2016-2017 ALA CD #19.9
2017 ALA Midwinter Meeting

Report from Intellectual Freedom Committee January 2017

Guidelines to Minimize the Negative Effects of Internet Content Filters on Intellectual Freedom

Introduction

For a variety of reasons, many public libraries and schools install content filters on the Internet access they provide to their patrons and students. A library may decide to filter in response to community standards or to comply with state filtering legislation in order to receive funding. A governing authority such as a school district or local government may also require a library under its jurisdiction to filter. Libraries that receive federal E-rate funds for Internet access or in-building network enhancements must also comply with the filtering and other requirements of the Children's Internet Protection Act (CIPA).

Whatever the reasons, many libraries must deal with the well-documented negative effects of content filters on intellectual freedom. Filters often block adults and minors from access to a wide range of vital information and forms of expression that are constitutionally protected speech. CIPA requires only a narrow category of speech to be blocked: visual images that are obscene, child pornography, or visual images that are deemed "harmful to minors" under the law. Filtering technology is not sophisticated enough to make such narrow distinctions, and as a result both over filtering and under filtering occurs in the attempt to block images that meet these criteria.

Filters also threaten the privacy of users by monitoring and logging Internet activity. As more websites move to HTTPS to secure communications from eavesdropping, this presents a challenge for filters that employ content inspection techniques. Some filters now include the ability to decrypt HTTPS protocols and can thereby monitor and log user activities on secure websites. Implementation of these capabilities is not required under legislation like CIPA, nor is it consistent with the mission and values of libraries.

These guidelines are issued to provide public and school libraries with information about how to select, configure, manage, and assess content filters to minimize the negative effects on free inquiry and the privacy of library users.

Selection

Library staff, who have an ethical obligation to protect intellectual freedom, and information technology (IT) staff, who typically must install and support the product, should work collaboratively to select filtering software.

The filter selection team should consider standard criteria for purchasing any technology product or service including features, performance, ease of administration, vendor support, cost, user privacy, etc. To minimize the negative effects on intellectual freedom, the following additional criteria should be considered when selecting a filter:

Ability to select narrow and specific categories of content to be blocked.
The technologies and procedures used by the vendor to categorize content.
Ability to permanently unblock content that is incorrectly blocked.

Ability to notify users that content is being blocked and their options, if any, for accessing the content.
Options to easily disable the filter upon request by library staff or directly by the users.
Ability to run reports or analytics on what is being blocked and how frequently it is blocked.

Configuration

Deciding what categories of content to filter is a law and policy decision that should be made by library and school administration and ultimately approved by their respective boards. Filter settings should not be selected solely by IT staff who likely do not have a background in the importance of intellectual freedom in libraries.

Filters often come pre-configured with many categories and types of content blocked by default. These settings should be carefully reviewed by library staff, school administrators, and educators. Only the minimal number of categories (e.g. only illegal categories of sexually explicit images, if the concern is CIPA compliance) should be blocked. Ideally a technology team (consisting of library staff, IT staff, administrators, educators, etc.) will test filter configurations by running sample searches before implementation to ensure that the chosen settings over-block and under-block as little as possible.

Avoid blocking content based on viewpoint or because the topic is controversial. Avoid blocking entire types of content (e.g. videos or social media) or protocols (i.e. music streaming). Some libraries may restrict these services not because of the nature of their content but because of the bandwidth they consume. However, bandwidth concerns can be managed without blocking protected speech by using other technologies and techniques that focus on the amount of network activity, rather than the type of content.

Limitations in filtering technology cause over filtering, a situation that occurs when content is blocked because it is incorrectly categorized. Schools and libraries should establish procedures that allow adults and minors to request content which is incorrectly categorized to be unblocked in a timely manner. Schools and libraries should also establish procedures to notify users about what is being filtered and what their options are to access incorrectly blocked content.

Many filters provide the ability to decrypt secure (HTTPS) transactions using a so-called “man-in-the-middle” method. This allows the filter to scan the content of web pages and URLs that would normally be secure. Without decryption, a filter can only block an entire HTTPS domain (e.g., ala.org), and it is unable to block individual web pages or sections of a website. The effects of decryption on the privacy of patrons can be profound if they use the library for web activities that require secure communications. For example, the security of usernames, passwords, and sensitive personal information, including commercial, educational, financial, legal, and medical information may be compromised. Because of this, decryption should not be enabled on library computers.

By default, most filters and routers generate logs of user activity data. Library staff have an ethical and often a legal obligation to protect the privacy of this information and thus access to these logs should be restricted to authorized staff. The library should configure the device to log the minimum amount of data and develop procedures to regularly delete the logfiles.

Report from Intellectual Freedom Committee   January 2017

Management

The ability to easily disable filters is crucial to mitigating their negative effects on free inquiry. The Supreme Court affirmed in its decision to uphold CIPA that adults and minors 17 or older have the right to have content unblocked or the filter disabled for research or any lawful purpose. Public and school libraries need to establish a set of procedures that allow the disabling of filters for adults and minors 17 and older quickly and easily with as little staff intervention as possible. Libraries of all types should be prepared to unblock incorrectly categorized or incorrectly blocked websites for users of all ages.

Here are some possible disabling scenarios to accommodate libraries of different sizes and technical capabilities.

A library could make some computers available with a browser extension that allows the user to disable the filter by enabling a web proxy. The library would need to have procedures in place to make sure only adults and minors 17 and older used the computers with the proxy extension.

A library could provide staff with the ability to disable the filter at the request of an adult. If the filter does not support disabling by staff on-the-fly, the computers could be configured with a second account with unfiltered access that requires staff login. The disadvantage of this scenario is that making users ask library staff for unfiltered access presents a barrier that may have a chilling effect on such requests.

A library with computer sign in software that includes user authentication could allow adults and minors 17 and older to choose their own filtering level, e.g. none, minimal or strict. If the sign in software does not support the ability of adult users to select their filtering level when logging in, the browser could be configured with an extension that allows the user to quickly and easily disable the filter by using a web proxy.

A library or school could set up procedures to allow users to request that specific web pages or websites become unblocked by library staff either temporarily for a specific activity (e.g. student assignment) or permanently. The procedures to permanently unblock a resource should include a request form that allows the user to explain why the resource should be unblocked, a review process by library staff or educators, and a way to notify the requester about the outcome of the review.

In addition if CIPA compliance is the concern, filters only have to be applied to devices provided by the library for use in the library or school. User-owned devices connecting to a library's wireless or wired network do not need to be filtered. Laptops and other devices checked out for use outside the library or school do not need to be filtered.

Assessment

All types of libraries should establish procedures to continually assess the impact of the filter on library users. The assessment should include:

Tests by library staff on common research topics to determine extent of over filtering and under filtering.
Regular reports on what is being blocked, recategorizations, disabling requests, etc.

Report from Intellectual Freedom Committee   January 2017

Survey of library and classroom users on the effect of the filter on their Internet activities.

The results of the assessment should be used to make continual improvements to the filter (i.e. to reduce the negative impacts on free inquiry and privacy). These improvements may involve changes to the filtering software's configuration, changes to library and school procedures, or the selection of different filtering software.

Additional Resources

Bandwidth Management (TechSoup for Libraries)

Children's Internet Protection Act (CIPA) Guidance for Libraries (Universal Service Administrative Company, July 2016)

Fencing Out Knowledge: Impacts of the Children's Internet Protection Act 10 Years Later (American Library Association, Office of Information Technology Policy OITP & Office for Intellectual Freedom Policy Brief No. 5, June 2014)

Filtering and the First Amendment (American Libraries, April 2013)

How to: Circumvent Online Censorship (Surveillance Self-Defense, Electronic Frontier Foundation)

Internet Filtering: An Interpretation of the Library Bill of Rights (American Library Association)

Issue Brief: The Time has Come to Move to HTTPS! (Center for Democracy & Technology, October 2016)

Libraries and the Internet Toolkit: Legal Issues: CIPA and Filtering (American Library Association)

SSL Filtering Whitepaper (Smoothwall)

The Man in the Middle: E-rate, Filtering and CyberSecurity (Knowledge Quest Blog Post by James LaRue: Journal of the American Association of School Librarians, September 28th 2016)