Recommended Actions for Libraries on Filtering

The following recommendations are described in detail below:

1. Consider refusing E-rate and LSTA funding
2. Choose least objectionable filtering software
3. Configure filtering software to block only material required by CIPA
4. Establish procedures to conveniently disable filtering
5. Establish procedures to unblock individual sites
6. Inform patrons of rights under CIPA
7. Establish policy for minors

Consider refusing E-rate and LSTA funding

The Children's Internet Protection Act (CIPA) only requires filtering if Internet access is funded partially through the Library Services and Technology Act (LSTA) or E-rate programs. If a library does not accept that funding, there is no need to install filtering software. Each library must therefore make its own decision about accepting funding, balancing the benefits of funding against the costs of filtering (both economic and intangible).

A careful examination should be made of the economic costs involved in filtering. It is necessary to consider the costs on both an upfront and ongoing basis. In addition to the obvious costs of licensing the software, consideration should be given to the staff costs involved in maintaining and updating the software, as well as handling disabling and unblocking requests. If a library is currently offering filtered access as an option to library patrons, the incremental costs of mandatory filtering are likely to be relatively low. However, a library that does not currently have filtering software may be faced with substantial costs – perhaps even greater than the funding provided by the E-rate and LSTA programs. It is important to note that E-rate funding cannot itself be used to buy or maintain filtering software.

Choose least objectionable filtering software

As mentioned above, no filtering program accurately blocks only what is required under CIPA – all programs also block considerable amounts of perfectly unobjectionable material. The ACLU therefore cannot recommend any particular software. Instead, we list several desirable characteristics that should be considered when choosing which filtering software to use.

First, the software should be able to be configured to block only images, not text. CIPA only requires the blocking of visual depictions. Unfortunately, the ACLU is not aware of any off-the-shelf software that has this as an option; the standard seems to be

blocking of entire web sites, rather than just images. It may be possible to run custom software in conjunction with standard filtering software in order to block only images – the Tacoma Public Library has used such a combination for several years. (Note, however, that as of this writing Tacoma's solution does not meet several of the other criteria listed below.)

It should be possible to disable filtering on a workstation-by-workstation basis. This is necessary in order to comply with the constitutional requirement of disabling filtering upon request of an adult user. Disabling should be easy and convenient; ideally it should be possible for individual patrons to disable the filter without requiring librarian intervention. Unfortunately, most filtering software is designed with the exact opposite goal – making it very difficult for an individual user to disable filtering. This may be appropriate in a home setting where parents do not want their children to turn the filter off, but it is entirely inappropriate in a library setting where disabling is constitutionally mandated.

The filtering software should have categories that closely correspond to the three categories required by CIPA:

- obscenity
- child pornography
- material harmful to minors

It should be easy to turn on and off filtering for material harmful to minors, as CIPA requires that to be blocked only for minor patrons.

The filtering software should accurately filter based upon the selected categories. In actuality, all software both underblocks (fails to block material that it should) and overblocks (blocks material that should be allowed). The determination of error rates is a difficult and controversial procedure, which is affected both by the method of testing used and by the configuration of the filtering software, so there is no definitive answer as to which programs are better or worse, although a number of studies have been done – see below under "Resources."

A highly desirable characteristic is the existence of an open list of blocked sites. Most companies consider their lists of blocked sites to be a trade secret, and go to great lengths (both legal and technical) to protect that secrecy. This seriously hampers the ability of a library (or any organization) to evaluate the accuracy of the filtering software. The American Library Association and the ACLU have urged filter companies to open their lists, and individual libraries should do so as well – with the added clout of being a potential customer.

Even the most accurate software will still overblock. It should be possible to override the software's blocking decision for individual sites or portions of sites, so that access is allowed. There should be a convenient way to have this apply to multiple workstations at once, preferably the entire library system.

Finally, the software should clearly indicate when it has blocked access to a site. This should take the form of a notice on screen, preferably with a description of the

procedure to be used if the blocking is in error. At a minimum, the message should state that the site was blocked, rather than looking like a normal access error (e.g., a broken link).

Summary of desirable characteristics:

- ability to block only images
- ability to disable filtering on a workstation-by-workstation basis
- categories that closely correspond to the three categories required by CIPA
- accuracy in blocking sites based on selected categories
- ability to unblock individual sites, applying to all workstations
- open list of blocked sites
- clear indication when it has blocked access to a site

Resources on filtering software accuracy:

Reports of overblocking by a variety of filtering programs can be found at http://www.peacefire.org.

Expert testimony presented in the challenge to CIPA, discussing the accuracy of filtering software, can be found at http://cyber.law.harvard.edu/people/edelman/mul-v-us.

A study commissioned by the Department of Justice in the defense of CIPA can be found at http://www.etestinglabs.com/clients/reports/usdoj/usdoj.pdf.

Most recently, the Kaiser Family Foundation examined blocking rates particularly in the area of health information; the results are at http://www.kff.org/content/2002/3294/Internet_Filtering_exec_summ.pdf.

Configure filtering software to block only material required by CIPA

Once a particular filtering program is chosen, it must still be configured. In all or most cases, the default configuration of filtering software upon installation blocks far more material than is required by CIPA. For example, it is not uncommon for a filter to defaultly block all “free” web sites – such as the personal home pages hosted by geocities.com.

In order to comply with CIPA, the software should be configured to block only a very few categories. The names vary from program to program, but are most likely to be something like “Pornography,” “Obscene,” or “Sex”. Only obscenity and child pornography need to be blocked for adults; in addition, material “harmful to minors” must be blocked for minor patrons. It is necessary to read the vendor’s description of the categories closely; for example, in one program “Pornography” may more closely

correspond to obscenity and "Sex" to "harmful to minors," whereas in another program "Sex" encompasses both.

Some filtering software also has subcategories that can override a larger category that is blocked. For example, a health information site that includes nudity may normally be blocked by "Sex," but would be allowed if the subcategory "Medical" is specified. In general, it probably makes sense to enable all of these subcategories – if a filtering company thinks it should be offered as an option, it indicates that the subcategory almost certainly doesn't fall with CIPA's narrow blocking requirement.

Some filtering companies are now recommending settings to comply with CIPA. Since the company best knows what material is blocked by each category, it probably makes sense to follow its recommendation. And, of course, if the software has an option to block only images, that option should be selected.

Establish procedures to conveniently disable filtering

Libraries must disable filtering software immediately upon the request of an adult patron, with no questions asked. The procedure for requesting disabling should be clearly posted. Selective disabling on individual workstations is likely to require at least some software to be installed on each computer, rather than handling all filtering at the server level.

The best method, requiring custom software, would allow an individual patron to disable the filter automatically, without having to contact a librarian. For example, the software could ask users whether they wish filtering to be disabled at the beginning of each session, or on any occasion when the user attempts to access a blocked site. Another possibility would be to have a bank of computers where filters are disabled, at least each morning or maybe even permanently, and allow only adults who wish unfiltered access to use those computers.

It may also be convenient to allow a library patron to request permanent disabling of filters. This makes most sense if a library uses a system of Internet access that requires signing in, perhaps with a library card number. If a patron requests permanent disabling, this could be noted on his or her library record, and filtering can be disabled automatically whenever the patron signs on.

Establish procedures to unblock individual sites

As mentioned above, all filtering software is notoriously inaccurate. Many sites end up being blocked even though they contain no objectionable material. However, most filtering programs allow the default blocking decisions to be overridden at the local level. We believe it is very important to do so – otherwise many valuable resources on the Internet will not be available to library patrons.

A procedure should be established for any person to request unblocking of an individual site. This procedure should allow for anonymous requests, though it should also have an option for the patron to provide a contact method (such as an email address)

to be notified when unblocking occurs (or if the request is denied). Ideally, it will be incorporated into the filtering software, so that whenever a site is blocked, a message comes up telling the user how to request unblocking – preferably with a single click. The message should also remind the patron they have the right to disable filtering entirely, and again would ideally do so with a single click. This level of incorporation may require custom software in conjunction with standard filtering software, as done in Tacoma.

When a request for unblocking is made, staff should evaluate the site promptly, and determine whether or not it falls into one of the three CIPA categories: obscenity, child pornography, or harmful to minors. If not, the site should be unblocked. Ideally, the unblocking should apply throughout the library system; at a minimum, it must apply to the workstation or library where the patron requested unblocking. Because the decision should apply widely, it is probably best to have the site evaluation done by a single, centralized person using standard criteria. It should be remembered that the CIPA categories are quite narrow, so most requests to unblock should be honored.

The trickiest situation is when an adult requests unblocking of a site that is not obscene, but might be considered to be "harmful to minors." Adults are entitled to see such sites; minors aren't. But most software only allows complete unblocking or complete blocking of a site for all workstations and for all patrons. Libraries can set up two entire software systems, one used by minors and one by adults, with sites that are "harmful to minors" blocked on the minors' system but not blocked on the adult system. Or, alternatively, libraries can tell the adult that it cannot unblock a "harmful to minors" site for her or him. Of course, the adult has the right to disable the filter entirely, and the library should remind the adult of that fact.

Inform patrons of rights under CIPA

Library patrons should be informed that their Internet access is filtered, and that they have a right to unfiltered access. This is also a good opportunity for a library to explain that the library itself is protective of free speech, and is being forced to compromise its principles by the federal government – to the extent of being forced to install software that is known to have problems. We recommend a notice something like:

> Federal law requires us to install blocking software on Internet access computers. Blocking software blocks access to sites the software company thinks offensive. It is well established that the software does not work properly. It overblocks (blocks sites no one would think objectionable) and underblocks (fails to block sites that some might think objectionable). The companies also won't tell us – or you – what they have blocked.
>
> Because of the problems with the software, we will turn it off for any adult (person 17 or older) who asks. We won't ask any questions. The procedure for that is [insert the local procedure]
>
> We will also unblock any site that is inappropriately blocked. If you want a site unblocked, the procedure is [insert the local procedure].
>
> If you are under 17, [insert the local procedure].

Establish policy for minors

Each library should establish a policy for how it will handle minor patrons. This policy should include the method used to verify age. No particular method is required by CIPA, so each library can choose any sensible way to distinguish patrons on the basis of age, as long as it is done in good faith. It can screen at the entry to the computers. It can have sign-on systems that are linked to patron databases that include age. It can have smart cards. It can probably rely on visual cues for most patrons. It can require proof of age where it has doubts. The system it uses may depend on how it decides to implement the unblocking decisions.

The policy should specify the procedure minors should use to request the unblocking of inappropriately blocked sites, which is clearly allowed by CIPA. It should also establish whether and how minors can receive unfiltered access (e.g., at any workstation, only in the adult section of the library, only with parental permission, or not at all). Unfortunately, the Supreme Court's decision did not clarify minors' rights. That ACLU recommends that libraries do what they, as professionals, think is right. If a library is protective of the First Amendment and encounters difficulties, it should call us and we'll try to help.