Plain Facts About Internet Filtering Software

Introduction

Filters (also known as content filters or blocking software) are software programs that block the transmission of data over the Internet. Internet content filters are one of a number of tools in the spectrum of resources available to librarians for managing Internet content. For over 100 years, public libraries have gradually become more open to the public, through additions to our services such as children's rooms, popular reading collections, open stacks, and outreach programs. In the last decade, the world has also come to us through the burgeoning Internet. The Internet, especially the Web, has changed library services in many positive ways, but it has also introduced new challenges. Internet filtering —now used by one in five public libraries, according to a study performed in 2000 by the University of Illinois—is one tool librarians consider when exploring how to improve Internet management.

All public librarians can benefit from understanding the concepts and challenges associated with Internet filtering, but you will find this information particularly helpful if:

- You receive federal or E-Rate funds for Internet Service Provider (ISP) costs directly or through any grant or regrant program—since recent legislation requires compliance with the Children's Internet Protection Act (CIPA) in order for your library to continue receiving these funds. See the section below, "Understanding CIPA."
- Your state or local government is considering or has passed legislation requiring filtering for some or all of the computers in your library that have open access to the Internet
- Library users, trustees, staff, media or other stakeholders have expressed concern about filtering (or the lack of it)
- You plan to use Internet filters in your library for any reason
- You are evaluating the wider range of tools available for managing Internet access, such as privacy screens, privacy desks, or proxy servers for configuring special-use machines

What Are Filters And How Do They Work?

Filters employ two primary methods for blocking data: word blocking and site blocking.

Regardless of the methods used for blocking Internet content, no filter is perfect. All filters under-block and over-block (see especially Ayre, 2001 and Schneider, 1997). The far-reaching claims of some filtering products may lead to a false sense of security among members of your community, who may believe that filters never block information they are interested in or that children will never see "surprising" Internet sites. Additionally, filters are useless in preventing adults from preying on children. Ensure that your Internet management practices include advising parents that filters can never substitute for parental involvement, and advising all members of your community that filters may block information they want to see.

Word Blocking

Word blocking (also known as keyword blocking) matches web pages against a list of keywords. If the web pages match the keywords, the web pages are blocked. Word blocking is the easiest form of filtering to implement, because it relies on software, rather than human review. Word blocking is also the most inaccurate form of filtering. When people talk about web pages blocked because they include the phrases "XXX" or "chicken breast," they are referring to keyword blocking. Many libraries that use filters disable keyword blocking because of its tendency to indiscriminately overblock. Some filtering companies make their keyword stoplists available on their websites, but most do not.

Site blocking

Site blocking matches web pages on the Internet against a list of predetermined sites. When the user attempts to access the site on the stop list, the filter's stoplist prevents this action, sometimes by displaying a web page, or "denial page," that announces that the site in question is blocked. The default denial page can range from an obscure error code (such as, "Cyber Patrol Code 2") to a list of the site or sites blocked with a link to email the library staff. In some cases, library technical support staff can customize this denial page to include alternate text or to point back to another webpage; be sure to watch for this feature when evaluating filters.

Most site-blocking stoplists are created in part or entirely by human review; employees of the filtering companies select sites to be included on the stoplist. (The article by Peter Lewis included in this bibliography is a revealing look inside the site selection process.) Because creating these proprietary databases is expensive, to protect the company's investment, most filtering stoplists are hidden; you (or anyone else) can't see any of the sites included in the filter's database. In four

years of evaluating filters, I have identified only one product that allowed a viewable stoplist—and it was such a short list that the product was essentially useless. In practice, the only way you will know if a filter blocks a website inappropriately is if someone reports it after the fact, or you constantly review all web activity. (Some filtering companies provide search engines for determining if a website is blocked, but this presents the same problem; you aren't going to enter all 116 million websites into the filter company's search engine.)

How often a company updates its stoplist, and how frequently your staff updates the filter's local database, impact the reliability of the filter. Filtering software, like anti-virus software, must be continually updated. Note that most filter companies charge maintenance fees for updated filtering lists as well as technical support.

What is your recourse when a site is inappropriately blocked (or not blocked)? In most cases, if you are aware of the problem, you can add or delete sites to a local stoplist, which addresses the needs of your own site, but actual changes to the filter itself to correct database errors must be forwarded to the company, which may take days, weeks or months to review the request. Of course, a site list created by one company is not going to be able to adapt itself to every community, let alone every person viewing a website. What we discovered in a filtering study conducted in 1997 is that over time, controversial websites disappear and reappear in filters —possibly due to requests to remove and then reinstate the sites. This underscores the highly subjective nature of filters; in the end, filters represent the opinions of the people who select their content content and the many different interpretations of what is, and is not, judged to be obscene, objectionable, or simply offensive.

Filtering Categories

Most filtering stoplists are broken into categories which can be selected for blocking or for open access. These categories are arbitrary; there is no "MARC" standard (or any other industry standard) for filtering categories. While most filters include categories related to sexual activity and nudity, the wide range of filtering categories reflect the target markets: filters produced for business environments may include categories for "vehicles," "travel," or other websites employers may not want employees using during business hours. Filters produced for the school market may include categories for "violence" or "hate sites." (Very few filters are produced primarily for the library market, which also means that the needs of library customers take a back seat in designing filters.)

Vendors usually provide the criteria for filter categories on their websites. However, these categories, and the websites assigned to them, are highly subjective, so when evaluating and configuring library filters, be careful about assumptions, such as "anything we would provide would automatically make it through a filter." A filter I tested recently blocked one of our in-house databases, Valueline, because the filter placed it in a category of financial resources inappropriate for use during "business hours." Additionally, due to human error,

websites can end up in any category—and due to the hidden nature of filters, this will not be obvious to you unless you see the site blocked, or someone who attempts to access a blocked site reports it. Organizations such as the Quakers, the Mormons, the American Association of University Women have been blocked by filters. Filtering sites that are not related to sexual content raise far more concerns about First Amendment rights.

Software, Server, or Remote Proxy?

Some Internet filters are client software, intended to be installed and managed on individual computers. Others are server-based software, which means they are centrally installed and managed. Finally, some filters are provided through remote servers, often called remote proxy servers and less frequently, but more accurately, ASPs (Application Service Providers).

Evaluations of Internet filtering software have identified characteristics common to client, server, and remote proxy servers. Client filters can interfere with other computer software, is the least reliable with respect to under- and over-blocking; however, in small libraries, or where you only plan to filter a few workstations, client filters are typically the least expensive alternative. Server-based filters require central installation and management, do not require software to be installed on individual computers, is more reliable than client software, is cost-effective in large numbers, and usually provides the most features and configuration options. Remote proxy filters provide some of the advantages of server-based filters, particularly centralized management, and can be cost-effective for libraries that do not maintain their own servers and do not want to maintain software on each computer, but in most cases provide few if any options for local configuration and control, such as the ability to configure the denial page or override a blocked site. Both server-based and remote proxy filters usually offer the ability to configure filtering per-machine or per-user; for example, if your library has a Microsoft NT network, the "staff" group could have one level of access and the "public" group could have another, or you could determine that a specific machine would be filtered or not filtered regardless of who logged in to it.

Finally, several vendors offer the capability to provide barcode or smart-card management. (Smart cards have computerized chips embedded in them that contain patron data; smart cards also require special readers on each computer.) Automated authentication is very good news, as managing who has access to filtered or unfiltered Internet computers can be a daunting and unpleasant task for front-line library employees, who may feel that their job title has changed from "reference librarian" to "police officer." Barcode management is the least expensive, since most libraries currently use barcode technology and configuring computers with barcode readers are not essential (patrons can type the numbers). Barcode readers are under $100, if you would like to make the Internet logon experience more comfortable for patrons.

Smart-card technology, while promising, is still expensive to implement; the one working configuration I am familiar with (Englewood Public Library, Colorado) requires a second, high-priced "smart card" exclusively for Internet access. Nevertheless, typed or "swiped" barcodes or smart-card technology offer the opportunity to do away with clumsy sign-in sheets, and give you the opportunity to place computers anywhere in the library.

Be Vendor-Savvy

Be wary of promises that a filter blocks "obscenity" or "illegal content," and also be cautious if a sales representative pressures you to use a particular product in order to comply with local, state or federal laws. While the recent CIPA legislation will require libraries to block transmission of content "harmful to minors," in practice, there is no way to guarantee that this has been accomplished, and all filters have demonstrated that they will let through content they are supposedly designed to block.

Only a court of law can determine if content is obscene, and filtering companies do not have police or lawyers on staff to determine whether content is "illegal." (Furthermore, reassurances that a filter complies with "the law" because it blocks "porn" should be ignored, as pornography is not illegal.) However, it is a legitimate sales pitch to say that a filter blocks (or attempts to block) websites depicting—for example—a content-neutral category such as "full nudity."

Some companies have begun pressuring libraries to purchase filtering software in order to be compliant with the Children's Internet Protection Act (CIPA). Libraries that receive federal funding, such as E-Rate and LSTA grants, will need to certify by late October, 2001, that they plan to implement "technology protection measures" by Funding Year 5 (July 1, 2002), or filtering, for all publicly-accessible Internet computers—staff as well as public, according to the FCC guidelines (there are also no exceptions for consortium staff). However, as of this writing, there is no legal requirement at the federal level to install or use a filter if you are not receiving E-Rate or LSTA funding for telecommunications costs. Some state have passed filtering legislation that impacts libraries. If CIPA is upheld, it will only apply to libraries receiving federal funding for the purposes outlined in the law.

What happens if a library (or library consortium) chooses not to comply? If the FCC audits the library and determines that the library certified it was in compliance but was not in fact compliant, the library could fail to receive (or be directed to return) its federal funding.

Inevitably, software companies have attempted to improve library filters. Some filters claim to incorporate artificial intelligence features. Vendors may toss around terms such as "dynamic document review" or "intelligent content recognition." These terms boil down to simple keyword analysis, sometimes with a small

mathematical algorithm tossed in for good measure—which, as librarians understand, is an extremely crude method of organizing or filtering information. While vendors claim that their products have become extremely sophisticated, the reality, demonstrated by all evaluations of filtering software performed outside the filtering industry, is that filters are still mechanical tools wrapped around subjective judgment, and no bell or whistle can change that.

Often, so-called "advanced" tools rely on unproven technologies—such as filters that claim to be able to distinguish human flesh from other images—or on embellishments to keyword blocking that sound sophisticated but are no great improvement. One "advanced" filter blocked a site with cat poetry because the word "pussy cat" appeared too often on the webpage. Use common sense in evaluating vendor claims; if it sounds like an amazing new discovery, it probably isn't.

How Much Do Filters Block?

Librarians should evaluate filter features (discussed in the next section), and should use a working environment to examine products carefully before purchase. However, evaluating filters by testing them against a few dozen websites or keywords—while useful for evaluating filters against one another--can be very misleading with respect to conclusions about filters in general. As of this writing, there are over 116 million web sites—with several new hosts added every second. If a filter blocks 1 out of a thousand websites, simple math tells us that the filter could, potentially, block hundreds of thousands of websites. A claim of 99% accuracy—not made by any filter known to this author—would still result in blocking 1.6 million websites. Any given host may provide millions of individual web pages, with many more added every day. Clearly, even a modest rate of error has the potential to block vast amounts of valuable—and Constitutionally-protected—information.

Conclusions about the impact of blocking "only" a number of websites should take into account how filters work. Your own library provides the best analogy. Websites removed by filters are not placed on book trucks for your inspection before final "weeding." Instead, imagine that every night a special weeding team crept in and removed a few books from your library's shelves, and the books' records were silently expunged from your catalog. Unless your library was extremely small, it would take a while to even realize that books were missing—and identifying what was gone would be extremely difficult. Nevertheless, the impact on your collection would be very real, particularly in areas of the collection that have controversial materials. That is how filters work—by silently removing all evidence that the sites in question ever existed, and relying on a very large data set (the Internet) to obscure the absence of this content.

Filters and Privacy

Many filters have the capability to gather information about Internet use. Depending on the filter, this information can be highly detailed, including time, date, machine, and sites accessed. Some products allow administrators to view actual Internet use per-machine in real time. Products that display and report user information can, of course, gather and store highly-sensitive data. Data gathered by filters can be very helpful for interpreting use patterns, filter effectiveness, and even network response time. However, ensure that you can configure a filter so it does not gather or store information that your policies and laws prevent you from gathering or storing.

Additionally, several proxy-based filters offer or plan to offer the capability to store information off-site. One product includes an "after hours" feature where websites or entire categories that are locally blocked can be deferred to an off-site server so the user can access the information later. [This feature raises legal and ethical questions about ownership of off-site data. State confidentiality laws or local policies may prevent you from signing contracts that delegate control of patron data to commercial third-parties.

Finally, remote proxy servers by definition store all data off-site, since the filtering servers are located at the parent company. In 2000, the Wall Street Journal revealed plans for N2H2, publishers of the widely-used Bess remote proxy server, to sell children's Internet-use data to the Department of Defense. After widespread publicity, N2H2 backed off, but this illustrates the importance of a contract that protects your patrons' Internet data.

CIPA and Filtering

At least this year, no discussion of filtering is complete without outlining compliance guidelines for CIPA. CIPA was passed as a rider to an appropriations bill in December, 2000. The ALA website for CIPA, www.ala.org/cipa , includes the full text of the bill, legal interpretations of CIPA by the legal counsel for the American Library Association (ALA), and current status of legal activity. Both ALA and the American Civil Liberties Union are challenging CIPA in court. (The case is scheduled to go to trial in February 2002.)

Key points:

- Applies to libraries, library consortia, and schools that receive federal funding, including E-Rate, LSTA and other federal sources
- Affects Internet Service Provider (ISP) costs, not the discounts received for data lines (phone service, dedicated Internet lines) or internal connections (hardware).
- Can be selectively implemented in consortia, provided that the system only request discounts for the libraries that certify compliance with CIPA
- Does not require consortia or state libraries to police compliance
- IMLS guidance for LSTA is still forthcoming—watch carefully for grant

guidelines

- Filtering is not required in E-Rate Funding Year 4 (July 1, 2001 through June 30, 2002)
- To receive discounts on ISP costs in Funding Year 5 (July 1, 2002 through June 30, 2003), a library must certify it is in compliance with CIPA. For E-Rate funding year 5, compliance means you have…
    - Implemented "technology protection measure" (interpreted to mean a filter) for all computers that have access to the open Internet, staff as well as public, adults as well as children (no exceptions for administrators, system staff, and so forth).
    - Developed an Internet policy on use of the Internet by adult and child users
    - Held public meetings about the library's Internet services and policies, including filtering

The resources at the end of this Technote can help you with the specifics of these compliance areas. However, it's important to note that the guidelines for CIPA vary according to the E-Rate funding year. For Year 4 (beginning July 1, 2001 through June 30, 2002, a library only has to be "undertaking action"—not actually filtering--to be in compliance with CIPA.

Be sure to thoroughly read the documents cited at the end of this Technote, particularly the resources from the FCC, ALA, and the Schools and Libraries Division. Guidance for CIPA is still evolving.

ALA's Position On Filtering

The position of the American Library Association on filtering is probably as misunderstood as filtering software itself.
In 1997, the Council of the American Library Association, a body elected by ALA members, voted overwhelmingly to approve a resolution that states in part, "RESOLVED, That the American Library Association affirms that the use of filtering software by libraries to block access to constitutionally protected speech violates the Library Bill of Rights."
In this statement, the American Library Association reminds libraries that Internet practices should be congruent with the principles of intellectual freedom. Filters are designed to block data; that is their purpose. The inherent characteristics of filters —which rely on hidden, anonymous third-party decision-making--make it inevitable that filters block some Constitutionally-protected speech. Therefore, any use of filters in libraries should be designed to ensure that patrons may have access for any lawful purpose to an entirely unfiltered Internet, without prior restraint. This emphasis on the patron's right to choose is consistent with our profession's commitment to intellectual freedom, and is consistent with many library practices. Libraries rarely limit what can be read in a library. Librarians do not search patrons' book-bags for titles the library would not purchase, or police reading

tables to see if patrons are reading materials consistent with local collection-development policies. In a similar vein, many libraries offer open access to the Internet, so that the patron may choose what to read. Librarians believe in supporting a wide variety of information needs.

In many libraries, standard practice and policy is to defer filtering decisions for children to their parents (and only the children's parents). Unlike teachers in many schools, public librarians do not act in loco parentis (in place of the family).

Key Questions For Planning Internet Management Strategies

Internet filters are just one of many tools available for managing Internet content, and integrating them into your service scheme is important. Before selecting a filter and determining how it will be configured, first ask:

- What is it you are trying to accomplish? (Prevent people from accidentally viewing sexually-explicit content? Provide a choice of filtered or unfiltered access? Provide adults with mechanisms for determining whether their children will have open or unfiltered Internet access? Compliance with legal mandates, such as CIPA or state or local laws?)
- What intellectual-freedom principles do you want to support? (A choice of unfiltered access for adults? Patron privacy? Open access for all, regardless of age?)
- What information should be provided to the patron about the filter? Should the patron be made aware that the search is filtered? Should he or she see the URLs for blocked sites? Should they have recourse to contacting library or company staff?
- Which tools will meet your needs? (The answers here could include filters, privacy screens, positioning computer monitors away from foot traffic, educational materials and programs, privacy desks, customized browsers that authenticate users based on access level, etc.)
- Which tools match the risk level that your governing board or commission is willing to accept?

As you begin the process of evaluating your Internet management options, including filtering, keep in mind that the process of anonymous third-party site selection means no filter can guarantee patrons will never see content you or anyone else considers inappropriate. This is also important to remember when writing Internet policies; you cannot promise that patrons will never access information they find offensive.

Evaluative Questions about Internet Filters

After these questions, I have provided "checklist" questions for you and your

technical support staff to use in evaluating Internet content filters, and in the bibliography, I have cited several recent evaluations of Internet content filters. Here are several broad questions to ask about each product:

- Is the vendor's contract congruent with your policies and laws?
- Can you configure the filter so it is congruent with your Internet access and privacy policies and laws?
- Does the Internet filter integrate well into your current network operating environment (such as your operating system and network support capabilities)?
- Compared to similar products, how well does the filter block the types of content you intend to block, and provide access to resources you intend to make available?

Pay attention as well to TCO issues (Total Cost of Ownership). Does the filtering software require a separate piece of hardware, such as a dedicated server, and how much will that cost to establish and maintain (including annual licensing requirements for the filtering database and technical support)? Will you require special training or more staff hours to support it? Do you need to purchase additional hardware to implement the filter? Who will be responsible for ensuring that it works properly? Will the company provide a list of current customers or at least several libraries that are using its product? Will you need to train library staff how to respond to inappropriate blocks? If it is an remote proxy server, does it require communicating with the company every time a minor change is required? One library wrote its own web browser in order to implement filtering in a manner consistent with its Internet policy; this was a significant investment. These are only a few questions to consider in introducing any new technology, including filters, in your network.

Features In Filters

In the table below, I have left two columns empty for you to fill in. The first column, Ranking, is where you would weight or prioritize each feature. Decide on a weighting scheme—for example, 1 for "must," 2 for "should," 3 for "nice to have," etc. The second column, Grade, lets you evaluate the ability of the product to fulfill this feature—any scale will do, but school grades (A through F) are one way to go. Finally, TCO is your calculation, based on the initial and ongoing costs of the filtering software and associated hardware, network, equipment, personnel and training costs, of what it will cost you to deploy this filter in your networking environment.

In some cases, you may end up with a requirement that no filter can meet. One recourse is to communicate your needs to the vendors whose products otherwise meet your top ranking criteria. For example, if the filters that are compatible with your network operating environment will not allow you to view the stoplists they use to block websites, you should take that concern back to the vendors and

negotiate from there. Since in some cases you may experience external pressure to use a particular filter, consider documenting your product decisions to explain to your stakeholders why you have chosen not to implement a product.

Finally, please note the extensive product notes below this table. For further explanation of these product criteria, see extended discussions in Schneider, Karen G., A Practical Guide to Internet Filters, Neal Schuman, 1997.

	Feature	***Found In***	***Ranking***	***Grade***	***TCO***
1	Vendor-supplied stoplist	Most filters			
2	Viewable stoplist	A couple of client filters			
3	Add or remove sites in stoplist	Most filters			
4	Automated stoplist download	Most filters			
5	Frequency of stoplist update	Varies widely			
6	Support third-party lists (Note 1)	Most filters			
7	Keyword filtering	Most filters			
8	Can disable keyword filtering	Most filters			
9	Block to file level (Note 2)	Most filters			
10	Block by protocol (Note 3)	Many filters			
11	Block by time of day (Note 4)	Many filters			
12	Block by NT or Novell user groups	Many service-based filters			
13	Block by IP of workstation	Many service-based filters			
14	Can talk to ILS patron database (Note 5)	One or two server-based filters			
15	Host name resolves to IP (Note 6)	Most filters			
16	Support barcode entry (Note 7)	Many server-based filters			
17	Support smart-card logins (Note 7)	Many server-based filters			
18	Support multi-choice login pace (Note 8)	Some server-based filters			

19	Vendor-defined categories	Most filters			

Notes Regarding Filters

Note 1. Support Third-Party Lists. This feature allows you to create your own filtering lists. This can be particularly useful for special-use computers, such as machines restricted to commercial databases, or children's computers you wish to restrict to several h undred "kid-friendly" resources.

Note 2. Block to file level. The filter is able to block individual files on websites, versus an "all or nothing" approach where the entire site is blocked or not blocked.

Note 3. Block by protocol. The filter can block or enable access to specific protocols, such as telnet, ftp, Usenet, and SMTP. This feature was more significant before most applications moved to the Web, but still can be useful in some settings.

Note 4. Block by time of day. The level of access can vary with the time of day. One useful application of this feature is to block all or most Internet access when the library is not open, to prevent contractors from using Internet computers for personal use.

Note 5. Can talk to ILS patron database. A very nontrivial feature. Vastly simplified for this Technote, a filter that can talk to a patron database presumably has an API (application programming interface) that allows data to pass between the filter and the integrated library system (ILS). This would provide the potential to use the ILS for authenticating and organizing access to the Internet, for example, providing filtered access for children and unfiltered access for adults.

Note 6. Host name resolves to IP. Some less-expensive filtering software is unable to translate the IP (numeric) address for a website to the hostname, meaning filtered websites can be easily bypassed by typing in their IP addresses. However, the flip side of this problem is that filters

Note 7. Support barcode and/or smart-card login. Several server-based filters offer the potential to authenticate users through barcoded cards or proprietary smart-cards.

Note 8. Support multiple-choice login page. The filter can support an authentication page that allows users to select how they log in (filtered or unfiltered access, for example).

Note 9. "After hours" feature. This feature, discussed earlier, stores selected websites in an offsite server, for later retrieval.

Note 10. Option to warn versus block. This feature provides the ability to present a warning screen which a patron could then choose to override.

Note 11. Option to monitor versus block. Some filters provide the capability to turn on the filter and run it in filtering mode without blocking, so you can analyse how the filter works, what sites are accessed, and what sites the filter blocks.

Note 12. Web rating systems are not in widespread use, but occasionally come up in discussion. These rely on voluntary rating systems for Internet websites, and browsers that support implementation of these ratings. See Schneider, A Practical Guide to Internet Filters, for a longer discussion. Web rating systems are not important criteria for an Internet filter.

Note 13. Administrative override for blocking. Some filters allow administrators to override a block by entering a password.

Note 14. Administrative delegation. Some filters provide the capability to delegate selected administrative functions to other staff, including the ability to administer an entire subnet without full access to the server. Selective delegation of administrative functions is particularly useful when it enables system staff to empower front-line staff, such as reference librarians, to override blocked content.

Note 15. Remote administration. Allows the software to be managed remotely, most often through a Web interface. Some server-based products require installation of the management module at each client used for administration—a cumbersome requirement.

Note 16. Report and logging capabilities. Analysing what the filter does requires its ability to log detailed filtering activities. Some filters provide internal report tools. Otherwise look for filter logs that can be interpreted by standard applications such as Excel, Access or Webtrends. Look for "canned," customizable reports.

Bibliography

1. Children's Internet Protection Act (CIPA)

Bocher, Robert. 2001. Wisconsin E-Rate Information.
Bocher, Technology Consultant for the Wisconsin Division of Public Instruction, also serves on the E-Rate Task Force of the American Library Association. His analyses of CIPA are excellent; other resources on this site include a chronology of filtering legislation.

[CIPA Website.] American Library Association. 2001.
This website provides information about the status of ALA's lawsuit, full text of the legislation, legal analyses, and additional citations related to the Internet, filtering, and intellectual freedom.

Center for Democracy and Technology. 2001.

A readable version of the actual text of the CIPA legislation.

Federal Communications Commission. 2001. [FCC CIPA Regulations.]

These are the FCC's regulations for compliance with CIPA. This document is essential reading for library administrators, systems librarians and E-Rate coordinators. The regulations provide most of the answers to commonly-asked questions about implementing CIPA.

Latham, Joyce. 2001. Positioning the Public Library in the Modern State: The Opportunity of the Children's Internet Protection Act (CIPA). First Monday, 6:7.

A legal and historical analysis of CIPA. Thoughtful and far-reaching; addresses the question of public forums and the library.

Schools and Libraries Division. Universal Service Corporation. 2001. Specific CIPA Guidance for Year 4 "Undertaking Actions" Certification.
Another helpful document for administrators navigating the CIPA implementation maze.

Filtering

Ayre, Lori Bowen (2001). Internet Filtering Options Analysis: An Interim Report. Infopeople Project.
An evaluation of key filtering products, with guidelines for assessing and selecting filters. Addresses limitations of filters without making that the focus of the report.

"Digital Chaperones for Kids," Consumer Reports, March, 2000.
This well-respected consumer magazine evaluated Internet filters and concluded they were imperfect.

Hunter, Christopher. Filtering the Future?: Software Filters, Porn, PICS, and the Internet Content Conundrum. 1999.
This lengthy paper, submitted in partial fulfillment of a thesis requirement, discusses the imperfections of filters.

Hunter, Christopher. "Internet Filter Effectiveness: Testing Over and Underinclusive Blocking Decisions of Four Popular Filters." Computers, Freedom, and Privacy 2000 Conference Proceedings.
Another analysis of the performance issues related to content filtering by a doctoral student who has followed this issue for several years.

Intellectual Freedom Committee, American Library Association. 2000. Statement on Library Use of Filtering Software
ALA's statement on filtering is frequently misquoted; read it carefully.

Lewis, Peter. "Web `watchdogs' work to block sex, violence from eyes of young surfers." *The Seattle Times* Dec. 17, 1997.
A reporter interviews the young part-time employees selecting sites to block in filters.

Meeks, Brock and McCullagh, Declan. 1996. Keys to the Kingdom.
An early expose of Internet content filters; one of the first recorded instances of a filter blocking innocuous sites such as the National Organization for Women.

"Lifting the Curtain on Web Filter Strategies ," *New York Times*, November 16, 2000.
A history of efforts by the filtering industry to protect the content of their stoplists.

Nunberg, Geoffrey. The Internet Filter Flimflam.
A scientist at Xerox PARC evaluates filtering.

3. Other Related Resources

Glogoff Stuart, The RFP Process. [1998.]
A concise and articulate overview of the process for establishing a Request For Proposal.

Schneider, Karen G. (1997). A Practical Guide to Internet Filters. Neal Schuman.
An early study of Internet content filters, including evaluation of 12 filtering products. Includes an in-depth discussion of how filters work.

For further reading about filtering, see in particular Christopher Hunter's bibliography,

Library Research Center. Graduate School of Library and Information Science. 2000. Survey of Internet Access Management in Public Libraries. University of Illinois.
A study found that approximately 15% of all public libraries filtered at least one Internet computer.

Author Notes

Karen G. Schneider is the Coordinator, Librarians' Index to the Internet, lii.org (as of October 1, 2001). Schneider, who has extensive public library experience, is also the author of A Practical Guide to Internet Filters (Neal Schuman, 1997), co-moderator of PUBLIB, the discussion list for public librarians, a columnist for American Libraries, and a frequent speaker on library issues. The Public Library Association's Tech Notes project grew out of the desire to continue the work of *Wired for the Future: Developing Your Library Technology Plan*, by Diane Mayo and Sandra Nelson, published for PLA by ALA in 1999. Each of the Tech Notes, written by GraceAnne A. DeCandido, is a Web-published document of 1500-2000 words, providing an introduction and overview to a specific technology topic of interest to public libraries at a particular point in time. Topics were identified by PLA's Technology in Public Libraries Committee. Each Note is marked with the date of its completion and posting, and with the date, approximately one year later, when links and other information were reviewed.

The Technology for Public Libraries Committee is currently evaluating if the Committee should request PLA funding for additional Tech Notes. Readers' comments and suggestions are welcome and should be addressed to pla@ala.org. Please use *Tech Notes* in your subject line.

Return to PLA home page

RFID Technology

Video Teleconferencing: Here, There, and Everywhere

Metadata: Always More Than You Think

DOI: The Persistence of Memory

Electronic Statistics: Counting Crows

Wireless Networks: Unplugged, and Play

Intranets: The Web Inside

Push Technology: Pushed to the Brink

Digital Disaster Planning: When Bad Things Happen to Good Systems

Filtering: No Easy Answers