The Southeastern Librarian

Volume 64 | Issue 4 Article 3

2-3-2017

Censorship: Filtering Content on the Web

Lizabeth Elaine Stem
Vance-Granville Community College, steme@vgcc.edu

Censorship: Filtering Content on the Web

Lizabeth Elaine Stem

Lizabeth Elaine Stem is the Director of Library Services at Vance-Granville Community College in Henderson, NC. She can be reached at steme@vgcc.edu. This paper is based on the Southeastern Librarian Association's New Voices Program winning presentation.

Introduction

The World Wide Web has become a vehicle of free expression for millions of people around the world. It also represents a type of international library with no geographical or physical boundaries, bringing a vast array of information into private homes, schools and businesses. Because the Web allows anyone to post anything at any time, many believe some sort of censorship should be imposed.

Censorship of the Web comes in the form of software which filters Web sites, blocking those which publish content deemed unsuitable by those administering the filtering software. Most content filtering software is used on computers in public schools, businesses, and libraries. The goal is to block sites that have no legitimate use in the workplace or in the classroom. These include sites promoting pornography, drugs, gambling, hacking, violence, and spyware among others (Sarrel, 2007).

How Web Content Filters Work

Filtering software may be placed on servers or on individual computers. These technologies fall into three general types -- list based URL filtering, text filtering, and content recognition technology (Chapin, 1999).

URL filtering is the most commonly used technology to filter content. In URL filtering, a database of unacceptable Websites and domain names are identified based on the type of content on the sites. Categories include illegal activity, hate speech, obscenity, sex, drugs, violence, and so forth. "List-based filtering has two weaknesses. First, it is costly. The lists must be updated frequently, and users must pay ongoing subscription fees. Second, and more importantly, vendors' ability to maintain their lists are being outstripped by current Web growth. Some analysts estimate that a new Web site is added an average of every 18 seconds. List-based technology cannot possibly keep up" (Chapin, 1999, p.46).

Filtering technologies also use text filtering to block pages with seemingly inappropriate content. For example, sites containing words such as "sex" or "breasts" would be blocked. "Unfortunately, simple text filters have trouble distinguishing appropriate uses of the same word from inappropriate uses. Thus, filtering solutions relying on text filters often block pages that students and teachers need or want to access" (Chapin, 1999, p.46).

Content recognition technology uses "trained neural networks to identify patterns on incoming Web pages and to permit or block the page. For example, when content recognition tools encounter the word 'breast' these tools will check the context and structure for words such as 'mammogram.' Students will be allowed to see the medical information, while a pornographic site will be blocked. By dynamically evaluating Web content in real time, content recognition technology is always current and avoids the costs and limitations of list based filtering" (Chapin, 1999, p.46).

According to the 2012 national longitudinal survey by the American Association of School Librarians (AASL), of the 4,039 responses received from school librarians, 70 percent of the librarians indicated that their schools used URL-based filtering, making it the most common type of Website filtering used in schools. Keyword-based filtering was second with 60 percent. Blocking the entire domain, not just a specific URL within the domain, was used 47 percent of the time, according to the survey (AASL, 2012).

Most librarians resist these attempts at filtering, arguing that the criteria used by filtering software are subjective. Software developers use their own judgments to decide what is acceptable, rather than allowing parents, teachers, and librarians to judge. Also, filtering software often cannot discern site content. Blocking a site with child pornography is expected, but using the same filtering logic, also blocks those sites teaching sex education, for instance. "Sites such as Middlesex.gov and SuperBowlxx.com were blocked simply due to their domain names. Commercial site-censoring filters have blocked NOW, EFF, Mother Jones, HotWired, Planned Parenthood, and many others" (Neumann & Weinstein, 1999, p. 152).

Other examples of some of the most commonly used Web content filtering software and information that has been incorrectly blocked by that software are below.

- Cyber Patrol blocked MIT's League for Programming Freedom, part of the City of Hiroshima Web site, Georgia O'Keeffe and Vincent Van Gogh sites, and the monogamy-advocating Society for the Promotion of Unconditional Relationships.

- CYBERsitter blocked virtually all gay and lesbian sites and, after detecting the phrase "least 21," blocked a news item on the Amnesty International Web site (the offending sentence read, "Reports of shootings in Irian Jaya bring to at least 21 the number of people in Indonesia and East Timor killed or wounded").
- Net Nanny, SurfWatch, Cybersitter, and BESS, among other products, blocked House Majority Leader Richard "Dick" Armey's official Web site upon detecting the word "dick."
- SmartFilter blocked the Declaration of Independence, Shakespeare's complete plays, Moby Dick, and Marijuana: Facts for Teens, a brochure published by the National Institute on Drug Abuse (a division of the National Institutes of Health) (Heins & Cho, 2001, p. 2).

Arguments Against Web Content Filtering

Opponents argue that filtering software is simply not effective at protecting users from unwanted content. Filtering software often creates a false sense for users that they are completely protected when, in reality, "the use of filtering and blocking software was associated with a modest reduction (40 percent) in unwanted exposure, suggesting that it may help but is far from foolproof" (Mitchell, Finkelhor & Wolak, 2003, p. 330).

Another concern voiced among opponents is that filtering software simply can't keep up with the creation of new Web sites. Karen Schneider of The Internet Filter Assessment Project (TIFAP) estimates that there are approximately 22,000 pornographic sites among the millions of Web pages on the Internet. Each day an additional 85 sites are added. "Even the most aggressive of filters cannot keep up identifying them all in a timely manner. One well-known filter, in an unguarded moment, admitted to allowing 51 percent of pornography sites through" (Willems, 1998, p.56).

Opponents of Web content filtering point to the fact that filtering software can be disabled by users. There are also numerous ways to bypass or workaround content filters. Some sites, such as Peacefire.org, are dedicated to helping users bypass filters. Another means of bypassing filters is through the use of proxy servers, such as Psiphon and StupidCensorship. Because of this, some site filtering software chooses to block all proxy-avoidance sites, URL translators, and other workaround sites. Many groups, such as political activists, dissidents, and others seeking to hide their identities or locations, use proxy-avoidance sites to mask their information from government factions and others seeking to harm them. This raises a completely new intellectual freedom concern beyond protecting minors from sexually explicit materials (Houghton, 2010).

Cell phone and mobile devices are another way to bypass content filtering software. Increasingly, students are using more mobile devices to access the Web. Personal devices such as cell phones and tablets often have the ability to connect to the Web via data plans and are thus able to bypass filtering software (Johnson 2012).

Mankato State University professor, Fran McDonald argues that schools and other agencies who adopt Web filtering software may be placing their organizations at greater legal risk by doing so. "By assuring parents and the community that students won't be exposed to 'harmful' materials, the responsibility for Internet use shifts from the student user to the school administration and staff. It also sets up a not-too-difficult challenge for the determined hacker" (Johnson, 1998, p.13).

Content filters also pose challenges to a library's core beliefs of personal privacy and privacy of information. Filtering software records vast collections of data about users' computer usage habits and Web searches. These collections are maintained by software developers and technicians within the content filtering organizations, not by librarians (Houghton, 2010).

Another detriment to content filtering is the cost. Filtering can be extremely expensive, especially for financially challenged schools and libraries. Setup fees can run about $50 per computer. Then there is often a monthly or annual update charge. There is also the cost for manpower to update each computer on an ongoing basis. If the filters are placed on the servers, instead of on individual computers, all computers on the network would automatically be blocked. This means that content blocked for minors would also be blocked from teachers, administrators, and older students. In general, the greater the cost of the filter, the more customization is allowed within the service. Freeware versions of these programs will have preset filtering levels which cannot be changed. "The temptation for financially challenged schools and libraries to use the least expensive filter, especially if mandated to do so, will be great" (Johnson, 1998, p. 12).

There have been several laws and court cases that affect the use of Internet filters in libraries with regard to federal funding. The most notable one, The Children's Internet Protection Act (CIPA), was passed by Congress in 1999. CIPA requires that schools and libraries receiving government funds for discounted Internet access, also known as the E-rate program, must "certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are obscene, child pornography, or harmful to minors" (Starr, 2003, p.1). Library funding tied to federal grants requires that libraries pay for expensive Web content filtering. Sometimes the cost of the content filtering service will outweigh the actual monetary benefit received by the library. By implementing filters, "the San José Public Library had $35,000 to gain in E-rate funding. Estimated start-up costs for the filtering software technology, staff training, hardware, and software totaled $400,000 per year with ongoing annual costs of $275,000-$300,000." In this case, filtering for the purposes of E-rate funding would mean a financial loss for the library (Houghton, 2010, p.31).

Arguments Made in Favor of Web Content Filtering

Network administrators -- and others responsible for content filtering on computers used in public schools, business, and libraries -- point to liability issues for the organizations if they do not provide some level of protection for minors and for employees. "Some companies are drawn to Web-filtering solutions by a lack of perceived control" especially in the wake of regulations such as Title IX and Sex Discrimination, Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Sarbanes-Oxley, which are meant respectively to protect against discrimination based on sex in education programs, customer privacy, and oversee financial dealings. In lieu of filtering "other companies with tons of bandwidth and productive employees have decided to block the truly offensive content and monitor the rest, keeping an audit trail and reacting only when egregious misuse occurs" (Lipschutz, 2004, p. 102).

The rapid growth of the Internet has made pornography sites easily accessible. Even though a US Department of Justice study found pornography Websites account for just 1.1 percent of the total content on the Web, these sites attract a high portion of Web traffic. This in turn has made companies very concerned about the level of freedom employees have to surf the Internet. With a rising number of Human Relations violation law suits being filed over sexual or lewd conduct in the workplace some Chief Information Officers feel a real need to monitor employees' Web traffic (Ilett, 2006).

One advantage of using filtering software is that it also looks for viruses embedded in pictures and other data, as well as malware (Ilett, 2006). The Internet is "a repository of malware, where companies can fall prey to infections, fraud, and data theft. Many people just don't realize how dangerous a place the Internet can be. And if they're using your network, you may even have a legal responsibility to protect them" (Sarrel, 2007, p. 80).

Another key point that is often brought up by proponents of Internet filtering in libraries is the idea of selection versus censorship. "Some courts contend that installing filters is equal to library selection of materials, or collection development decisions, and that each individual library has the right to make those selection decisions and they do not violate First Amendment rights as a result" (Houghton, 2010, p. 28) Along the same lines, proponents argue that teachers already take responsibility for selecting and "filtering" the information content of a student's education. "By teaching them arithmetic before we teach them calculus we filter their exposure to mathematical information" (Chapin, 1999, 44).

Filtering proponents also argue that while 61 percent of Americans are not in favor of government regulation of Web content, "a survey also indicated that 80 percent of the public answered 'yes' to the question: 'Do you think the government should take steps to control access to pornographic or sexually explicit material on the Internet to protect children and teens under 18 years of age?'" (Johnson, 1998, p. 11).

As a final point, proponents to Web content filtering point to the great deal of customization current Web filtering operations now offer. "Schools can enable or disable broad categories of blocked sites. They can also override filters by adding sites to white lists of allowed sites or black lists of blocked sites. Schools can legally turn off filtering on specific computers or provide a filter bypass login for specific users" (Johnson, 2012, p. 86).

Views of the ALA and Alternatives to Filtering

The American Library Association (ALA) has stated that limiting anyone's access, including children, is not acceptable. The ALA Library Bill of Rights states very clearly that a person's right to use information within the library should not be denied based on that person's views, origin, background, or age. The ALA and many librarians believe that Web content filters are in direct conflict with the mission of libraries to provide open access to all information for all age groups (ALA, 1996). The American Library Association states that "when libraries restrict access based on content ratings developed and applied by a filtering vendor, sometimes with no knowledge of how these ratings are applied or what sites have been restricted, they are delegating their public responsibility to a private agency" (Houghton, 2010, p. 29). Most librarians believe that children and citizens are better protected if "librarians, parents and thoughtful individuals everywhere in our communities work together to find ways to educate, prepare, and support community members as digital citizens" (Houghton, 2010, p. 31).

Children and adults need to learn the critical viewing and information skills needed to help them make good decisions about the material they encounter on the Web. As concluded by the National Research Council:

> Swimming pools pose some threat to the safety and well-being of children. But swimming pools provide benefits to their owners—and children—in many different ways. Technology—in the form of fences around pools, pool alarms, and locks—can help protect children from drowning in swimming pools. However, teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning (Kranich, 2004, p.18).

Privacy screens on public computers would provide a level of Internet privacy to library patrons. Also, placing computers in more isolated areas would also allow patrons to view Web pages with a level of privacy. Some libraries create profiles that are age-based, allowing users who are under 18, or under 12, to login only on certain computers. Placing children's computers in an isolated area can help to protect the data that children are entering on the computer as fewer adults are likely to be wandering that area (Houghton, 2010).

The "toggle switch" is another approach to filtering. In this method, a customizable filter is installed on a portion of the Internet public access computers. For those computers serving the adult section of the library, the filtering software would be turned off with clear notice that the "Internet can be filtered for those who may be sensitive to pornography; the filter has a 5-10 percent chance of allowing material that it purports to filter, and it filters legitimate information." For the children's section, filters would always be turned on with a notice posted that the filters could be turned off for children whose parents had given them permission to have unfiltered access to the Internet (Willems, 1998, p. 56).

A final suggestion is that libraries "have clear Internet usage policies that provide unfiltered access to online information. A clear policy provides some protection from outside interference and indicates that the library has given due consideration to the Internet access issue" (Willems, 1998, p. 58).

Conclusion

Proponents of Web content filtering believe that Web filters protect children and safe guard employees and businesses. Opponents believe Web filtering blocks valuable information, while doing a poor job of blocking illegal activity, hate speech, obscenity, sex, drugs, violence, and so forth. Web blocking technologies have not matched the public's expectations on how they should work. The data reveal that both sides have valid concerns, and until a foolproof method can be found to block the most egregious, illegal content on the Web such as child pornography, only a combination of strategies overseen by conscientious individuals may be the best course of action.

Bibliography

American Association of School Librarians (2012). *School Libraries Count!* Retrieved from http://www.ala.org/aasl/sites/ala.org.aasl/files/content/researchandstatistics/slcsurvey/2012/AASL_Filtering_Exec_Summary.pdf

American Library Association (1996). *Library Bill Of Rights.* Retrieved from http://www.ala.org/advocacy/intfreedom/librarybill

Chapin, R. (1999). Content management filtering and the world wide web. T.H.E. Journal, 27 (2), 44-50.

Heins, M. & Cho, C. (2001). Internet filters: a public policy report. *National Coalition Against Censorship.* Retrieved from http://www.fepproject.org/policyreports/filters2.pdf

Houghton-Jan, S. (2010). Internet filtering. *Library Technology Reports,* 46(8), 25-33,45.

Ilett, D. (2006). Porn at work: limits on freedom to surf. *FT.com. Financial Times Limited.*

Johnson, D. (1998). Internet filters: censorship by any other name? *Emergency Librarian,* 25(5), 11-13.

Johnson, D. (2012). Power up! *Educational Leadership,* 70(4), 86.

Kranich, N. (2004). Why filters won't protect children or adults. *Library Administr4ation & Management,* 18(1), 14-18.

Libshutz, R. P. (2004). Don't go there: seven tools that help businesses stop their employees from visiting inappropriate sites. *PC Magazine*, 23, 102.

Mitchell, K., Finkelhor, D. & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the Internet: a national survey of risk, impact, and prevention. *Youth and Society,* 34(3), 330-358.

Neumann, P. & Weinstein, L. (1999). Risk of content filtering. *Communications of the ACM,* 42(11), 152. Doi:10.1145/319382.319403

Sarrel, M. D. (2007). Web content filtering: filtering isn't just about inappropriate web sites. *PC Magazine,* 26, 1-80.

Starr, L. (2003). Filtering software: The educators speak out. *Education World Online*, 1.

Willems, H. (1998). Filtering the net in libraries: the case (mostly) against. *Computers in Libraries,* 18(3), 55-58.