Internet Filtering Companies with Religious Affiliations in the Context of Indiana Public Libraries[1]

Rachel Radom

University of North Carolina Wilmington

Abstract

Since the U.S. Supreme Court decided to uphold the Children's Internet Protection Act (CIPA) in 2003, public libraries accepting federal E-rate funds have been required to install technology protection measures on computers with Internet access. Many libraries use Internet filters to fulfill this requirement. Using research by Nancy Willard, which disclosed affiliations between Internet filtering companies and religious organizations, it was found that at least 15.9% of Indiana public libraries used filters with connections to conservative religious groups in 2005. Ethical implications of this research are discussed and recommendations for balancing First Amendment rights with a financial need for CIPA compliance are included.

[1] This article was originally published in *LIBRES: Library and Information Science Research Electronic Journal* and is cited as follows:

Radom, R. (2007, September). Internet filtering companies with religious affiliations in the context of Indiana public libraries. *LIBRES: Library and Information Science Research Electronic Journal*, *17*(2). Retrieved from http://libres.curtin.edu.au/libres17n2/Radom_2007_07_30_Ess%20&%20Op_final.pdf.

Internet Filtering Companies with Religious Affiliations in the Context of Indiana Public Libraries

Introduction

Since the U.S. Supreme Court's 2003 decision to uphold the Children's Internet Protection Act (CIPA), public libraries and schools receiving federal E-rate funds have been required to install technology protection measures (TPMs) on computers with Internet access. Considering limitations of time, staff, and money, many libraries choose proprietary filtering programs as their TPM instead of more time consuming measures, such as creating and maintaining their own lists of permitted or forbidden Web sites, known as whitelists or blacklists.

One of the problems with delegating TPMs to private companies is that libraries themselves have little control over what is filtered or not. Most filtering companies "protect the actual lists of blocked sites, searching and blocking key words, blocking criteria, and blocking processes as…trade secret information" (Willard, 2002, p. 2), making libraries subject to filtering companies' decisions about what is appropriate to view. Most filtering companies, whose main consumer group is parents filtering home computers, "generally perceive the risks of failing to block access to inappropriate material as more significant than the risks of blocking access to appropriate material" (Willard, p. 3).

Filtering companies provide little data about how their filters function and tend to block questionable content without consideration of First Amendment rights, actions which are perfectly legal for a private company to do; however, these factors complicate the process of choosing an appropriate filter for a public library. Even though filtering companies' protocols are not known, there are a number of methods librarians may use to evaluate filtering products.

These methods include examining particular software companies in order to learn about each corporation's decision-making processes, attitudes, and principles.

This paper will focus on examining several filtering companies in the context of CIPA-affected public libraries. Based on research from Nancy Willard of the University of Oregon, it is found that filtering products created by four companies previously known to have religious affiliations are used in a number of Indiana public libraries. A discussion is given of some of the ethical implications resulting from public institutions' use of products with such affiliations.

Literature Review

TPMs are intended to prevent library patrons from accessing Web sites with objectionable material. According to Mary Minow (2004), "CIPA requires that each participating library enforce a policy of Internet 'safety' by using, on all of its computers with Internet access, a technology protection measure (TPM) that protects against access to visual depictions in specified categories: child pornography, obscenity, and material that is 'harmful to minors' (C-O-H)." In accord with CIPA, library patrons using the Internet who are under the age of 18 should be prevented from accessing graphic materials in all three categories (C-O-H); for adults, or people over the age of 18, access should be restricted only in cases of graphic child pornography or obscenity (C-O).

Minow notes a number of interesting issues in her discussion of CIPA and libraries. First, an Internet filtering program is only one type of TPM. Libraries may use technology options other than Internet filters and still be in compliance with CIPA. Second, Minow states that "the law uses the phrase 'protects against access' *not* 'absolutely blocks access.' This recognizes that *underblocking* will inevitably occur... [emphasis original]," allowing that libraries and TPMs, including filters, cannot prevent all C-O or C-O-H images from being

accessed. Third, CIPA distinguishes between access restrictions for adults (C-O) and restrictions for minors (C-O-H). Yet, Minow notes that there are few, if any, TPMs that will shift blocking criteria based on an Internet user's age. Finally, "an often under-emphasized yet critical aspect of CIPA is that *only visual depictions* are at issue [emphasis original] (Minow)." Thus, there is neither a legal requirement nor expectation that patrons will be prohibited from accessing text, no matter the subject. Even a filter that would effectively block only C-O Web sites for adults would *still* be overblocking if it prohibited access to text on those sites.

Minow believes that libraries may face more lawsuits by overblocking Internet access than by underblocking. Part of her analysis is based on the decisions in two court cases involving filters, both of which predate CIPA's inception. The judge in *Kathleen R. v. City of Livermore* (2001) found that libraries have no constitutional duty to filter the Internet. In *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library* (1998), the judge found that filters violate the First Amendment and are therefore unconstitutional in the public library setting. These cases may influence any further litigation involving filters in libraries.

Although the constitutionality of filtering the Internet in public libraries is questionable, most libraries that accept E-rate funds use Internet filtering programs for CIPA compliance. In the state of Indiana, for example, 85% of public libraries use filters (Indiana State Library, LDO, 2006). While filters are notoriously known to overblock the Internet (Heins, Cho, & Feldman, 2006), librarians seem to accept this as inevitable. Perhaps their consent is tempered, in part, by Internet policies in many libraries that support the quick disabling of filters for adults in order to avoid overblocking for patrons over the age of 18; however, some libraries do not inform their adult patrons that filters can be disabled. Recently, the American Civil Liberties Union (ACLU) announced that several Rhode Island libraries purposely overblocked the Internet. The ACLU's

2005 report prompted many libraries to reconsider their filtering procedures in terms of the First Amendment and examine their responsibilities to clearly inform adult users of the ability to deactivate filters and to comply with CIPA at the minimum legal level (Oder, 2005).

For those under 18, however, the disabling of filters prior to online searching is not an option. While librarians are legally expected to unblock Web sites with constitutionally protected information, the young searcher must ask librarians—despite embarrassment, uncertainty, or fear—to unblock each legal but filtered Web site in order to view it. In situations where young adults must request mediation in order to view information of a private or sensitive nature, many will not ask for it (Adams, 2002). This intimidation or reluctance highlights the chilling effect that results from Internet filtering.

Despite these serious flaws, libraries choose filters as their TPM for many reasons. Filters are relatively affordable and fairly easy to use. Filters are also widely available in the market and there are many models from which to choose. Most board members, library staff, and patrons are familiar with filtering programs and understand both their purpose and their presence on library budgets. In addition, some alternatives to filters, including technologies based on the Platform for Internet Content Selection (or PICS) classification, are not at a point where they are practically viable for implementation. Furthermore, filters arguably require less staff time and effort to implement or maintain than other measures, such as blacklists or whitelists.

Many librarians appreciate filters because they have reduced the number of complaints received about pornography and limited librarians' own exposure to it (Controversial, 2001). A significant number of patrons also approve of filtering and are supportive of the practice in

libraries. On the other hand, some librarians and patrons are concerned about the ways that filters limit intellectual freedom by censoring materials, either by expurgation or prior restraint.

Regardless of personal opinions, most librarians recognize their professional responsibility to evaluate the filtering program they install on their computers. Even though filtering companies guard information about how their products function as trade secrets (Willard, p. 2), there are a number of other methods librarians may use in the evaluation process. These include testing the system on a trial basis, researching public policy reports that examine filtering performance, asking companies for as much information about their filtering practices as possible, and understanding what customization options are available in each product (Hansen, 2003; Best Practices, 2004). In addition, libraries may seek out company histories and affiliations in order to learn a little about each corporation's objectives and biases.

With this last point in mind, Nancy Willard of the University of Oregon wrote a report in 2002 on filtering companies whose products are used in public schools. Many of these products are also used in public libraries. Willard found links between several filtering companies and conservative religious organizations. Her research identifies the following kinds of associations between eight filtering companies and religious organizations:

- Some companies sell their filtering products to conservative religious Internet Service Providers (ISPs)
- Some companies have served as religious ISPs
- Some companies' executives have publicly announced that a conservative religious philosophy guides their filtering (Willard, 2002, p. 3)

These findings should give librarians reason to pause. Filtering products used by conservative religious ISPs are likely to have scrupulous filtering criteria designed in congruence

with particular religious beliefs. Since many public libraries are funded in part by the state—are in fact mandated by the federal government to filter or implement some other TPM if they accept certain federal funds—then choosing an Internet filter that financially supports and/or gives preference to one religious ideology may infringe upon the establishment of religion clause of the First Amendment (Willard, p. 7). Thus, public libraries' use of the filtering products Willard highlights is grounds for potential litigation as libraries may be in violation of the separation between church and state. Furthermore, librarians might be uncomfortable about offering patrons information that has been filtered through an extremely subjective system guided by the beliefs of a single group with, perhaps, an interest in preventing access to particular topics or perspectives.

For these reasons, public libraries may benefit from investigating filtering companies as part of their evaluation of filtering products if they have not already done so. The remainder of this paper will attempt to answer the following questions, in relation to Willard's findings: how many Indiana public libraries use filtering programs with previously identified ties to religious organizations? Which of these filtering programs are used? What is the nature of the relationships between pertinent filtering companies and religious organizations? What information is available on these companies' practices and guiding principles, and what are the implications of these findings for librarians?

Methodology

Every year, the Library Development Office (LDO) of the Indiana State Library compiles statistics based on each Indiana public library system's self-reported data. The statistics are published online and in *Statistics of Indiana Public Libraries*. The online version is updated throughout the year following each reporting period. In the 2005 report, the third supplement

question asked each library to report data related to filtering. The LDO compiled the responses in a Microsoft Excel document available on the Indiana State Library Web site (Indiana State Library, LDO, 2006).

From this document, a list was made of all filtering products used in Indiana public libraries and the number of libraries using each product. These numbers were then converted into percentages based on the following: the percent of all 239 Indiana public library systems using the particular filtering program (all libraries) and the percent of library systems that filter the Internet which use the program (filtering libraries). (A total of 204 libraries in Indiana filter the Internet, but the LDO report included eight libraries that reported filtering without identifying their filtering system. Two of these eight libraries could not be reached at the time of publication to confirm their choice of filtering program so their choice of program is unknown. The data for the percent of filtering libraries was figured by dividing the number of libraries using each system by 202 in order to account for this discrepancy.) Once the filtering programs Willard identified as having a relationship to a religious organization (hereafter referred to as "Willard's list") were highlighted on the library list, Web searches on the names of these filtering products were conducted to determine the current status of the companies and products.

It is important to note a number of limitations in this methodology. Perhaps most significant is that much of this analysis is based on research published in 2002. Some of the findings in Willard's 2002 report have since changed and, although the author of this paper has attempted to verify the accuracy of information to date when related to Indiana libraries, not all filtering companies in the 2002 report have been investigated. Furthermore, not all filtering companies with ties to religious organizations have been identified. The current research only highlights companies previously identified by Willard. There are also many features other than

religious associations, such as a filter's performance history, that a library may analyze when choosing a filter, and these are not discussed in detail in this paper.

There are also limitations in using the LDO's 2005 data set. Because the LDO's data is the result of library systems' self-reporting, there may be unintentional errors made at the time of reporting. For example, eight libraries, which stated that they do filter, failed to report the filtering system used on their computers. Errors may also have occurred when the data was entered into the LDO document.

Results

Table I lists all filtering programs used in more than one Indiana public library system. (See the Appendix for a list of programs used by only one library.) A program shaded in gray indicates that the filtering program was included on Willard's list. Summing the percentage of libraries using a filter shaded in gray, a total of 15.9% of all public libraries in the state use filtering programs that have some association with religious organizations. This number is a minimum; there may be other filtering companies with ties to religious organizations that have not been identified.

The Bess and SmartFilter programs are noted with an asterisk because, in the time since Willard's publication, another company bought Bess filtering software. Bess was developed and owned by N2H2—and N2H2 was included on Willard's list—but Secure Computing acquired N2H2 in 2003 (Secure, 2006). Secure Computing now offers two filters: SmartFilter and SmartFilter, Bess edition, which is specifically marketed to schools and libraries. According to the Secure Computing Web site, no N2H2 products could be purchased after 2005, and no support (no new software releases, no maintenance patches) for N2H2 products would be offered after September 2006. Secure Computing claims that "the key features and functionality" (Ibid.)

of N2H2's Bess are still available in the SmartFilter, Bess edition. This suggests that the categories and filtering procedures used by N2H2 have been carried over to SmartFilter, Bess edition.

Evidence of SmartFilter's plethoric filtering policy is available in the periods both before and after their acquisition of N2H2 (Heins et al., 2006). Furthermore, the OpenNet Initiative documents that "Iran…is among a small group of states with the most sophisticated state-mandated filtering systems in the world.…Iran has recently acknowledged, as our testing confirms, that it uses the commercial filtering package SmartFilter—made by the US-based company, Secure Computing—as the primary technical engine of its filtering system" (OpenNet Initiative, 2005, p. 3). Because Iran is a theocracy with a state mandate to filter the Internet, and the Iranian national ISP uses Secure Computing filtering products, Secure Computing's products (both SmartFilter and SmartFilter, Bess edition) are considered part of Willard's list. Like N2H2, Secure Computing falls under Willard's category of filtering companies that "are selling their product to conservative religious ISPs" (Willard, p. 3).

The other three filtering programs on Willard's list that are used in Indiana public libraries are CYBERSitter, S4F, and a Symantec product. As of March 2007, CYBERSitter was owned by Solid Oak Software, Inc., as cited by Willard, and S4F still offers filtering programs. The latter's Web site states "Advanced Internet Management (AIM) is a dba [doing business as] of S4F, Inc.…The company was originally established as a Filtered Internet Service Provider in 1997.… S4F, Inc. currently sells products into schools and businesses through the dba of Advanced Internet Management and into the home through the dba of FamilyConnect" (S4F, Inc., 2006). From this information, and based on Willard's findings that "SF4 appears to have started as a religious ISP, known as FamilyConnect. S4F also provides filtering to other

religious ISPs" (Willard, p. 20), it is apparent that the S4F program used in Indiana libraries is a product of the same company Willard identified. Willard also examined the Symantec filtering program I-Gear. In 2005, "Symantec had reconfigured I-Gear to be a component of larger products such as 'Symantec Web Security…'" (Heins et al., 2006, p. 26). Unlike Bess, I-Gear has not changed ownership and, since Willard found that Symantec has sold its filtering products to religious ISPs, Symantec filtering programs are also considered part of Willard's list.

Discussion

At the time of Willard's publication, N2H2 provided filtering services to several religious ISPs and had a church affiliate program, which allowed churches to use N2H2 filtering for free. Secure Computing advertises no such program on their Web site; however, Heins et al. (p. 72) cite a 2006 *New York Times* article, which discussed the popular Web site/blog *Boing Boing* being blacklisted by SmartFilter for "nudity." The single page that sparked a block of the entire site discussed two books on the photographic history of adult magazines and contained two thumbnail images that might be considered pornographic. As a result of the *Boing Boing* block, the Web site's five authors/editors received e-mails from regular readers indicating that the national ISP providers in not only Iran but also Qatar, Saudi Arabia, Tunisia, and the United Arab Emirates also use SmartFilter (Doctorow et al., 2006). This further supports the OpenNet Initiative's 2005 findings cited above.

In her 2002 research, Willard reported that:

- Symantec provided filtering services to religious ISPs
- Soft Oak Software/CYBERSitter's president stated that they attempt to enforce a moral code when filtering ("We're not politically conservative, we're morally conservative," as

cited in Willard from the *Los Angeles Times*). CYBERSitter was also sold by Focus on the Family, a conservative religious organization

- S4F may have started as a religious ISP and, at least prior to 2003, provided filtering services to other religious ISPs
- All three of these filter programs have filtering categories that can be selected to exclude Web sites on the "occult/New Age," sex/sexuality, homosexuality, and/or "illegal/radical activities"

The categories listed in this last point represent very broad and complex ideas, yet decisions to refuse access are based on these overgeneralized and nebulous labels. Each of the products offered by these companies has its own standard list of sites blocked within each filtering category. Libraries submit to these blocks merely by enabling the filtering program on their computers since they must choose at least one of these standard categories for the filter to function in compliance with CIPA.

The fact that any number of public libraries use the same products supported and used by religious organizations to filter and block information poses ethical problems for the librarians involved. One such ethical concern is that libraries using filtering programs on Willard's list are promoting a particular religious ideology in a public institution. The decision to deny or allow access to information on the Internet is based on an author's adherence to particular precepts. This conflicts with professional codes espoused in the American Library Association's Library Bill of Rights, which states, "Materials should not be proscribed or removed because of partisan or doctrinal disapproval."

A related issue is the degree to which libraries, with a professional code that advances intellectual freedom, continue to rely on commercial businesses with no such code to decide the

suitability of information in a library. Librarians essentially give up their roles as selectors—a key part of collection development—to agents with purposes and codes very different from their own, who seek reasons to reject (censor) the material rather than reasons to keep (select) it (Asheim, 1953). The result is the exclusion of materials based on content alone. In this case, wittingly or not, at least 15.9% of Indiana libraries are condoning religious censorship.

Children and young adults, often impressionable and hopefully encouraged to seek a variety of perspectives in order to understand the world, are arguably the group most affected by filters. Filters, which attempt to protect children from "harmful" information, also harm their intellectual development. For example, how can information literacy be taught when critical perspectives are blocked? Furthermore, how can a library with a mission to provide equitable access to balanced information meet this purpose when an Internet filter—especially a filter associated with religious tenets—censors Web sites? This is particularly worrisome considering the popularity of Web sites as sources of information for young adults. According to a 2005 report by the Pew Internet & American Life Project, 87% of Americans between the ages of 12 and 17 use the Internet and 51% of teens connect daily (Lenhart, Madden, & Hitlin, 2005).

Librarians have been forced to walk this tightrope between CIPA compliance and First Amendment rights since the Supreme Court's decision in 2003 and CIPA presents a much larger ethical quandary of which these religious connections are just one facet. Nonetheless, reconsideration of current and future filtering choices is continually needed as new research is made available and new technologies are developed. One example of a relevant new technology is the development of the OpenChoice Internet filter by researchers at the University of Texas at Austin. The filter is "an open source platform with a non-proprietary and transparent list of blocked sites" and allows for human review of the blacklist (Efron, Smith, & Roy, 2005). A

similar project is Kanguard, used in Kansas public libraries. Notably, however, both programs continue to block access to entire Web sites, not just images on those sites.

Conclusion

Censorship is defined as "the suppression of ideas and information that certain persons—individuals, group, or government officials—find objectionable or dangerous" (ALA, "Intellectual," 2006). When librarians use filtering software in their libraries, especially software identified by Willard as having religious ties, librarians find themselves in the position of accomplices in the act of censorship.

Part of the difficulty of this situation arises from the following facts: TPMs are mandatory in libraries that accept E-rate funds. Libraries that accept E-rate funds often cannot afford to refuse such funds. The CIPA requirement for a TPM is an unfunded mandate and filters are a widely used and affordable TPM. The issue is further complicated by the fact that many states and local governments that fund public libraries are passing their own CIPA-like laws, which are often more restrictive than and very different from the federal CIPA (Liebler, 2004).

Librarians who agree with the American Library Association's stand against all forms of censorship, but who must also accept E-rate funds in order to remain open, have been in a difficult position for four years. Besides following the minimum legal requirements of CIPA and keeping access available to as much information as possible, creativity, communication, and action may help ease some the discomfort in this seemingly long-term professional imbroglio. While libraries are not filtering companies' largest consumer group, they are a substantial market. Librarians may consider advocating for a filtering program distinguishable from filters used in homes, schools, and private companies. Such a product would surpass OpenChoice or

Kangaurd (admirable programs though they are) by restricting access to images alone (the .jpg, .mpg, and other file formats of images) while permitting users to view text. This would support the "freedom to read" endorsed by the ALA (ALA, "Freedom," 2006). The product would also allow different levels of access depending on the patron's age (C-O versus C-O-H).

This advocacy might put librarians even further into murky territory by supporting the development of a program that violates the professional code of conduct via censorship. Such an act could be construed as supporting a "good" filtering program; for librarians, there is, practically speaking, no "good" Internet filtering program. (Would an image-blocking filter block images based on a ratio of image to text on a Web site? If so, what percentage would be acceptable? What about allowing for regional variances in the definition of "obscene?" And what is "harmful to minors?") At the same time, since many libraries must install a filtering program in order to keep their doors open, there is clearly a need for a filtering program that supports minimum CIPA compliance, if not for ethical reasons then certainly for legal protection.

In addition, librarians may choose to give parents the option of permitting their children to disable filters. As previously stated, because many libraries recognize the inherent tendency of filters to overblock, Internet use policies often allow adults to readily disable filters. Minow, among other First Amendment advocates and several of the Supreme Court Justices involved in the CIPA decision, strongly promotes this ease of disabling for adults. In the same vein, parents should be allowed to permit their children to disable filters at the library and librarians should honor such parental decisions. Furthermore, librarians should commit to publicizing their readiness to disable filters for adults and unblock non C-O-H Web sites for children and young adults while emphasizing their respect for patron privacy. Outreach and discussions about

privacy are especially needed with regard to young adults who may be particularly wary of approaching librarians for access to information.

Naturally, there is still a need for librarians, parents, and others to educate children about the responsible use of media and information. Filters will underblock Web sites simply because more sites are always being added to the Web. Filters provide a false sense of security to people concerned about pornography and obscenity, and family and society must still help children learn how to handle various subjects and situations. This responsibility is related to the development of a media/information literate society, the support of which is increasingly seen as an imperative of librarians. Similarly, librarians should speak with members of their communities about intellectual freedom and the reasons librarians do not agree with filtering on a professional level. This is as important as educating patrons about the limitations of library databases.

Librarians should continue to be vigilant in considering the impacts of Internet filtering and censorship in general. Is PICS, or any labeling of the Internet based on content, a good idea? How might legislation such as the Deletion of Online Predators Act (DOPA), which seeks to limit access to social networking sites, be viewed in terms of censorship? And, what aren't filters filtering? Should librarians be concerned about advertisements and the commercial collection of personal information, actions and information that filters aren't censoring and may even be encouraging (Frechette, 2005)? Better communication between researchers and practitioners on all of these topics would benefit the profession as a whole.

Finally, more transparency about filtering companies and their practices is needed. In spite of trade secrecy, when information about filtering companies' practices, policies, and principles is disclosed or discovered, it should be shared readily within the library community. Many organizations, such as Peacefire and the Free Expression Policy Project at NYU's Brennan

Center for Justice, have investigated the types of Web sites blocked by particular filtering products; however, more can be done to review the filtering companies themselves in order to gain a greater understanding of the products they offer. In the words of Karen Schneider, filters are "mechanical tools wrapped around subjective judgment" (Schneider, 1997, p. xiv). It is a matter of much importance that librarians know whose subjective judgments they are relying on.

Update: On February 26, 2007, ContentWatch purchased the filtering program Net Nanny (see http://www.contentwatch.com/). ContentWatch's Web site reveals clear affiliations with a religious ideology. See, for example, their page at http://www.netnanny.com/learn_center/ safe_sites_family, which links to http://www.child-internet-safety.com/. This Web site features a quote from Tommera Press, which is prominently featured on Tom Buford's site www.firesofdarkness.com. See also ContentWatch's article archive on pornography (http://www.netnanny.com/learn_center/article_list/ cat/pornography) with articles written by Mark Kastleman and Janet LaRue. This change of ownership increases the number of filtering products with religious affiliations used by public libraries and indicates the need for watchfulness and further research.

References

Adams, H. R. (2002). Privacy and confidentiality: Now, more than ever, youngsters need to keep their library use under wraps. *American Libraries, 33*(10), 44-46, 48.

ALA (American Library Association). (2006). ALA | Freedom to read statement. Retrieved June 16, 2006, from http://www.ala.org/ala/oif/statementspols/ftrstatement/freedomreadstatement.htm

ALA (American Library Association). (2006). ALA | Intellectual freedom and censorship Q&A. Retrieved June 16, 2006, from http://www.ala.org/ala/oif/basics/intellectual.htm

ALA (American Library Association). (2006). ALA | Library bill of rights. Retrieved June 16, 2006, from http://www.ala.org/ala/oif/statementspols/statementsif/librarybillrights.htm

American Civil Liberties Union. (2005). *Reader's block: Internet censorship in Rhode Island public libraries*. Retrieved January 30, 2007, from http://www.riaclu.org/friendly/documents/2005libraryinternetreport.pdf

Asheim, L. E. (1953). Not censorship but selection. *Wilson Library Bulletin, 28*, 63-67.

Best Practices (2004). *Library Technology Reports, 40*(2), 49-61.

Controversial ruling in Minneapolis filter case: EEOC supports contention by library staff that exposure to Internet porn constitutes a hostile work environment. (2001). *Newsletter on Intellectual Freedom, 50*(5), 187-196.

Doctorow, C., Frauenfelder, M., Jardin, X., Pescovitz, D., & Battelle, J. (2006). *Boing Boing: Boing Boing banned in UAE, Qatar, elsewhere. Our response to Net-censors: Get bent!* Retrieved June 16, 2006, from http://www.boingboing.net/2006/02/27/

boingboing_banned_in.html

Efron, M., Smith, A. A., & Roy, L. (2005). OpenChoice: An Internet filter for public libraries. *Texas Library Journal, 81*(3), 4-6.

Frechette, J. (2005). Cyber-democracy or cyber-hegemony? Exploring the political and economic structures of the Internet as an alternative source of information. *Library Trends, 53*(4), 555-575.

Hansen, D. (2003). *CIPA: Which filtering software to use?* Retrieved July 19, 2006, from http://webjunction.org/do/DisplayContent?id=992

Heins, M., Cho, C., & Feldman, A. (2006). *Internet filters: A public policy report*. Retrieved June 16, 2006, from The Free Expression Policy Project, Brennan Center for Justice at NYU School of Law Web site: http://www.fepproject.org/policyreports/filters2intro.html

Kathleen R. v. City of Livermore, 87 Cal.App.4th 684, 104 Cal.Rptr.2d 772 (Cal. Ct. App. 2001).

Leibler, R. (2004). Beware the mini-CIPAs. *American Libraries, 35*(7), 39.

Lenhart, A., Madden, M. & Hitlin, P. (2005). *Teens and technology: Youth are leading the transition to a fully wired and mobile nation*. Retrieved July 24, 2006, from Pew Internet & American Life Project Web site: http://www.pewinternet.org/PPF/r/162/report_display.asp

Mainstream Loudoun v. Board of Trustees of Loudoun County Library, 24 F.Supp.2d 552, 27 Media L. Rep. 1065 (D. Va. 1998).

Minow, M. (2004). Lawfully surfing the Net: Disabling public library Internet filters to avoid more lawsuits in the United States. *First Monday, 9*(4). Retrieved June 13, 2006,

from http://www.firstmonday.org/issues/issue9_4/minow/

Oder, N. (2005). Rhode Island PLs fix filtering. *Library Journal*, *130*(18), 19.

OpenNet Initiative. (2005). *Country study: Internet filtering in Iran 2004-2005*. Retrieved March 7, 2007, from OpenNet Initiative Web site: http://www.opennetinitiative.net/studies/iran/ONI_Country_Study_Iran.pdf

S4F, Inc. (2006). *aimconnect.com: A note from the CEO.* Retrieved March 7, 2007, from http://www.aimconnect.com/about.html

Schneider, K. G. (1997). A practical guide to Internet filters. New York: Neal Schuman Publishers.

Secure Computing Corporation. (2006). *Secure Computing: N2H2 product information*. Retrieved June 16, 2006 from http://www.securecomputing.com/index.cfm?skey=1453

Statistics of Indiana public libraries 2005. (2006). Retrieved June 10, 2006, from the Indiana State Library, Library Development Office Web site: http://www.statelib.lib.in.us/www/ISL/ldo/statsmenu05.html

Willard, N. (2002). *Filtering software: The religious connection*. Retrieved June 13, 2006, from the Center for Safe and Responsible Internet Use Web site: http://csriu.org/onlinedocs/documents/religious2.html

Appendix 1

Filter Programs Used in Only One Indiana Public Library*

Blackford
Blacklist
Cobian
Cornerstone Solutions
CSInet
Family Safe
Filter Gate
Firebox 700
Firewall filter
Fortress
Gale Filter
Gatefilter
Gates
Grisoft-AVG
Lightspeed
Microsoft
MSN
Netscape 7.1
PC-cillin Internet Security 2006
Sentry
Software 602
Spam and Spyware
Surf Center
Web Marshal
Webxence

* Please note that the names of these programs were self-reported by employees at each library system. No attempt has been made to clarify the system names or identify these programs.

Author Note

Many thanks to Dr. Howard Rosenbaum and Dr. Noriko Hara at the School of Library and Information Science, Indiana University, Bloomington, for providing inspiration, suggestions, and advice.

Table 1

Filter Programs Used in More Than One Indiana Public Library

FILTER PROGRAM	NO. OF LIBRARIES	% OF ALL LIBRARIES	% OF FILTERING LIBRARIES
Websense	43	18.0	21.3
WebBalance	27	11.3	13.4
CYBERSitter	17	7.1	8.4
CyberPatrol	16	6.7	7.9
SonicWALL	12	5.0	5.9
Symantec	10	4.2	5.0
SurfControl	9	3.8	4.5
Bess*	7	3.0	3.5
Puresight for Wingate	7	3.0	3.5
We-Blocker	7	3.0	3.5
squidGuard	6	2.5	3.0
Net Nanny	5	2.1	2.5
DansGuardian	4	1.7	2.0
ComSifter	3	1.3	1.5
WatchGuard	3	1.3	1.5
Bluecoat	2	0.8	1.0
Content Advisor	2	0.8	1.0
iPrism (St. Bernard)	2	0.8	1.0

Norton	2	0.8	1.0
S4F/Family Connect/EduGuard	2	0.8	1.0
SmartFilter*	2	0.8	1.0