Filter Assignment

Ryan Kawaguchi

San Jose State University

1. Type of Library: Public Library

2. Patron Access

No, filtering software will not be used on any computer available for public/patron use, or the computer network as a whole, to prevent users from accessing content. As director of the Seatown Public Library, I will maintain an acceptable use policy holding to respect for the First Amendment rights of users over any other consideration.

Although there is internet information which some of our patrons may consider inaccurate, offensive, or even dangerous (especially, but not limited to, children), using filters to "protect" patrons from any form of information, and limiting them to information which the Library (acting as an agency of government, by extension) and/or the filter creator deems "acceptable," inherently limits the freedom of choice for all patrons of Seatown Public Library.

While some patrons consider certain forms of information and content available on the internet "dangerous," a greater danger to patrons (and also to the computer network of Seatown Public Library) involve the risk of introducing viruses, trojans, spam, and other malware. A malware-infected computer limits our ability to provide computer and internet service to patrons by preventing them from using computer(s) rendered inoperable (or difficult to use) by infection with malware. There is the possibility that malware may also retrieve personally-identifiable information, including personally-identifiable information about minors to third-party individuals with malevolent intentions. This could expose minors to the possibility of identity theft, "internet predators," and publication of personally-identifiable information on the internet. The computers will use anti-virus software to filter out malware, but they will never filter content on the basis of possible "offensiveness."

Aside from the stated prohibition on downloading malware, time restrictions, and prohibitions on downloading copyrighted material are the only other restrictions in force on library patrons using the internet and other computer resources of Seatown Public Library.

Additionally, there are alternatives to filtering software, consistent with respecting user privacy. These alternative(s) include, but are not limited to, privacy screens which prevent other users from observing another patron's internet and computer activities and the placement of library computer terminals away from children's areas.

The greatest alternative to filtering (at least as far as "protecting children" is concerned) are parents themselves, who maintain parental rights and responsibilities for the wellness and proper guidance of their child(ren). Therefore, it shall be noted in the acceptable use policy of Seatown Public Library that parents are responsible for the content their child(ren) access while online, and parents should discuss with their child(ren) their expectations about responsible internet use.

3. Employee Access

No, I will not filter internet access of employees of Seatown Public Library. There are various concerns about "cyberloafing", some of which were described by Gain (2009), who argued that employees using the internet for personal reasons decrease their productivity and pose threats to the integrity of the organizational computer system, and to the organization itself, such as "dowload[ing] viruses, transmit[ting] sensitive company information, or us[ing] enterprise property to break the law" (p. 26).

However, there are ethical, as well as practical, considerations to make when considering the use of internet monitoring and filtering software for employees, such as the fact that many of the issues and threats related to employee internet use for non-organizational (i.e., personal reasons) are, in fact, “exaggerated.” Much of the monitoring and filtering done to further an organizational objective of employee productivity is often not “tailored to meet the specific objective or balanced with employee privacy concerns.” Gain also argued that with longer hours being spent working, “[i]t should be acceptable to allow for reasonable personal and private use of computers” (Gain, 2009, p. 26).

Another ethical issue with employee internet monitoring was raised by an International Labor Organization report cited by Grodzinsky, Gumbus, & Lilley (2010) which argued that “[internet monitoring] jeopardizes employees health and welfare . . . [can cause] [i]ncreased stress and adverse working conditions . . . fear of job loss . . . and reduced social support can result from monitoring.” The ILO report also argued that “[e]xcessive monitoring can be counterproductive and result in low morale and depression that affect productivity” (p. 434).

Aside from ethical issues arguing against employee internet filtering and monitoring, internet filtering would not be practical for many of the basic functions of this library, collection development and reference department being two specific examples.

Many of the professional librarians need to use the internet simply to garner and look at reviews on items they are considering adding to the collection, and if they were being monitored or their access to material reviews with controversial topics were being filtered, then this would limit their ability to understand what kinds of materials were available on various subjects. Their inability to locate relevant material would in turn limit library service to patrons. In summary, filtering of materials would create an unacceptable conflict between the collection development policy and the internet acceptable use policy.

The reference librarian, in particular, needs the internet to help patrons locate information, and if they were prevented from observing, for example, a web page discussing prostate cancer, which the filter cited as containing sexual material, how would they explain this to a patron needing the information on how to deal with the issue, since their doctor did not provide the patron with this information at a previous clinical visit.

The practical problems created for library employees by internet filtering outweigh ethical issues raised by a pro-filtering stance, and concerns about personal use affecting the productivity of library staff should be set aside for this reason.

4. I'm not filtering patron internet access, and my message to people who want to authorize filters includes the following . . .

First, our patrons should understand how filtering software works, since "[p]roducts that filter based on domains and IP addresses typically use a search engine . . . to run canned searches for trigger words or phrases . . . [the] results list is then run through an algorithm which creates a blacklist of blocked pages for that topic or subject matter. Other algorithms block entire domain or IP addresses" (p. 26). Blacklist filtering software is based on the compilation of a "pre-determined list of URLs for 'inappropriate' websites . . . created by the company make their blocking decisions, and access to these URLs is blocked entirely." The "composition of (and rationale behind the lists of blocked urls," known as black lists, "is maintained as a trade secret," and not based on the selection criteria or internet acceptable use policies which our library has developed (Kolderup, 2013, p. 26). In contrast, white lists, according to PC Magazine (2014), a white list is "[a] list of websites that are allowed to be accessed" (n.p.). And as Houghton-Jan (2010) pointed out, "what is on the software's core blacklists and whitelists is up to machines and filtering software company staff who are untrained on freedom of information, constitutional issues, or best practices for information objectivity" (p. 29). For instance, filter blacklists have been known to limit or block access to websites discussing Wicca and Native American spiritualities. In other cases, LGBT issues websites have been known to fall within internet blacklists, while internet white lists have allowed access to “ex-gay ministries” and organizations “advocat[ing] against gay rights” (Caldwell-Stone, 2013, p. 58). In another example, the Censorware Project found in a 1999 study that the “Declaration of Independence, the Bible, and the complete works of Shakespeare were all blocked by SmartFilter, which was being used in the Utah public school system” (Kolderup, 2013, p. 26).

Second, although community members who support our library purchasing filtering software have argued that filtering software can be disabled upon request (from an adult patron), there is often a waiting period for the filter to be disabled, which can take from an hour to several days for staff to process, and the patron must personally make a formal request for disabling of the filter. Although the text of the United States Constitution does not guarantee an explicit right to privacy, the Supreme Court has dealt with certain cases and has “granted citizens some rights to privacy.” The need for patrons to make a formal written request and the concomitant waiting period can create a barrier to patrons wishing to access our library’s resources (Kolderup, 2013, p. 27).

Third, as Houghton-Jan (2010) pointed out, filtering software blocks material the filter creator, rather than the library, deems “offensive,” regardless of the software creator providing the option to block only certain types of content, “[a]ll filters overblock (incorrectly blocking something objectionable) and underblock (incorrectly allowing something objectionable).” The studies which Houghton-Jan cited found that 78% of the time, filters blocked material that “it was supposed to,” but that the material it blocked was exclusively text, while images were not included in this criteria. Houghton-Jan looked at other filtering software studies from 2007 to

2008 and found that for images, the filter did not prevent 54% of images considered objectionable by the researchers (p. 27).

Fourth, internet filtering can be circumvented. In fact, as Spacey, Muir, and Creaser (2013) argued, library users can use web proxies and information available on the internet on bypass internet filters (p. 485). There is the possibility that a technically-savvy minor could circumvent internet filtering software. Additionally, as director of Seatown Public Library, I have concerns that internet filtering software may be used by the software creators to track patrons and then disclose this information to online advertisers, compromising the privacy of users (Spacey, Muir, and Creaser, 2013, p. 486).

Fifth, the issue of access to computer and internet resources, regardless of economic status, was considered as well in making the decision to not filter internet resources. While many young people have home internet access, other young people lack home internet connections due to poverty. There are almost 60 million Americans who lack a smartphone or broadband subscription ("over-filtering harms education," 2014, p. 109). Farrelly (2011) argued that because some user's basic online access at home is limited for reasons of poverty (as some users may not be able to afford an internet subscription at home), these patrons (especially younger people) may come to view filtered internet access at the library "as limited . . . by the restrictions placed on them [by filtering, and] are less likely to see the library as a valuable part of their lives (p. 29).

The Seatown Public Library has alternative measures which will negate the perceived need for filtering. These ideas, recommended by Caldwell-Stone (2013) include the arrangement of computer terminals to face away from areas which children are expected to be present. In other libraries, such as our library, children's areas (and areas where children and their parents are expected to congregate) are not located near public access computer terminals. Additionally, privacy screens prevent patrons from viewing other computer screens. The Library believes that through communicating the ideals of the library system and educating library patrons on protecting their online identity, search strategies, and how to prevent children from accessing materials which parents may consider “dangerous,” the need for internet filtering is lessened or eliminated (p. 59).

5. Seattle Public Library (2012) created an internet use policy which “upholds the rights of all library users to read, seek information and speak freely as guaranteed by the First Amendment” (n.p.). While the library recognizes that certain information “sources may be offensive, disturbing, and/or illegal,” privacy is paramount to the policy, as “[a]ll users are asked to respect the privacy of other users and not attempt to censor or comment upon what others are viewing.” This emphasis on privacy is further protected by “intentional placement of computers and provision of privacy screens” (Seattle Public Library, 2012, n.p.).

With regard to children, the Library “affirms the right of parents and legal guardians to determine and monitor their own children’s use of Library materials and resources.” This is implemented by providing links to “age appropriate Internet sites and to filtered search engines” and the provision of computers with “commercial filtering software for public use in the children’s area at each location in The Seattle Public Library system.” However, the policy also cautions that “[p]arents should inform their children of materials they do not want them to use and may wish to supervise their children’s Internet sessions” (Seattle Public Library, 2012, n.p.).

Reference List

Caldwell-Stone, D. (2013). Filtering and the First Amendment. *American Libraries, 44*(3/4), 58-61.

Farrelly, M. G. (2011). Digital (Generation) Divide. *Public Libraries, 50*(2), 28-29.

Gain, B. (2009). Playing IT big brother: When is employee monitoring warranted? *The Canadian Manager, 34*(1), 26-27. Retrieved from http://search.proquest.com.libaccess.sjlibrary.org/docview/1371368480?accountid=10361

Grodzinsky, F. S., Gumbus, A., & Lilley, S. (2010). Ethical implications of internet monitoring: A comparative study. *Information Systems Frontiers, 12*(4), 433-441. doi:http://dx.doi.org/10.1007/s10796-009-9205-9

Houghton-Jan, S. (2010). Chapter 4: Internet Filtering. *Library Technology Reports, 46*(8), 25-33.

Kolderup, G. (2013). The first amendment and internet filtering in public libraries. *Indiana Libraries, 32*(1), 26-29.

over-filtering harms education, new ALA report finds. (2014). *Newsletter on Intellectual Freedom, 63*(4), 109-135.

Seattle Public Library. (2012, June 27). Public use of the internet policy. Retrieved October 30, 2014, from http://www.spl.org/about-the-library/library-use-policies/public-use-of-the-internet-policy

Spacey, R., Cooke, L., Muir, A. , & Creaser, C. (2013). Regulating use of the internet in public libraries: A review. *Journal of Documentation, 70*(3), 478-497.

PC Magazine. (2014). Definition of: whitelist. Retrieved November 7, 2014, from http://www.pcmag.com/encyclopedia/term/54441/whitelist