. See *Board of Education v. Pico*, 457 U.S. 853, at 871 (1982).

72. See *Paris Adult Theatre I v. Slaton*, 413 U.S. 49, at 59-60 (1973), quoting the words of the late Chief Justice Earl Warren in *Jacobellis v. Ohio*, 378 U.S. 184, 199 (1964)(dissenting opinion), who stated there is a "right of the Nation and of the States to maintain a decent society..."

73. *Public Libraries And The Internet 2000: Summary Findings And Data Tables*. A report based on research sponsored by the U.S. National Commission on Libraries and Information Science (NCLIS) and conducted by John Carlo Bertot and Charles R. McClure. NCLIS Web Release Version, September 7, 2000 (visited February 8, 2000) <http://www.nclis.gov/statsurv/2000plo.pdf> (hereinafter "Internet 2000").

74. *U.S. National Commission on Libraries and Information Science, Moving Toward Effective Public Internet Access: The 1998 National Survey of Public Library Internet Connectivity*. A report based on research sponsored by the U.S. National Commission on Libraries and Information Science and the American Library Association and conducted by John Carlo Bertot and Charles R. McClure. Washington, DC: U.S. Government Printing Office, 1999 (visited February 8, 2000) <http://www.nclis.gov/statsurv/1998plo.pdf> (hereinafter "The 1998 Survey"). Out of a total population of 11,519 public libraries providing public Internet access (see Figure 8, p. D-10), 878 or 7.6% filtered all terminals (see Figure 48, p. D-50), and 801 or 7.0% filtered some (see Figure 49, p. D-51).

75. Internet 2000, at Figure 11, p. 18. Out of a total population of 15,128 public libraries providing public Internet access (see Figure 4, p. 11), 1,446 or 9.6% filtered all terminals (see Figure 11, p. 18), and 2,265 or 15% filtered some (see Figure 11, p. 18).

76. Internet 2000, at Figure 11, p. 18.

77. *The 1998 Survey*, at Figure 48, p. D-50, and Figure 49, at p. D-51.

78. *The 1998 Survey*, at Figure 8, D-10.

79. Internet 2000, at Figure 4, p. 11.

80. *The 1998 Survey*, at Figure 49, D-50.

81. Internet 2000, at Figure 11, p. 18.

82. *The 1998 Survey*, at Figure 48, D-50.

83. Internet 2000, at Figure 11, p. 18.

84. See *Pocket Internet*, *supra* note 2, at 141.

Libraries In The Cyberage from page 42

This testimony emphasizes the fact filters are effective, but that "effectiveness" of filtering technology must be judged as part of an evolutionary process. The good faith implementation of filtering technology is critical to its success.

§ 3. Is filtering of pornographic content within First Amendment boundaries?

Filtering of pornography content for both adults and children can be fully consistent with First Amendment boundaries, if properly implemented. Care should be taken to create a record documenting the reasons for adopting a **Filtered Internet Access Policy**, a method for correcting unintentional under-blocking or over-blocking should be established, and dispute resolution procedures should be clearly identified.

Consistent with the requirements of the First Amendment, Public Libraries may block access to the following pornographic materials:

(1) **Obscenity.** Federal law completely bans the cyberspace transmission¹³³ of obscene pornographic material for all audiences (*i.e.*, it is illegal for both children and adults, including "consenting adults"¹³⁴). Under the so-called "*Miller test*," obscenity is pornographic material in which, taken as a whole, the following three essential elements coalesce or come together:

(a) prurient appeal (*i.e.*, an erotic, shameful or morbid attraction to nudity, sex, or excretion);

(b) sexual conduct (patently offensive representations or depictions of actual or simulated sexual conduct, including lewd exhibition of the genitals);

(c) lack of literary, artistic, political, or scientific value.¹³⁵

(2) **Child pornography.** Federal law completely bans the cyberspace transmission¹³⁶ of child pornography for all audiences (*i.e.*, it is illegal for both children and adults, including "consenting adults"¹³⁷). This type of pornographic material consists of a visual depiction of a minor (federal law defines this as "under 18 years of age"), engaged in actual or simulated sexual conduct, including a lewd or lascivious exhibition of the genitals.¹³⁸

(3) **Material Harmful to Minors.** Material Harmful to Minors (HTM) is a legal "term of art" used to describe a particular type of pornography that is regarded as "obscene for minors" and "harmful" when distributed to minors. When it is knowingly disseminated to minors, this type of pornography is not protected speech, and is therefore subject to regulation in cyberspace.¹³⁹ This term is much broader than either "obscenity" or "child pornography." Many states have laws that ban the dissemination of materials harmful to minors.¹⁴⁰ The problem with attempting to regulate this type of material on the Internet centers around the fact that the dissemination of "material harmful to minors" to adults is not

per se illegal, unless it is also "obscene" or "child pornography." However, Courts have recognized that the interest in protecting minors from HTM is "compelling."¹⁴¹ See the April 25, 2000 legal opinion from **South Carolina Attorney General** supporting Library Internet filter use to protect children, which concludes:

A public library is not an adult bookstore or pornographic peep show. The First Amendment does not prohibit public libraries from using Internet filters to protect minors from harmful, vulgar material. While the Internet is a powerful learning tool for children, it also poses substantial dangers to young people. Public libraries must therefore take steps to shield children from the salacious side of the Internet. Otherwise, they will be subject to potential liability for exposing minors to harm.

In other words, taxpayers do not have to stand idly by while their public library tax dollars are used to expose children to smut or indecent material. A parent would not expect his or her child to go to the public library and find "*Hustler*" next to *Hemingway*, or pornography along side *Pride and Prejudice*. Neither should it be any different because the Internet is now a mainstay of the public library.

The Internet filter provides a constitutional means to make sure children continue going to the public library in a safe, healthy environment. The purpose of the filter, as its name indicates, is to block out harmful, vulgar material from the reach of minors. A public library can constitutionally filter filth from the eyes of children. State and local governments possess a compelling interest in protecting minors from harmful material, from vulgar material and from offensive material. The Internet filter is the least restrictive means to carry out the duty to protect minors. It is thus our opinion that the Internet filter used by public libraries is constitutional under the First Amendment.¹⁴²

Attempts to regulate this type of pornography on the Internet have stimulated litigation.¹⁴³ A recent piece of federal legislation dealing with this subject, the **Child Online Protection Act (COPA)**, makes it a criminal offense to make any communication for commercial purposes by means of the World Wide Web that is available to minors and that includes material that is "harmful to minor," unless good faith efforts are made to prevent children from obtaining access to such material. This federal law bans commercial Websites from disseminating this type of material to minors, and requires that any commercial Website that distributes this type of material verify the "adult status" of recipients through the use of credit cards, adult access codes, adult PIN numbers, or other technologies that may be developed in the future.¹⁴⁴

continued on page 46

Cyberage Endnotes (continued)

85. 521 U.S. 844 (1997). In 1997, in *Reno v. ACLU*, the United States Supreme Court was examining the issue of what were legally acceptable alternatives for advancing the Government's interest in protecting children from non-obscene but harmful pornographic materials. The Plaintiffs, in that lawsuit, acknowledged that the government had an interest in protecting children from exposure to such materials, and made significant concessions regarding the effectiveness of Internet filter use in protecting children. See discussion *infra* at ' 2. Are filters reliable?.
86. See Pocket Internet, *supra* note 2, at 89.
87. *Id.*, at 188: a "Uniform Resource Locator" is an Internet address that describes the location of a specific site or document, usually on the World Wide Web. A complete URL describes both the Protocol used by the site in questions (HTTP, FTP, GOPHER, and so on) and a Domain Name (Website.com, for example).
88. *Id.*, at 55.
89. For an example of a filter that blocks access to visual pornography, but not access to text or to the actual Web page itself, see Biek, *supra* note 53.
90. *Id.*, at 55 and 57.
91. See Mark Nadel, "The First Amendment's Limitations on the Use of Internet Filtering in Public and School Libraries: What Content Can Librarians Exclude?" 78 *Texas Law Review* 1120-1121. (2000) (hereinafter Nadel). An updated version of this paper is available for download from the Social Science Research Network Electronic Library (SSRN), at <http://papers.ssrn.com> (visited February 8, 2001).
92. See *id.*
93. See *id.*
94. See Pocket Internet, *supra* note 2, at 155-156.
95. *Id.*, at 168-169.
96. *Id.*, at 156.
97. See Nadel, *supra* note 82, at 1120-1121, citing at footnote 13 John Tierney, Paid to Surf, and Filter, Net, *N.Y. Times* (D.C. ed.), Feb. 23, 2000, at A22, available in LEXIS, News Library, NYT File (discussing the 'fuzzy logic' Internet filter introduced at www.clicksafe.com), and also citing Andrew W. Appel & Edward W. Felten, Viewpoint: Technological Access Control Interferes with Non-infringing Scholarship, *COMMUNICATIONS OF THE ACM*, Sept. 2000, at 21, 22, citing E. Sahouria & A. Zakhor, Content Analysis of Video Using Principal Components, 8 *IEEE Trans. Circuits And Systems For Video Technology* 9 1290 (1999) and F. Pereira, et al., Introduction to the Special Issue on Object-Based Video Coding and Description, *id.*, at 1144.
98. See Jack Boulware, SALON.COM, "One small peep for man...NASA software is at the heart of a new product that could hunt for porn on the Internet," June 19, 2000 <http://www.salon.com>, which discusses the introduction of a Beta version of a new software product purportedly based on this innovative technology.
99. See Nadel, *supra* note 82, at 1120-1121.
100. The Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998) (codified at 47 U.S.C. ' 231) (COPA).

Libraries In The Cyberage from page 44

COPA takes an approach that is similar to state newsrack laws that have been upheld in the Courts. Compare, for example, California Penal Code § 313.1(c)(2), which makes it a criminal offense to knowingly display, sell, or offer to sell "harmful matter" (so-called "soft-core" pornography, even if the material is not obscene or illegal for adults), in any coin-operated vending machine that is not supervised by an adult and that is located in a public place, other than a public place from which minors are excluded. The California newsrack statute was intended to address the following problem: For years, "smut peddlers" had taken material (which they would label as, "For Sale to Adults Only") out of so-called "adult" businesses and the "adult" section of businesses open to minors, and would place it in public news racks, knowing that children with the correct change could and did purchase the material. There is no First Amendment right to exploit children in this way.

§ 313.1(c)(2) of the California Penal Code corrected this situation, and was upheld by the federal courts.¹⁴⁵ In *Crawford*, the publishers of the *Sun* magazine and others brought a legal action in federal court, challenging the Constitutionality of the California news rack statute. The publishers were granted a temporary restraining order and then successfully obtained a preliminary injunction against enforcement by the U.S. District Court. However, after a trial on the merits, the U.S. District Court's final ruling held that the statute "is declared to violate no provision of the Constitution either on its face or as applied to plaintiffs."

The publishers appealed to the Ninth Circuit Court of Appeals, continuing their attack on the newsrack statute, arguing that the law was written too broadly and that it substantially interfered with the ability of adults to obtain their publications. The Ninth Circuit, by a vote of 3-0, disagreed, stating:

[T]he statute is effective in limiting the children's exposure and has a narrow focus, which still allows adults to purchase the materials from alternative sources.¹⁴⁶

According to the three-judge federal panel:

[T]he state's compelling need to protect children from these publications has been satisfied by the use of a statute which accomplishes the purpose with a precision that protects our First Amendment interests.¹⁴⁷

(4) Sexually Explicit Pornographic Visual Displays Used to Sexually Harass. Displays of sexually explicit pornographic materials are not protected by the First Amendment when used for an improper purpose, such as illegal sexual harassment (where the creation of a hostile work environment results). Sexually explicit pornography is not protected speech where it acts as "discriminatory conduct"

creating a hostile work environment under either federal or state law, since there is no right to make use of even protected speech for purposes of sexual or racial harassment or discrimination.

Pornography in the workplace can constitute, or be evidence of, sexual harassment in violation of state and federal civil rights laws and create or contribute to a hostile environment in violation of Title VII's general prohibition against sexual discrimination in employment practices.¹⁴⁸ Pornographic displays contribute to the creation of work environments which are "heavily charged" or "heavily polluted" with sexual abuse, which are at the core of the hostile environment theory. There is a compelling interest in cleansing the workplace of impediments to the equality of women, and in eradicating discrimination against women. See *Roberts v. United States Jaycees*.¹⁴⁹ Banning the "reading or otherwise publicizing in the work environment materials that are in any way sexually revealing, sexually suggestive, sexually demeaning or pornographic," and "banning sexist speech in the workplace does not censor such speech everywhere and for all time." See *Robinson v. Jacksonville Shipyards*.¹⁵⁰

The problem with providing unfiltered access to Internet pornography is that it can foreseeably result in a statistical increase of inappropriate sexual conduct or sexually harassing behavior, which in turn can create a hostile environment constituting sexual harassment in violation of state and federal civil rights laws. The benefit of Internet filters is that their use in connection with offering Library interactive computer services can be regarded as a "reasonable step" taken to prevent instances of sexual harassment, where the record demands that some action be taken.

Where there is some notice of objectionable conduct, the failure to take "reasonable steps" to prevent sexual harassment from occurring may subject a Public Library to potential liability. Compare *Oona, R.S. v. McCaffrey et al.*,¹⁵¹ in which a complaint was filed seeking to hold school officials liable for failure to prevent sexual harassment from two different sources: (1) failure to take steps to prevent inappropriate conduct by a student teacher; and (2) failure to take steps to prevent male students in the class from harassing the females, thereby creating a hostile environment for Plaintiff and her female classmates.

The court found that school officials were under a duty imposed by Title IX of the Education Amendments of 1972, 20 U.S.C. Section 1681 et seq. (as amended), to take reasonable steps to prevent sexual harassment of students:

We stress that the issue before us is narrow. We do not consider what steps school officials may reasonably be required to take to address harassment by fellow students, or when they are required to take them. Hence, we do not consider the extent to which such action may differ from the action reasonably expected of employers to remedy

continued on page 47

harassment by fellow employees. We hold only that in this circuit the duty to take reasonable steps to remedy a known hostile environment created by a peer is clearly established. Parents have long had a right to expect school officials to do what they reasonably can to protect the children who are temporarily in their custody and to provide an appropriate learning atmosphere. The dissent's position that there is a duty under Title IX to remedy one type of sex discrimination but not another is contrary to controlling authority and to parents' expectations.

Defendants' conduct also violated **Oona's** clearly established rights under Title IX by failing to supervise **Ibach**. A supervisor may be found liable under § 1983 if the supervisor is "aware of a specific risk of harm to the plaintiff." *Ketchum v. Alameda County*, 811 F.2d 1243, 1247 (9th Cir.1987). This court has also held that, as early as 1988, "complete inaction in the face of claimed harassment cannot be objectively reasonable conduct entitling a supervisor to qualified immunity." *Bator v. Hawaii*, 39 F.3d 1021, 1029 (9th Cir.1994) (denying qualified immunity in a § 1983 action where the violation took place in 1988).

Oona has alleged that defendants here, who were all in supervisory positions to **Ibach**, knew or had reason to know that **Ibach** sexually harassed, fondled, and inappropriately touched **Oona**. **Ibach's** alleged conduct of sexually harassing a student constitutes sex discrimination, in violation of **Oona's** federal rights under Title IX. See *Franklin*, 503 U.S. at 75, 112 S.Ct. at 1037-38. Thus, after *Franklin*, a school official in a supervisory position cannot claim immunity for the failure to respond to complaints of harassment and discrimination. Other circuits have reached this conclusion as well. See *Claiborne*, 103 F.3d at 515 (holding that elements to state a supervisory hostile environment claim under Title VII equally apply under Title IX); *Rosa H. v. San Elizario Indep. Sch. Dist.*, 106 F.3d 648, 660 (5th Cir.1997) (finding Title IX liability for supervisory school officials with actual knowledge of sexual abuse or harassment). The allegations that defendants knew of **Ibach's** behavior and failed to prevent it are sufficient to show violations of clearly established Title IX rights during the 1992-93 year.¹⁵²

In *Mainstream Loudoun v. Board of Trustees of the Loudoun County*,¹⁵³ the U.S. District Court for the Eastern District of VA., Alexandria Division, reviewed a Library Internet Policy ostensibly designed to prevent "Internet

Sexual Harassment." The Court found the Policy to be invalid on the grounds that it was "over-inclusive," and was not narrowly tailored to advance any state governmental interest. Noting that the Library may have had a legitimate interest in regulating obscenity and child pornography, the Court specifically assumed that minimizing access to illegal pornography and avoidance of creation of a sexually hostile environment were compelling government interests. Yet because of an *inadequate record*, the Court found that the "Library Internet Sexual Harassment Policy" was not tailored to advance those interests.

On its face, the *Loudoun* Policy permitted all patrons, adult and juvenile, to access only material deemed fit for juveniles (*i.e.*, only material deemed "not harmful to minors"), in order to avoid instances of "sexual harassment." However, the Court noted that distribution to adults of at least some of the restricted material may be protected by the First Amendment. Because any prior restraint of "protected speech" warrants a more stringent review by the Court, the implementation of the Internet Sexual Harassment Policy had to meet the "strict scrutiny" test. The trial judge held that the record was *factually insufficient* to prove that the government's interest in preventing "sexual harassment" had been sufficiently implicated, under a strict scrutiny standard:

To satisfy strict scrutiny, defendant must do more than demonstrate that it has a compelling interest; it must also demonstrate that the Policy is necessary to further that interest. In other words, defendant must demonstrate that in the absence of the Policy, a sexually hostile environment might exist and/or there would be a problem with individuals accessing child pornography or obscenity or minors accessing materials that are illegal as to them. Defendant "must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way. [cites omitted]. '[S]imply alleging the need to avoid harassment is not enough[.]. . . the defendant[] must show the threat of disruption is actual, material, and substantial.'") The defendant bears this burden. . . ."¹⁵⁴

On the record, the defendant *failed to factually demonstrate* that the Policy was reasonably necessary to further compelling state interests, and that the Policy was narrowly tailored to achieve those interests. The Court stated that the Policy was not narrowly tailored, because it appeared that less restrictive means were available to further defendant's interests (*i.e.*, reduction of sexual harassment). In order to "save" the Policy, the defendants urged that the Court should rule on the broader issue of:

[W]hether a public library can or cannot filter obscene materials on its public Internet terminals and, if so, under what criteria and procedures.¹⁵⁵

The Court refused to answer this question,

Cyberge Endnotes (continued)

101. See, for example, *Hearing on Filtering, Labeling and Rating Before the Commission on Online Child Protection (COPA)* (July 2001) (written statement of Gordon Ross, President and CEO, Net Nanny Software International, Inc.) (hereinafter Ross) (visited February 5, 2001) www.copacommission.com/meetings/hearing2/ross.test.pdf.

102. The testimony regarding the design and use of filters can be accessed via the Internet at: <http://www.copacommission.org/meetings/hearing2/agenda.shtml> (visited February 5, 2001).

103. See *Hearing on Filtering, Labeling and Rating Before the Commission on Online Child Protection (COPA)* (July 2001) (written statement of Dr. Lorrie Faith Cranor) (hereinafter Cranor) (visited February 5, 2001) <http://www.copacommission.com/meetings/hearing2/cranor.test.pdf>. Dr. Cranor is Senior Technical Staff Member in the Secure Systems Research Department at AT&T Labs-Research Shannon Laboratory in Florham Park, New Jersey. She is chair of the Platform for Privacy Preferences Project (P3P) Specification Working Group at the World Wide Web Consortium. Her research has focused on a variety of areas where technology and policy issues interact, including online privacy, electronic voting, and spam. In 1997 Dr. Cranor co-authored a report (updated in 1998) on tools that support parents' ability to choose online content appropriate for their children.

104. See Cranor, *supra* note 94, at p. 1.

105. *Id.*, at 1-2.

106. See Cranor, *supra* note 94, at 2.

107. *Id.*

108. *Id.*, at 2-3. See also Ross, *supra* note 92, at 3: "Many people think that if a filter is installed, it automatically blocks access to content. In many cases, parents choose other options that don't involve blocking at all."

109. *Id.*, at 4.

110. *Id.*

111. *Id.*

112. Compare, for example, the methodology utilized in Biek, *supra* note 53, a study using actual logs of Library access to determine the demographics of the Internet Users at the Tacoma Public Library, with a special reference to the issue of Internet pornography. "The study showed that 96% of the intercepts did indeed conform to the requirements of the policy of the Tacoma Public Library — that the pictorial content of the site included — graphic materials depicting full nudity and sexual acts which are portrayed obviously and exclusively for sensational or pornographic purposes." A confidence interval of 3.11 at the 95% confidence level is indicated for a sample of this size. Biek, at 23-24, endnote 2.

stating that the issue was not before the Court:

In other words, the defendant asks this court to consider a hypothetical situation that is not before us. The federal court, however, may not provide advisory opinions; we may rule only on the Policy before us. Defendant cannot save its Policy by asking the Court to decide hypothetical questions for which there is no case or controversy.¹⁵⁶

The trial enjoined implementation of the
continued on page 50

Cyberage Endnotes (continued)

113. Bruce Watson, President, Enough Is Enough, Letter to David Heim, Managing Editor, *Consumer Reports*.
114. 521 U.S. 844 (1997).
115. 529 U.S. 803 (2000).
116. See *Reno v. ACLU, et al.*, No. 96-511, United States Supreme Court, October Term, 1996: Brief for Appellees, filed February 30, 1997 on behalf of the following Reno Plaintiffs: Electronic Privacy Information Center, Electronic Frontier Foundation, Legal Action for Reproductive Rights, Planned Parenthood Federation of America, American Civil Liberties Union Foundation, and ACLU of Pennsylvania Foundation, 1997 WL 74378; and Brief of Appellees American Library Association, *et al.*, filed Feb. 20, 1997, 1997 WL 74380. Listen to the RealAudio sound recording version of the oral argument in *Reno v. ACLU*, available from The Oyez Project/ Northwestern University (visited February 9, 2001) at <http://www.oyez.com>. This Website provides audio recordings of oral argument in selected United States Supreme Court cases. Visitors can hear the oral argument that occurred on March 19, 1997, in *Reno v. ACLU*, by using the Oyez Website search feature to request *Reno v. ACLU*, 521 U.S. 844 (1997). However, in order to listen to the recording, it is necessary to use the software program "RealPlayer." (The Oyez Website contains instructions regarding how RealPlayer can be downloaded free from the Internet.) References in this paper to the *Reno v. ACLU* oral argument were not taken from an official written transcript, but were manually transcribed using the RealAudio sound recording version available from The Oyez Project. (Note that some inaccuracies may be present because of the possibility of hearing and sound difficulties in transcription.) In order to access an identified timed portion of the argument, on the RealPlayer screen, select "Play," then select "Seek To," then type in the designated time of reference.
117. 521 U.S. 844 (1997).
118. In regulating the Internet, Great Britain had taken a "Broadcasting approach." See *MSN News* (May 16, 1997), reporting that users of the British Interactive Broadcasting service, a system which was scheduled to bring T.V. Internet access to an estimated 20 million television owners, would have to comply with the independent Television Commission rules. The report noted that "[t]he prevalence of copyright infringement and sexual material on the Web made much of the content unsuitable for broadcasting."
119. *Reno v. ACLU* Oral argument, at 00:51:46. See *supra* note 107.
120. Brief of Appellees American Library Association, *et al.*, at 33-34, in *Reno v. ACLU, et al.*, No. 96-511, United States Supreme Court Appellee Brief, October Term, 1996, filed Feb. 20, 1997, 1997 WL 74380.
121. *Reno*, 521 U.S. 844, at 855, citing District Court Finding No. 73.
122. *Id.*, at 877.
123. 529 U.S. 803, 120 S.Ct. 1878 (2000).

Libraries In The Cyberage from page 47

Library Internet Sexual Harassment Policy. This decision was not appealed, so it remains only a trial court decision, with limited or no value as precedent. It should also be noted that a variety of commentators have criticized the trial court's analysis (particularly with respect to the discussion of whether the Internet presents a "forum" issue, that would require elevated Court scrutiny). It is open to debate whether the implementation of all Library Internet Use Policies must be evaluated under a strict scrutiny standard. See, for example, the April 25, 2000 legal opinion from **South Carolina Attorney General**¹⁵⁷ which supports Library Internet filter use. See, also, **Center for the Community Interest**, "Making Public Libraries Safe for Children: The Constitutionality of Restricting Access to Pornography on Library Internet Terminals."¹⁵⁸

The Library encountered a major problem in the *Loudoun* case, because it could not prove to the trial court's satisfaction that there was a link between "sexual harassment" (the governmental interest supporting its Library Internet Policy) and providing unfiltered Internet access to non-obscene sexually oriented materials:

The only evidence to which defendant can point in support of its argument that the Policy is necessary consists of a record of a single complaint arising from Internet use in another Virginia library and reports of isolated incidents in three other libraries across the country. In the **Bedford County Central Public Library** in Bedford County, Virginia, a patron complained that she had observed a boy viewing what she believed were pornographic pictures on the Internet. See Pls.Ex. 15 at 4-7. This incident was the only one defendant discovered within Virginia and the only one in the 16 months in which the Bedford County public library system had offered unfiltered public access to the Internet. After the incident, the library merely installed privacy screens on its Internet terminals which, according to the librarian, "work great." *Id.* at 4.

The only other evidence of problems arising from unfiltered Internet access is described by **David Burt**, defendant's expert, who was only able to find three libraries that allegedly had experienced such problems, one in Los Angeles County, [footnote omitted] another in Orange County, Florida, [footnote omitted] and one in Austin, Texas. [footnote omitted] See Burt Rep. at 14. There is no evidence in the record establishing that any other libraries have encountered problems; rather, **Burt's** own statements indicate that such problems are practically nonexistent. See Burt Dep. at 253-55 (acknowledging that an email requesting information about sexual harassment complaints

relating to Internet use that he sent to "several thousand" librarians did not yield a single serious response). Significantly, defendant has not pointed to a single incident in which a library employee or patron has complained that material being accessed on the Internet was harassing or created a hostile environment. As a matter of law, we find this evidence insufficient to sustain defendant's burden of showing that the Policy is reasonably necessary. No reasonable trier of fact could conclude that three isolated incidents nationally, one very minor isolated incident in Virginia, no evidence whatsoever of problems in Loudoun County, and not a single employee complaint from anywhere in the country establish that the Policy is necessary to prevent sexual harassment or access to obscenity or child pornography.¹⁵⁹

Since the *Loudoun* decision, evidence linking unfiltered Library Internet access to visual depictions of pornography has geometrically expanded. The record has substantially changed in light of reports such as *Dangerous Access 2000 Edition*¹⁶⁰ and *The Greenville County Library Board Report*,¹⁶¹ neither of which were available to the *Loudoun* trial court. Reports of legal action being taken by Library staff are now surfacing¹⁶² that protest acts of "sexual harassment" linked to the presence of unfiltered access to Internet pornography in the Library workplace. These complaints are not confined to just American libraries, but have become international. The universal frustration of Library workers was aptly expressed by one Dublin, Ireland librarian, who complained that both he and his staff were constantly exposed to "sick sex sites:"

I have seen kids as young as eight-years-old looking at beastiality sites... Why should we have to look at pictures of a father raping his daughter when we are simply trying to do our jobs?¹⁶³

(5) Non-Obscene Sexually Explicit Pornography: Restricting Dissemination Zones. Under an approach common in land use cases, the state police power may be used to control the "time/place/manner" in which non-obscene sexually explicit pornography (as a generic category) may be disseminated. As a matter of law, distinctions based upon "sexual explicit content" have been treated as "content neutral regulations," as long as they are aimed at restricting "sexually explicit materials" as a *generic category*, and are not designed to restrict the "viewpoint" of a particular speaker. These regulations must be narrowly tailored to advance the governmental interest involved, and reasonable, alternative avenues of communication should be left available.¹⁶⁴

It is permissive to categorize and control "sexually explicit materials," and to treat them in a manner different from other materials, because of the governmental interests involved. These interests include the goals of protecting minors, and public health and safety concerns. It also includes curbing the "sec-

continued on page 52

Cyberage Endnotes (continued)

124. 529 U.S. 803, 120 S.Ct. 1878, at 1887 (2000). See observation made in the *Playboy* case by the Brief of the Media Institute, as Amicus Curiae in support of Appellee, 1999 WL 766039, at pages 16-17: "In *Reno* the Court relied in part on user-based control of the technology to keep the Internet free of government restrictions. . . ." This approach of relying on user control that technology facilitates, rather than broad government fiat, should apply generally to electronic media. . . . For the Internet, as the Court acknowledged in *Reno*, 521 U.S. at 876-77, parents can use ever more sophisticated and powerful software to filter the material their children can access.
125. See *supra* note 91.
126. See *Hearing on Filtering, Labeling and Rating Before the Commission on Online Child Protection (COPA)* (July 2001) (written statement of Susan Getgood, Vice President and General Manager, Cyber Patrol at 1) (visited February 5, 2001) <http://www.copacommission.com/meetings/hearing2/getgood.test/pdf>.
127. See Cranor, *supra* note 94, at p. 5.
128. See *supra* note 92.
129. See Ross, *supra* note 92, at 1.
130. *Id.*, at 4.
131. *Id.*, at 8.
132. See *Hearing on Filtering, Labeling and Rating Before the Commission on Online Child Protection (COPA)* (July 2001) (written statement of Kevin Fink, Chief Technology Officer, N2H2, Inc.).
133. See *Reno v. ACLU*, 521 U.S. 844, at 877, footnote 44 (1997).
134. See *Paris Adult Theatre v. Slaton*, 413 U.S. 49 (1973).
135. For a more complete explanation of the three-prong constitutional criteria for obscenity, see *Miller v. California*, 413 U.S. 15 (1973). See also *Smith v. United States*, 431 U.S. 291, at 300-02, 309 (1977); and *Pope v. Illinois*, 481 U.S. 497, at 500-01 (1987). See, also, *Mishkin v. New York*, 383 U.S. 506, 508 (1966), and Taylor, B., "Hard-Core Pornography: A Proposal for a Per Se Rule," 21 *U. Mich. J. Law Ref.* 255 (1988).
136. See *Reno v. ACLU*, 521 U.S. 844, at 877, footnote 44 (1997).
137. See *Paris Adult Theatre v. Slaton*, 413 U.S. 49 (1973).
138. See *New York v. Ferber*, 458 U.S. 747 (1982); *Osborne v. Ohio*, 495 U.S. 103 (1990); *United States v. X-Citement Video, Inc.*, 513 U.S. 64 (1994). See also *United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *cert. den.*, 484 U.S. 856 (1987); *United States v. Knox*, 32 F.3d 733 (3rd Cir. 1994), *cert. den.* 513 U.S. 1109 (1995). Note that in 1996, the federal law was amended (adding 18 U.S.C. ' 2252A, and amending 18 U.S.C. ' 2256) to specifically include as *child pornography* any visual depiction that is or appears to be that of an actual minor engaging in *sexually explicit* conduct. See *United States v. Hilton*, 167 F.3d 61 (1st Cir. 1999), *cert. den.* 528 U.S. 844 (1999); *United States v. Acheson*, 195 F.3d 645 (11th Cir. 1999); and *United States v. Mento*, 231 F.3d 912 (4th Cir. 2000), *petition for cert. filed* (Jan. 22, 2001) (No. 00-8114) [upholding law]. But see *Free Speech Coalition v. Reno*, 198 F.3d 1083 (9th Cir. 1999), *reh. denied* 220 F.3d 1113 (9th Cir. 2000), *cert. granted sub. nom. Ashcroft v. Free Speech Coalition*, 121 S.Ct. 876, 69 USLW 3382 (U.S. Jan 22, 2001) (No. 00-795) [invalidating law].

Libraries In The Cyberage from page 50

ondary effects" commonly associated with establishments that disseminate sexually oriented materials as a regular course of conduct. "Secondary effects" can include the following problems:

1. increased crime (both against the person and against property)
2. increased potential for the spreading of sexually transmitted diseases
3. increased potential for sexual harassment
4. increased environmental blighting effect
5. increased traffic, noise, and disruptive behaviors (such as "cruising" activities)
6. may result in public littering of pornographic materials
7. may attract an undesirable quantity and quality of transients
8. may encourage law abiding citizens to move elsewhere

In the land use planning context, "Porn-free" zones may be created, in order to protect places designated as "sensitive uses" from the harmful "secondary effects" associated with establishments that disseminate non-obscene sexually explicit pornography as a substantial, continuing and regular course of conduct. "Sensitive uses" can include places where children regularly congregate (e.g., libraries, schools, churches, residential areas), as well as other areas of the city that could be adversely affected by harmful "secondary effects."

There is an analogy to be drawn between these land use cases that regulate the so-called "adult" bookstore, and the case in which a Public Library gains the reputation as a place that provides easy, continuous access to sexually explicit pornography. Moreover, providing unfiltered Library Internet access to children is the "equivalent of allowing children to browse in 'adult' bookstores."¹⁶⁵

Internet access has been shown to act like a magnet, attracting in particular male adolescents as an identifiable group, who repetitively attempt to violate Library policies against accessing Internet cyberporn. A recent Tacoma, Washington, study¹⁶⁶ analyzed use of library computers by patrons who were attempting to find sexually explicit materials on the Internet. Using actual Library Internet logs, substantial cyberporn trafficking requests by both minor and adult Library patrons were discovered: *during a one-year period a total of nearly 28,000 attempts to access sexually explicit materials were made.* This study indicated that cyberporn-seeking activity was heaviest among males between the ages of 12 and 15, and that most of all such activity took place in the after-school hours in branch libraries that were heavily used by young people during those times.

In addition, the Tacoma study also found that all patrons who sought sexually explicit

materials exhibited directed and intentional behavior, concluding that for some it was likely to be the primary reason for visiting the Library:

There is a near-absence of correlations between pornography-seeking behavior in the library and other aspects of library use. This makes it clear that such behavior is directed and intentional. It is likely for some individuals to be the primary reason for visiting the library.¹⁶⁷

This study demonstrates that Internet access can act as a magnet for both children and adults, who may come to the Library *only* to view cyberporn, and that there are indications that the level of cyberporn trafficking regularly sought from an average Library Internet (as documented by *actual* Library logs) should be regarded as a continuous and substantial figure (*i.e.* nearly 28,000 requests).

Other reports describe situations that have already occurred, where providing unfiltered Library Internet access can be associated with the creation of a number of diverse secondary effects. See, for example, *Dangerous Access 2000 Edition*,¹⁶⁸ *supra*, and *The Greenville County Library Board Report*,¹⁶⁹ *supra*. Internet filters should be used to combat these secondary effects and to protect the Public Library premises as a "sensitive use."

§ 4. If libraries do not filter out pornographic sites, are they subject to pornographic distribution laws?

A recent *Tennessee Attorney General's Opinion*¹⁷⁰ answered this question in the affirmative, expressing the opinion that a Public Library would be subject to state pornographic distribution laws, provided that the following three elements are present:

1. The Library does not filter out pornographic sites (that meet the statutory definition of "material harmful to minors"); and
2. The Library *knowingly* permits a minor to have access to pornographic material (proscribed by law) on the Internet, *having knowledge of the content and character of the specific material viewed by the minor*; and
3. A minor accessed pornography or viewed the computer screen of an adult accessing pornography on Library Internet computers.

The Opinion, *inter alia*, examined the following two related questions:

- (1) If a Public Library provides Internet access to patrons, would the library violate Tenn. Code Ann. § 39-17-911(a)(1) if a minor accessed pornography or viewed the computer screen of an adult accessing pornography?¹⁷¹
- (2) Would the statute be violated if the library used filtering software in an effort to avoid making such material available to minors even though the software will not block every pornographic site?¹⁷²

continued on page 54

Cyberage Endnotes (continued)

139. See *Ginsberg v. New York*, 390 U.S. 629 (1968). See also *Com. v. Am. Booksellers Ass'n*, 372 S.E.2d 618 (Va. 1988), followed, *Am. Booksellers Ass'n v. Com. of Va.*, 882 F.2d 125 (4th Cir. 1989); *Crawford v. Lungren*, 96 F.3d 380 (9th Cir. 1996), cert. den., 520 U.S. 1117 (1997). See also *supra* note 24, and accompanying text.
140. See the concurring and dissenting opinion of Justice O'Connor, in *Reno v. ACLU*, 521 U.S. 844 (1997), at 887, footnotes 1 (listing states that have denied minors access to certain establishments frequented by adults) and footnote 2 (listing states that have denied minors access to speech deemed to be *Harmful to Minors*). Some state exempt libraries from the operation of such laws, while other states do not. See, *infra*, at * 4. If libraries do not filter out pornographic sites, are they subject to pornographic distribution laws?
141. See *New York v. Ginsberg*, 390 U.S. 629 (1968), and *Reno v. ACLU*, 521 U.S. 844 (1997).
142. 2000 WL 655474 (S.C.A.G.).
143. See, for example, *Reno v. ACLU*, 521 U.S. 844 (1997). See also *infra* note 135.
144. This law is being challenged in the Court system. The federal trial court issued a preliminary injunction in *ACLU v. Reno*, 31 F.Supp.2d 473 (E.D. Pa. 1999)(preliminary injunction granted); *aff'd* 217 F.3d 162 (3rd Cir. (Pa) 2000)(upholding issuance of temporary injunction, and barring enforcement of COPA on First Amendment grounds because it relies on community standards to identify material that is harmful to minors); *petition for cert. filed* February 2001, *sub nom. Ashcroft v. ACLU*, No. 00-1293.
145. See *Crawford v. Lungren*, 96 F.3d 380 (9th Cir. 1996), cert. den. 520 U.S. 1117 (1997).
146. *Id.*, at 387.
147. *Id.*, at 389.
148. See 42 U.S.C. ' 2000e-2; 29 CFR ' 1604.11; 18 U.S.C. ' 242; 42 U.S.C. ' 1981, 1982. See *Pornography, Equality, and a Discrimination-Free Workplace: A Comparative Perspective*, 106 *Harvard Law Review*, pp. 1075-92 (1993); *Robinson v. Jacksonville Shipyards*, 760 F. Supp. 1486 (M.D. Fla. 1991). See also *supra* note 26, note 27, note 42, and accompanying text.
149. 468 U.S. 609, 628 (1984). See *supra* note 25, and accompanying text.
150. 760 F. Supp. 1486 (M.D. Fla. 1991). See *supra* note 26, and accompanying text.
151. 143 F.3d 473 (9th Cir. 1998).
152. *Id.*, at 478-479.
153. *Mainstream Loudoun v. Board of Trustees of the Loudoun County*, U.S. District Court for the Eastern District of VA., Alexandria Division, Civil Action No. 97-2045-A. See federal trial court opinions at 2 F.Supp.2d 783 (April 7, 1998) and 24 F.Supp.2d 552 (Nov. 23, 1998).
154. 24 F.Supp.2d 552, 565 (1998).
155. *Id.*, at 567.
156. *Id.*
157. 2000 WL 655474 (S.C.A.G.).
158. Center for the Community Interest, "Making Public Libraries Safe for Children: The Constitutionality of Restricting Access to Pornography on Library Internet Terminals" (visited February 4, 2001) <http://www.communityinterest.org/backgrounders/lib-bkdr.htm>.

Libraries In The Cyberage from page 52

The Opinion reviewed what was necessary in order to establish criminal liability under state law, stating:

[T]o establish criminal liability for a violation of Tenn. Code Ann. § 39-17-911(a)(1), the State must show that a defendant had actual knowledge of the content and character of the materials sold, lent, or exhibited. See *State v. Pendergrass*, ___ S.W.3d ___ (Tenn. Crim. App. 1999) ("knowing" means actual, not constructive, knowledge). See also *Davis-Kidd Booksellers, Inc.*, 866 S.W.2d at 528-29 (because knowledge on the part of the defendant is necessary for conviction, display statute does not impose strict liability). Merely providing Internet access to patrons will not lead to criminal liability on the part of a Public Library that is unaware that providing Internet access would be reasonably certain to exhibit or make available pornographic matters to unemancipated persons under eighteen. In other words, a library would not be criminally liable where a minor accessed pornography without the knowledge of the library. The knowledge requirement would likewise protect a library from criminal liability if a minor viewed the computer screen of an adult accessing pornography if the library was unaware of the minor's conduct.¹⁷³

The Opinion concluded:

A Public Library that provides Internet access to patrons would not violate Tenn. Code Ann. § 39-17-911(a)(1) if a minor accessed pornography or viewed the computer screen of an adult accessing pornography, *unless the library knowingly permitted the minor access to the material and did so having knowledge of the content and character of the specific material viewed by the minor*. A library's use of filtering software to avoid having minors access materials obscene as to them might provide a defense against the culpable mental state in Tenn. Code Ann. § 39-17-911(a)(1).¹⁷⁴

There is also a recent **Georgia Attorney General's Unofficial Opinion** which addresses the question of whether the state legislature may, within constitutional limitations, enact legislation which *requires* the Public Libraries of a state to distinguish between materials which are "harmful to minors" and other materials in order to prevent the exposure of such materials to children.¹⁷⁵

The Opinion states:

You have requested my opinion on whether it is within the constitutional power of the General Assembly to require, as a matter of legislation and public policy, that the public libraries of this state distinguish between adult

materials and those materials considered suitable for children so as to accommodate the legitimate concerns of Georgia parents. You have informed me that Georgia public libraries have adopted the **American Library Association's (ALA) "Library Bill of Rights."** One of the tenets of the **ALA Bill of Rights** is that "a person's right to use a library should not be denied or abridged because of origin, age, background or views." This tenet has been construed by some to mean that local or regional library boards may not make distinctions between material which is suitable for minors and that which is not. In this regard, you have asked whether the ALA's "Library Bill of Rights" has the force and effect of law in Georgia.¹⁷⁶

The Opinion continued:

As stated by the court in *American Booksellers Ass'n v. Webb*, 643 F. Supp. 1546, 1547 (N.D. Ga. 1986) quoted at 919 F.2d 1493, 1495 (11th Cir. 1990), your question "presents a conflict between one of society's most cherished rights - freedom of expression - and one of government's most profound obligations - the protection of minors."¹⁷⁷

Examining constraints imposed upon the legislature by the **Constitution**, the Opinion states:

From a constitutional law standpoint, materials can presently be divided into three different categories: (1) obscene materials; (2) harmful to minors materials; and (3) all other materials. If the legislature were to attempt to further define and segregate materials which might be offensive to some parents, but which are not obscene or "harmful to minors," a number of serious constitutional problems arise. First, formulating a definition for such materials which meets constitutional requirements is extremely problematic. For example, in *American Booksellers Ass'n v. McAuliffe*, 533 F. Supp. 50 (N.D. Ga. 1981) the court invalidated an overbreadth grounds a Georgia statute banning the distribution of, among other things, representations of "nude or partially denuded figures posed or presented in a manner to provoke or arouse lust or passion or to exploit sex." The court found the language attempted to regulate material protected under the First Amendment even as to minors and was therefore overbroad. *Id.* at 52-53. The definition of "harmful to minors" material does not suffer from this infirmity. *American Booksellers v. Webb, supra.*¹⁷⁸

Continuing, the Opinion examined a Georgia state statutory exemption accorded to Libraries:

Assuming that "harmful to minors" criteria is the benchmark, as I believe we must, the General Assembly may

continued on page 55

Libraries In The Cyberge from page 54

still legislate to require public libraries to take precautions to protect minors from exposure to these materials. In O.C.G.A. § 16-12-104 there exists a "library exception" to the criminal penalties for exhibiting harmful to minors materials to children. It is my opinion that this exception was inserted into the law to protect librarians from criminal liability where materials which might be considered harmful to minors are legitimately available for educational purposes, in an atmosphere free of commercial pressure. *Webb, supra* at 1512. The library exception was designed, in part, as a mechanism for making "harmful to minors" material available for adult consumption.

However, while the library exception exempts public and school librarians from criminal sanctions, it does not prevent them from distinguishing between adult materials and those suitable for children, and clearly does not prohibit librarians from taking steps to restrict access to "harmful to minors" material to adults only. In my opinion, legislation could be passed to require such action by libraries.

With respect to the **American Library Association's** "Library Bill of Rights," I have found nothing to indicate that it has the force or effect of law in this state. The law of Georgia consists of our **Constitution**, enactments of the General Assembly, interpretations and common law of our courts, and the rules and regulations properly promulgated by executive agencies of state government. I have found no evidence that the "Library Bill of Rights" has been adopted as a part of any of these, and therefore it is not legally binding. However, it certainly may be considered aspirational and adherence to it might even be a prerequisite to some **ALA** accreditation program for Public Library systems. In my view, the "Library Bill of Rights" can be interpreted consistently with the public's obligation to protect our children, as outlined above.¹⁷⁹

The Opinion concluded:

In summary, public libraries may be required by legislation to take appropriate action to protect minors from exposure to materials which fall within the definition of harmful to minors. The **ALA's** "Library Bill of Rights" has no legal effect in this state.¹⁸⁰

Whether the same result would be obtained in other states, is a matter of individual statutory interpretation for each state. In addition, even if such laws are held to apply, whether there are circumstances under which a Public Library would *actually* be named as defendant in a public enforcement lawsuit against

the distribution of pornography remains a question that cannot be immediately answered. The *ultimate* answer is dependent upon the law of the particular jurisdiction involved, and upon the facts and circumstances of a particular case.

The complete answer to this question involves more than mere statutory interpretation — it also depends upon the balancing of prosecutorial discretion, in light of important public policy considerations. A prosecutor, in deciding to file such a public action against a library, would have to carefully weigh its advisability, given a variety of factors, such as: (1) the limited resources of most federal and state prosecutors' offices; (2) the widespread nature of the cyberporn problem and the importance of directing prosecutorial efforts at the most culpable targets; and (3) the enormous *historical* respect and regard that the general public has had for the Public Library as a reputable institution and a resource of information and knowledge.¹⁸¹

§ 5. Do parents have a right to expect libraries to exercise modest in loco parentis restraints with respect to the Internet?

The phrase *in loco parentis* means "in the place of a parent."¹⁸² **Sir William Blackstone** is credited with first using this phrase in his commentaries on English law (circa 1770) to describe the relationship between the schoolmaster and his pupil. Under Common Law, the doctrine initially was a type of "immunity" doctrine, that permitted a school, or the school master, to "stand in the place of the parent." In fashioning regulations governing the conduct of students, the authority of the school was viewed as "co-extensive" with that of the parent. Students had no grounds to contest school decisions, as long as they were reasonable. Under this historical approach, courts deferred greatly to the discretionary decisions of schools, when made *in loco parentis*. While earlier cases used the *in loco parentis* doctrine to provide the schoolmaster with an immunity from liability, later decisions expanded the doctrine to serve as a basis for imposing a duty upon schools to supervise students. Under this approach, schools could be subjected to liability in tort for the breach of this duty.¹⁸³

The legal meaning of the phrase "*in loco parentis*" is as follows: Those acting *in loco parentis* function as surrogates for the parents, deriving their authority from the parents, as opposed to the State. The authority exercised is that of the parent, not the State, and is therefore not subject to any of the limitations imposed upon *government action* under the **Bill of Rights** (e.g., First Amendment, Fourteenth Amendment, etc.). Older case law uniformly held that when teachers and school administrators acted *in loco parentis* in their dealings with students, the authority exercised was that of the parent, and not the State. As stated before, this accorded to teachers and school administrators important immunity rights, co-extensive with those of the parent. With respect to schools, the modern Court recog-

continued on page 56

Libraries to the People Histories of Outreach

Edited by Robert S. Freeman and David M. Hovde. [200]pp., 2002, \$39.95 softcover (7x10), photographs, notes, index, ISBN 0-7864-1359-X.

Libraries, Community, and Technology

Andy Barnett. 168pp., 2002, \$35 softcover (7x10), bibliography, index, ISBN 0-7864-1379-4.

Encyclopedia of Alzheimer's Disease; With Directories of Research, Treatment and Care Facilities

Elaine A. Moore with Lisa Moore. [408]pp., 2002, \$55 illustrated case binding (7x10), photographs, bibliography, index, ISBN 0-7864-1438-3.

Encyclopedia of Abortion in the United States

Louis J. Palmer, Jr. 428pp., 2002, \$75 illustrated case binding (8½x11), 194 graphs and illustrations, bibliography, index, ISBN 0-7864-1386-7.

McFarland

Box 611 • Jefferson NC 28640
Orders 800-253-2187 • FAX 336-246-5018
www.mcfarlandpub.com

Cyberage Endnotes (continued)

159. *Id.*, at 565-566.
160. See *supra* note 38 and accompanying text.
161. See *supra* note 39 and accompanying text.
162. In May 2000, a lawyer for 12 employees of the Minneapolis Public Library filed a sex-discrimination claim against the Library with the federal Equal Opportunity Employment Commission, charging that access to Internet Sex Sites created an *indisputably hostile, offensive and palpably unlawful working environment*. News reports described one of the Librarian plaintiffs as wanting to draw the line at helping patrons indulge their sexual curiosity on the Internet, who objected to patrons who exposed her to pornographic imagery: "One guy was really into bondage. A lot of them had a thing for torture scenes." See Sara Downey, "Not on the Reading List," *NEWSWEEK*, July 8, 2000 (visited July 12, 2000) <http://www.msnbc.com/news/430449.asp>.
163. "Kids of 8 click on porn in library," *The Mirror*, February 17, 2001.
164. See *Young v. American Mini Theatres, Inc.*, 427 U.S. 50 (1976), *Renton v. Playtime Theatres, Inc.*, 475 U.S. 41 (1986), *Ward v. Rock Against Racism*, 491 U.S. 781 (1989); *City of Erie et al. v. PAP's A.M., dba Kandyland*.
165. Compare, for example, the Brief of American Library Association, et al., at 33-34, in *Reno v. ACLU*, *supra*, note 111, and accompanying text, which stressed that because of the nature of Internet searching and the volume of foreign cyberporn, children, acting without supervision and using computers with no screening or blocking, could not be effectively deterred from actively seeking and accessing sexually oriented images, and that the solution to this problem must focus on the only place where effective measures can be taken — at the recipient end. This Brief supports user-based filtering software, as constituting a matter of parental judgment, and expresses the opinion that providing children with unfiltered Internet access, in situations where only criminal prohibitions were relied upon to protect children, would be the *equivalent of allowing children to browse in adult bookstores*...
166. See Biek, *supra* note 53.
167. See Biek, *supra* note 53, at 19.
168. See *supra* note 38.
169. See *supra* note 39.
170. See February 22, 2000 legal opinion from Tennessee Attorney General regarding filter use, at 2000 WL 261662 (Tenn.A.G.).
171. *Id.*, at 1.
172. *Id.*
173. *Id.*, at 3.
174. *Id.*, at 1. The Opinion also raised and briefly examined the question of whether recent case law suggested that the use of such software may violate the First Amendment to the extent that it restricts adult access to sexually explicit, non-obscene material. At 3, the Opinion cautions: "Thus, although the use of filtering software could help a Library comply with the prohibitions of the statute, any such use of filtering software would have to be pursuant to a policy that comports with the competing rights guaranteed by the First Amendment."
175. See Unofficial Opinion No. U95-24, October 13, 1995, Honorable Clinton M. Day, 1995 Ga. Op. Atty. Gen. 189, Ga. Op. Atty. Gen. No. U95-24, 1995 WL 662648 (Ga. A.G.).

Libraries In The Cyberage from page 55

nizes that today's public school officials do not merely exercise authority voluntarily conferred on them by individual parents; rather, they act in furtherance of publicly mandated educational and disciplinary policies.¹⁸⁴ To the extent that they act on behalf of the State, school officials are subject to the restrictions embodied in the Bill of Rights.

Courts have held that those acting *in loco parentis* have an interest in protecting children — especially in a captive audience — from exposure to sexually explicit, indecent, or lewd speech. In *Bethel School Dist. No. 403 v. Fraser*¹⁸⁵ the United States Supreme Court explained:

This Court's First Amendment jurisprudence has acknowledged limitations on the otherwise absolute interest of the speaker in reaching an unlimited audience where the speech is sexually explicit and the audience may include children. In *Ginsberg v. New York*, 390 U.S. 629 (1968), this Court upheld a New York statute banning the sale of sexually oriented material to minors, even though the material in question was entitled to First Amendment protection with respect to adults. And in addressing the question whether the First Amendment places any limit on the authority of public schools to remove books from a public school library, all Members of the Court, otherwise sharply divided, acknowledged that the school board has the authority to remove books that are vulgar. *Board of Education v. Pico*, 457 U.S. 853, 871-872 (1982) (plurality opinion); *id.*, at 879-881 (**Blackmun, J.**, concurring in part and in judgment); *id.*, at 918-920 (**Rehnquist, J.**, dissenting). *These cases recognize the obvious concern on the part of parents, and school authorities acting in loco parentis, to protect children - especially in a captive audience - from exposure to sexually explicit, indecent, or lewd speech.*¹⁸⁶ (Emphasis added.)

The reason the doctrine of *in loco parentis* has not been applied to Public Libraries is that the doctrine arose by operation of law and was developed in a very specific historical context (*i.e.*, schoolmasters). However, there is no legal reason why parents, using parental judgment, could not delegate to the Public Library the power held by them to restrict their child's access to the Internet. As pointed out by the Plaintiffs in *Reno v. ACLU*, parents have the right to restrict their own child's access to the Internet through the exercise of "parental judgment," and this does not create a First Amendment issue.¹⁸⁷

There is no legal reason why parents could not request that the Library, in providing filtered Internet access to minors, act in their place as surrogates for the parent, and deriving authority from the parent. This could be

accomplished by a properly drafted "Parental Consent Form." This would have great benefit for certain parents or guardians who are unable to accompany their child to the Public Library every time their child wants to access the Internet. If parents, *as a matter of parental judgment*, have the *legal power* to restrain their child's access to the Internet using a filter of the parent's choice, they should be able to *delegate* that power. It should make no legal difference whether parents exercise that power (in person) by providing filtered access "at home," or (by delegation) "by choosing public library access" under an Internet Use Policy (implementing the Library's chosen software program) specifically approved by the parent. The *source of the power* exercised in restricting a child's access through specific filtering software remains the same in both instances: *namely*, it is the parent, or their voluntarily chosen surrogate, who is "acting."

§ 6. What role should parents play in the restriction of their children's reading materials?

Parents should play a major role in the consideration of how or whether to restrict their children's reading materials. It is probably unrealistic to expect that a parent can be present every time their child goes online. **Justice Scalia** raised this problem during the oral arguments in *Reno v. ACLU*:

Mr. Ennis, if I had to be present whenever my 16-year-old is on the Internet, I would know less about this case than I know today. [Laughter.] That is simply not a realistic possibility. To tell every parent, 'if you are worried about it, just don't let your teenager use the Internet, unless you are there'... It's not reasonable.¹⁸⁸

Parents are faced with the dilemma of how to adequately protect their child from potential danger, while at the same time helping their child to develop into an independent and mature individual, who will be able to understand and use the new technologies (such as the Internet) for his or her benefit. Parents must help educate their child, but first parents must educate themselves. They should study the issues surrounding Internet access. As a starting point, parents should visit the public service Website <http://www.getnetwise.com>, which provides information on filtering products, as well as a glossary of basic Internet terms. Parents might also visit the Website of Internet education organizations, such as <http://www.enough.org>, which contains educational materials, including a paper entitled "Just Harmless Fun? Understanding the Impact of Pornography." For information on child danger, parents can visit <http://www.missing-kids.com>. Parents wanting to understand some of the legal issues can visit <http://www.NationalLawCenter.org>, or <http://www.morality-inmedia.org>, or <http://www.frc.org>.

Nothing can ever replace the active participation of a parent in the life of their child. As one software executive testified before the

continued on page 57

EBSCO's
Electronic
Journals
Service
Enhanced
offers

More

links to content and solutions to the challenges of managing e-journals.

EBSCO's Electronic Journals Service Enhanced...

Whether you are ordering for your individual library or on behalf of a group, EBSCO can handle your electronic journal access and management needs. Our new service provides consolidated access to titles combined with the most comprehensive linking support of any e-journals system to create an end-user gateway to thousands of electronic journals. Plus a full suite of administrative tools. All from one source – EBSCO.

www.ebsco.com

EBSCO
INFORMATION SERVICES

CUSTOMER FOCUSED CONTENT DRIVEN

Libraries In The Cyberage from page 56

COPA Commission:

Whichever option a parent chooses, the importance of parental or caregiver responsibility must not be underestimated. Using a filter doesn't mean that parents shouldn't continue parenting, it simply makes their lives a little easier and offers some peace-of-mind, by serving as an electronic extension of their own values system. It is crucial that parents ALWAYS pay attention to what their kids are doing online....

It is my hope that people involved in protecting children and the integrity of the Internet will seek to find a middle ground where both goals can be met through accurate product and issue analysis, sharing of constructive ideas and a willingness to look beyond individual agendas to achieve a workable solution. The alternative is more confusion for consumers and the danger that both child safety and our constitutional rights will fall through the cracks. Like most things, client-side filters are not perfect, but they will reach their potential if they are built with constructive input from people who care. Ideally, their potential will be reached when people understand that filtering tools should never replace parenting in

the digital age, but rather assist it. With the proper combination of technology, education and policies, we will succeed in protecting children online and preserving the integrity and openness of the Internet.¹⁸⁹

In considering whether their child should have access to the Public Library Internet, parents should clearly understand whether and how their child's access will be filtered. They should take an active interest in making sure the Public Library provides their child with Internet access, using an adequate filtering system.

§ 7. What impact does filtering have on the library's ability to serve the public?

If properly implemented, filtering greatly assists the Library in its ability to serve the public. Libraries have the power and the duty to exclude anything that interferes with the Library's ability to successfully perform its main functions. Internet filtering technology can be used as a wise management tool to control data transmission and organize the flow of materials being accessed via Public Library property, consistent with Public Library selection or removal policies. This protects the limited resources of the Public Library, and ensures that the interests expressed in the Public Library's Mission Statement will be preserved and advanced.

In defense of filter use, some writers¹⁹⁰ contend that, consistent with the First Amendment, librarians may use filters to manage

patrons' use of the library's limited resources to maximize computer terminal availability for accessing the categories of content chosen by librarians to be in their collections.¹⁹¹ These authorities argue that libraries are free to block access to Websites providing material outside the scope of the library collection, including "protected speech," (for example, gambling, shipping services and non-obscene photos advertised as "XXX"). These authorities also argue that libraries may use removable filters to empower parents to diminish their children's access to so-called "adult material" (i.e., sexually oriented material that would be inappropriate for or harmful to children). In taking this position, these authorities adopt the position that libraries using filters:

- Should retain the "final say" over selection decisions;
- Should understand the criteria that the filter uses to exclude content; and
- Should allocate resources to correct any unintended blocking that may occur.

In order to adequately protect both library property and their patrons and employees, every Public Library that offers Internet access must become aware of the rapidly evolving "online" environment, and educate their patrons and employees concerning the advantages and disadvantages of Internet use. While the use of "non-technological" solutions (such as training programs and printed educational materials) as an adjunct to the use of Internet

continued on page 58

Cyberage Endnotes (continued)

176. *Id.*, at 1.

177. *Id.*, at 2.

178. *Id.*, at 3.

179. *Id.*, at 3-4.

180. *Id.*, at 4.

181. These considerations could either weigh in favor of: (1) *not* filing a legal enforcement action, particularly where there is a weak record and inferences of mere *technical violations*, making it highly unlikely that a conviction would result under the statute; or (2) *filing* a legal enforcement action in a particularly egregious case, where there is danger that the public's confidence and trust in the Library has been sufficiently betrayed, or where public safety considerations mandate that action *must* be taken.

182. See Theodore C. Stamatakis, *The Doctrine of In Loco Parentis, Tort Liability and the Student-College Relationship*, 65 *Ind.L.J.* 471, 474 (1990).

183. Robert D. Bickel & Peter F. Lake, *Reconceptualizing the University's Duty to Provide a Safe Learning Environment: A Criticism of the Doctrine of In Loco Parentis and the Restatement (Second) of Torts*, 20 *J.S. & U.L.* 261, 264 (1994). There is a nexus between the doctrine of *in loco parentis* and traditional negligence principles; namely, the expectation that the teacher exercise that degree of reasonable care that the parent of ordinary prudence would exercise under similar circumstances for the physical safety of the child.

184. See *New Jersey v. T.L.O.*, 469 U.S. 325 (1985).

185. 478 U.S. 675 (1986).

186. *Id.*, at 684.

187. *Reno v. ACLU* Oral argument, at 00:51:46. See *supra* note 107.

188. *Reno v. ACLU* Oral argument, at 1:07:08. See *supra* note 107.

189. Ross, *supra* note 90.

190. See, for example, Nadel, *supra* note 80. See, also, Center for the Community Interest, "Making Public Libraries Safe for Children: The Constitutionality of Restricting Access to Pornography on Library Internet Terminals" (visited February 4, 2001) <http://www.communityinterest.org/backgrounders/lib-bkdr.htm>.

191. In connection with this assertion, note the wording of 47 U.S.C. § 230(c)(2)(A): (2) Civil liability. No provider or user of an interactive computer service shall be held liable on account of - (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, *whether or not such material is constitutionally protected*. (Emphasis added.)

192. With respect to use of the Library Internet by children and "Internet Safety classes," see Biek, *supra* note 80, at 20: "The evidence from this study is clear: many young people are not making good choices" in their use of the Internet and it is debatable whether classes and tips offered by the library will affect this.

193. See *supra* note 46 through note 50, and accompanying text. See also *supra* note 54 through 58, and accompanying text.

Libraries In The Cyberage from page 57

filters is often helpful in educating Library patrons and staff, as well as other members of the community, and should be encouraged, "non-technological solutions" alone are *completely ineffective in protecting against the occurrence of the types of negative behavior discussed in this paper*.¹⁹²

In light of the predatory nature of preferential child sex offenders, it is not safe to provide minors or adults with unfiltered and unsupervised Internet access, particularly with respect to chat room services. Without filters, minors are "sitting targets." No amount of "Internet training" can protect children, who lack maturity and judgment by reason of their youth, from these hidden dangers. As various child exploitation cases related to unfiltered Library Internet access demonstrate,¹⁹³ online predators of children are unlikely to be deterred *without* the use of filtering software. Child exploitation crimes are *always* performed *clandestinely* by adults. Where access to the Internet is free and unmonitored, predators are virtually undetectable.

Without filters, aggressive or fraudulent "bait and switch" cyberporn marketing practices can make it impossible to avoid confrontation with sexually explicit hard-core images. No amount of "Internet training" can protect Library patrons and Library property from falling prey to surreptitious ploys, as the following examples illustrate:

(1) **Stealth Sites:** Some porn Websites (called "stealth sites") intentionally mimic the names of well-known companies or entities, in an attempt to lure the unwary (or bad typist). For example, one pornography site called itself "teen magazine," and deflected traffic away from a legitimate online magazine for teens called "www.teenmag.com." Another example is "whitehouse.com" (a porn site) and "whitehouse.gov" (the official Website for the White House in Washington, D.C.).

(2) **Hijacking of Computer Modems:** In another case, an adult Website hijacked consumers' computer modems by surreptitiously disconnecting them from their local ISP, and then reconnecting them to high-priced international telephone calls, purportedly going to Moldova (a country near the Black Sea bordering Romania) but actually terminating in Canada.¹⁹⁴

(3) **Credit Card Scams:** In another scam, consumers visited "free" adult Websites that required visitors to enter credit-card information in order to see a "free sample." Thereafter, consumers were billed between \$20 and \$90 in recurring membership fees.¹⁹⁵

(4) **Page-Jacking:** The Federal Trade Commission has brought a number of legal actions against unscrupulous porn Website operations. One FTC case involved the use of meta-tags (these summarize a Website's content in order to help search engines locate a specific site). The perpetrator copied the legitimate Web pages of others, and added a

redirect script which included the URL of a Web site selected by the perpetrator. Porn operations used meta-tags to "page-jack," or draw traffic to porn sites having no relevance to the desired original site.¹⁹⁶

(5) **Mouse-traps:** In another scam, visitors were trapped in an endless pornographic maze, through the use of a software program (called a "mousetrap"). With mouse-trapping, scripts are added to the pages containing porn ads which cause more porn ad pages to be displayed when the user clicks the browser's back or close buttons, which make it impossible to leave the pornographic sites except by turning off the computer.¹⁹⁷

Because of the nature of the problem,¹⁹⁸ there is no "non-technological" solution that is as effective as the use of Internet filtering technology in deterring or preventing wrongful use of Public Library property. Unfiltered Library Internet access has the potential for encouraging the growth of a network at the Library for the regular and continuous dissemination of sexually explicit and illegal pornography. It can attract a type of adult Library patron who can easily become entrenched in illegal online activity.¹⁹⁹

Filters are not perfect, but achieve the maximum possible in protecting Public Library patrons and employees from the foreseeable harm caused by the creation of both the primary and secondary effects associated with the unfiltered Internet access. In the Public Library context, the use of Internet filtering software:

- (1) affords *some* protection to both adults and children from direct confrontation with illegal materials or embroilment in serious cybercrime-related activity;
- (2) can reduce the likelihood of the creation of a hostile work environment, and deter patrons or staff from engaging in or being victims of sexually harassing behavior;
- (3) may assist in the better management of library resources, by controlling Internet access terminals, so that misuse of library property will not significantly inhibit access to interactive computer services by researchers or other patrons who wish to make lawful use of such services; and
- (4) can ensure that content falling under the library selection policy will be more easily accessible to patrons.

In order to achieve its goals, a Library must construct a number of rules that its patrons and employees have to follow.²⁰⁰ In the new Millennium, the Public Library and its rules must keep pace with the times. Many Public Libraries have incorporated use of new technologies as a service to the general public, and offer some form of Internet access to their patrons. A significant number of those offering Internet access employ some type of Internet filtering or blocking device.²⁰¹

The Public Library, as a provider of developing technologies, must itself responsibly

continued on page 59

The Most Requested Reference in the Field of Psychology—Now Available in Paperback!

"This edition of *Corsini* is an essential, solid, and important reference work in psychology and behavioral science."
—*Choice*

0471-24400-7
Four Volumes

"A go-to source when someone wants a no-nonsense, fast, ready reference..."
—*American Reference Books Annual*

THE CORSINI ENCYCLOPEDIA OF PSYCHOLOGY AND BEHAVIORAL SCIENCE THIRD EDITION

Edited by **W. Edward Craighead, Ph.D.**, University of Colorado, Boulder
and **Charles B. Nemeroff, M.D., Ph.D.**, Emory University, Atlanta

For over 15 years *The Corsini Encyclopedia of Psychology and Behavioral Science* has been the reference tool psychologists, teachers, and students have turned to for the most up-to-date and comprehensive information in the fields of psychology and behavioral science. Completely updated and expanded—over 60% of the material is new or revised—this latest edition is the only reference source that blends the expanding fields of psychology and behavioral science.

Entries cover everything from the most basic information to the more complex—making this edition suitable for everyone from the high school to university level.

- Over 1,200 entries
- 700+ expert contributors from around the world
- Extensive cross-referencing throughout
- Illustrations and recommended reading lists
- 4-volumes (over 2,500 pages)

WILEY

www.wiley.com

Available through your vendor

Libraries In The Cyberage from page 58

Failure of a Library to create or enforce *effective* rules against Internet related negative behavior in the library reading room hampers the ability of the library to achieve the Mission of the Library. This is a "public safety" issue, which goes to the very heart of the Library's Mission. If the Library becomes a "sexually charged" environment because of open, unfiltered Internet access, the Library will no longer be universally regarded as a "safe place" for children.

The development of the Internet has been made possible because of a series of fairly recent technological advances. Filters are part of the continually evolving technology that shapes the Internet. There are two points that must be emphasized: (1) New technology in itself is neither good nor bad — it just provides new capabilities and possibilities. It is the use that people make of technology that is either beneficial or destructive; and (2) While appearances may change, the fundamental role of the Library does not change.

This paper has discussed situations where offering unfiltered Internet access resulted in abusive and potentially dangerous situations. The risk of foreseeable harm can be reduced (although not eliminated) *only* through the use of Internet filters. Internet filters represent a wise choice, in which technology is used to control technology, preserving the Public Library as an indispensable resource tool for the advancement of education and the dissemination of knowledge within a community. Every year substantial taxpayer dollars are used to subsidize the Library, because of the public's perception that it performs a special service that is *important to the welfare of the community*. Those taxpayer dollars are spent with the expectation that the Library will exercise common sense in meeting its obligation to the community — especially in the Cyberage.

Please Note: Forums 3 and 4 in this series of forums, will appear in the next two issues *Against the Grain*. The entire proceedings will also be available online at www.charlestonco.com. — **MYH**

adapt and learn to use technological solutions to solve technological problems.

Cyberage Endnotes (continued)

194. The Federal Trade Commission obtained an *ex parte* Temporary Restraining Order within 31 day of learning about the scam. The two resulting orders bar the unlawful practices. Over 38,000 consumers had been injured, and total damage was estimated at \$2.74 million. See Address by Commissioner Orson Swindle, U.S. Federal Trade Commission, to the National Conference on State Legislatures, "Cyberspace and the FTC: Some Current Matters of Interest" (July 26, 1999) (visited September 30, 1999) <http://www.ftc.gov/speeches/swindle/indy2.htm>.

195. Betsy Schiffman, "FTC, Credit-Card Cos. Bump, Grind Web Porn," *Forbes.com* (August 25, 2000) <http://www.forbes.com/2000/08/25/mu4.html>.

196. *TECH LAW JOURNAL*, "FTC Obtains Injunction of Page Jacking and Mouse Trapping Scam" (September 24, 1999) <http://www.techlawjournal.com/internet/19990924a.htm>.

197. *Id.*

198. Given its clandestine nature, without analysis of actual Library logs, the extent of the problem may remain hidden. See Biek, *supra* note 53, at 20: "Another implication of this study is that public librarians should not believe that a lack of patron complaints, both formal and informal, about sexually explicit materials displayed on library computers or the scarcity of staff observations of the same mean that no such behavior is taking place in their libraries." Certainly, staff at the Tacoma Public Library would not have guessed that Internet users made nearly 28,000 attempts to access sexually explicit materials last year. It is likely that other libraries would find similar results to those presented here if they were to analyze logs of traffic from their public Internet computers.

199. See *Dangerous Access 2000 Edition*, *supra* note 38, and *Greenville County Library Board Report*, *supra* note 39.

200. See *Kreimer v. Bureau of Police for the Town of Morristown*, 958 F.2d 1242 (1992). (Homeless man challenged constitutionality of city Library rules regarding use of Library and behavior in it. The Third Circuit Court of Appeals held that the rules did not violate the First Amendment or due process or equal protection clauses.)

201. See *infra* notes 64 through 72.