

**Ohio Library Council  
Children's Internet Protection Act (CIPA)**

**“TECHNOLOGY PROTECTION MEASURES”  
WITHIN THE CHILDREN'S INTERNET PROTECTION ACT**

**Introduction**

The following discussion is designed to assist Ohio public library directors, trustees and library employees understand some of the basic technological implications of the United States Supreme Court decision regarding Children's Internet Protection Act (CIPA). Further, this document will offer an overview of the technologies and choices that need to be made regarding the Act's requirement for “technology protection measures.”

The Ohio Library Council, OPLIN, the State Library of Ohio and other organizations have made a number of attempts to communicate with decision makers as to the economic and political implication of the decisions they make regarding the use of Internet filters. The following discussion is not intended to answer the questions about whether a library should apply for E-Rate refunds or LSTA grants, whether a library should filter its Internet computers; or how many computers should be filtered. The intent is to provide decision makers with information about the technologies available and the choices available to them in configuring such products. Finally, this discussion will explore features within these products that enable library staff or the adult user to “disable the filter on request for “bona fide research or other lawful purposes.”

**What are technology protection measures?**

What does the phrase “technology protection measures” really mean? Are we talking about “filters” and “blocking/software”? For the most part the answer is yes. However, filtering and blocking software programs come in a variety of formats, using different underlying technologies, and may be bundled with other products that extend beyond the scope of simply a “filter”. A good example is the incorporation of filtering capabilities within public access computer scheduling software. Other products have sold themselves as not being a filter, but as “a selection tool.” How these products should work isn't described in the Act or by the Court but the goal is to “filter or block access to visual depictions...that are obscene...child pornography...or harmful to minors...”

**What kinds of filters are there?**

There is a wide range of products on the market. Some are not very appropriate for the public library environment. For instance, there are products that don't block sites but allow for tracking usage for later review and counseling. Parents might find this useful with children if inappropriate sites are being accessed. While tracking software may be a useful tool in the home, such products don't fit well in a library setting where patron privacy is protected under state law.

By far the most common filtering products used in the library market work with an internal database of web site addresses or specific URLs. When computers controlled by these products access the Internet, the internal database is consulted and users are denied access when the requested pages match what is in the database. In the case of standalone filters, software is loaded onto individual machines, configured by library staff with the control and management features hidden and password protected.

Some products only provide the tools, but require the administrator to manually add a list of “blocked” sites, but with the number of sites with adult content growing daily, the most effective web filter products require a subscription service for regular updates of the list. Some vendors claim that

their products have millions of blocked sites. Commonly used products in Ohio public libraries include: N2H2, CyberPatrol, IPrism, Surf Control, and WebSense. Other products in use include, Censornet, Content Watch, Cybersitter, Norton Internet Security, Novel Border Management, SonicWall, SAM, Symantec and X-Stop.

How these products work vary greatly. Some are standalone packages that are intended for a single copy to be installed on a single computer. If a library has only four or five computers such products are quite appropriate. Other products are designed for larger groups of computers and may require a centralized server to operate and specialized network management skills on staff.

### **What is to be blocked?**

The Children's Internet Protection Act only requires blocking of "visual depictions". Theoretically setting a browser to "text only" would satisfy the requirement, but such a strategy is probably not practical as the pervasively graphic nature of the Internet makes use of a text-only browser less than satisfactory to most users.

Each product offers administrative tools to select specific categories of content to be blocked, such as "pornography", "nudity" or "sex". Since the products sold to schools and libraries are also the same packages sold to corporate accounts, a librarian may be surprised by the wide range of Internet content that can be blocked, such as, "sports", "travel", "job hunting", and "humor". One of the biggest decisions a library has to make if it decides to employ a filtering product is to decide which categories to filter. Limiting the categories to be blocked increases the likelihood that some inappropriate content will not be blocked. As libraries select additional categories, they run the risk of blocking sites that were not intended. A 2001 Department of Justice study found that typically filters miss at least 2% of the content they attempt to filter and erroneously block access to 4% of the materials that they shouldn't block. Critics of filtering products estimate a much higher error rate.

Knowing which sites are being blocked erroneously is big challenge. Filtering products are criticized for keeping secret the sites that are being blocked by their products. Most vendors see the blocked site lists they build as confidential and proprietary. They see them as a part of their competitive advantage. Some vendors have been accused of having an ideological agenda and using such a product could compromise the library's role as an impartial source of information. The buyer needs to be aware. Finally there is no CIPA approved list of sites or category of sites. Each library needs to interpret the needs of its own community and its filter setting will have that same local interpretation.

### **What can be unblocked?**

Library staff and patrons may encounter sites or web pages that they feel should be blocked or unblocked. Sites blocked by a vendor's product might be a simple mistake. They may also be the result of an oversight or a new set of pages at an old address. Vendors should provide end users and filter administrators a mechanism for reporting problems and a feedback mechanism to let the user know what action if any the vendor has taken or plans to take in re-evaluating a label or rating. Ideally in a public library setting, a blocked site reconsideration request by a patron should be reported to the library so that the library knows how responsive the vendor is.

The library should have the ultimate say over whether a site is blocked or unblocked. Some vendors have an override file that library staff can enter addresses for sites that the library feels are erroneously rated and that the vendor is unwilling to re-evaluate.

## **How can the library disable the filter temporarily for adult patrons?**

CIPA requires that all library computers should be filtered but that adult patrons should be able to have the filter temporarily disabled for “bona fide research and other lawful purposes”. The Supreme Court’s decision has broader implications as there are many libraries that choose to use filters but do not apply for E-Rate funding or LSTA grants. The Court, in its ruling, warns that access to blocked sites within a reasonable time period must be granted. But how can this be achieved is the subject of considerable discussion.

Different filter products have different override options. Most have a button or other path to where an authorized staff member can disable the filter for selected sites or for a certain time frame. Typically this would mean that a reference librarian or other public service staff member would receive a request from an adult patron to disable the filter. The staff member would enter a password on the user’s computer and disable the filter. Depending on the nature of the override feature the Internet web-browser may have to be restarted. Some products may require that the computer be restarted.

Some products take advantage of library circulation records in either profiling the user or allowing a user to enter their library card bar code number to initiate the override process. For instance, one product interacts with computer registration software and queries the user for their barcode number during the login process. Adult patrons who enter their card number may choose filtered or unfiltered access to the Internet during their session.

Another automated mechanism allows adult users to temporarily disable its filters when a blocked site is encountered. A page warning that the site is blocked appears and the user can use their library card number and in some cases a personal identification number (PIN) to disable the filter. Once disabled the user has unblocked access for the rest of their Internet session or for a specific time period.

The library needs to be sensitive to how the library disables its filter for “bona fide research or other lawful purposes.” Any mechanism that requires intervention by a staff member must be done in a way that is done within a reasonable time frame and is done without inquiry as to why the user wants the site unblocked. Any automated system that allows unfiltered access or temporary disabling of the filter should ensure a level of patron privacy and confidentiality or the library runs the risk of placing a chilling effect on users. Among the most significant implications of the Supreme Court’s ruling is that regardless of whether or not the library seeks E-Rate monies or LSTA grants, if the library chooses to filter all of its public Internet computers, the library must provide a mechanism for adults to have unfiltered Internet access.