

MEETING CIPA REQUIREMENTS WITH TECHNOLOGY

By Richard W. Boss

Public libraries have been concerned with the issue of access control versus access management for a number of years. While some public libraries have sought to deny access by children to some Web sites, a larger number have focused on managing access, including authenticating patrons, providing links to selected Web sites, metering of use, and compiling of reports. As recently as 2002, fewer than 25 percent of public libraries had blocking or filtering products on all public Internet workstations and 17 percent had blocking or filtering products on only some. More than 58 percent used nothing at all. With the adoption of the Children's Internet Protection Act (CIPA), the issue has become financial as well as philosophical because schools and libraries will lose federal funds if they do not control access by minors to sites that are proscribed by the legislation.

Despite the fact that the terms "blocking" and "filtering" are often used interchangeably, including by legislators, they do have different meanings. "Blocking" refers to stopping access to something based on its URL; "filtering" refers to stopping access to something based on its content. Almost all of the available products do blocking, but not all do filtering. Nevertheless, vendors may refer to a product that does only blocking as a "filter."

CIPA compliance is required when using funds for particular purposes from three federal programs: E-rate, ESEA Title II D, and LSTA. When a school or library receives discounts from the E-rate program and either or both of the other programs, its CIPA requirements take precedence over the requirements in the ESEA or LSAT programs. A related act known as the Neighborhood Children's Internet Protection Act (NCIPA) focuses on what has to be included in a school or library's Internet safety policy.

There are two basic requirements in the CIPA legislation:

1. A school or library must have some type of blocking or filtering technology on all of its computers from which there is access to the Internet. Both patron and staff computers are affected. The technology must protect against access to visual depictions described as obscene, child pornography, or harmful to minors in the Act. CIPA does not require the blocking or filtering of text. The law does not address the question of laptops brought in by staff and patrons, but a consensus has emerged that these need not be blocked or filtered.
2. A school or library must have an Internet safety policy and hold a public meeting to review the policy. The policy must incorporate the criteria described in NCIPA.

Whether a school or library blocks and filters content other than the visual depictions defined in the law is a local decision.

The FCC has ruled that if a member of a consortium is not in compliance with the law, only the non-compliant members will be penalized.

The law states that any authorized school or library staff member may disable the blocking or filtering product to allow an adult to have unrestricted Internet access for any lawful purpose. Adults are defined as persons 17 years of age or older. A strict reading of the law would preclude coding the status of a patron in the library card and automatically turning off the blocking or filtering when the I.D. was entered.

The Federal Communications Commission (FCC) is charged with enforcement of CIPA/NCIPA for the E-rate program. The Department of Education (DOE) and the Institute for Museum and Library Services (IMLS) are charged with ESEA and LSTA enforcement respectively, but a school or library receiving E-rate discounts and ESEA or LSTA funding needs to comply with CIPA's E-rate requirements to obtain funding from any of the programs. Schools not receiving E-rate discounts, must certify that they have an Internet Safety Policy in place in order to receive ESEA funding that will be used for Internet access; public libraries not receiving E-rate discounts must certify that they have an Internet Safety Policy in place in order to receive LSTA funding that will be used for Internet access.

It is not possible to discuss all of the available blocking and filtering products in this TechNote. The eight that appear to have been most widely adopted by libraries are discussed herein. For additional objective evaluation of blocking and filtering products, consult a report by Australia's CSIRO for NetAlert and the Australian Broadcasting Authority at www.aba.gov.au/internet/research/filtering/filtereffectiveness.pdf

All of the products were developed before CIPA, either as products for home use or for organizations seeking to control the activities of employees. They, therefore, block and filter words as well as images. All of the products contain a list of URLs that are blocked, but the list is often not available for review. Some also contain content analysis tools that filter. Only two use object analysis. For example, a graphic image with a great deal of flesh tones will be filtered. All of the products are password controlled. Online and telephone technical support is available for all of the products.

The products developed for home use are client-based; those developed for organizations are server based. However, two vendors of client-based products introduced a server option after CIPA was passed.

Blocking and Filtering Products

[Best N2H2](#) is a server-based blocking product that can be run on a wide variety of platforms, including firewall servers and network servers. The company targets corporate and institutional users. Best employs a full-time staff to categorize Web content. The 45 categories include adults only, drugs, lingerie, nudity, personals, sex, swimsuits, and violence. More than 150,000 sites that are blocked. A purchaser can select the categories to be blocked. The product may be used to block e-mail and chat rooms. There is a 30-

day free evaluation period, however, the time and effort required to configure the product on a server make it a good idea to undertake careful screening by consulting reviewing media before undertaking a trial.

A study by eTesting Labs for the U.S. Department of Justice in 2001 determined that N2H2 had the highest accuracy rate of any product it tested. It blocked 98 percent of the inappropriate sites used in the test. The study report does not appear to be available.

The author's own experience with N2H2 is that it blocks a lower percentage of non-pornographic sites than others.

[CyberPatrol 6.1](#) is a client-based blocking and filtering product developed to be run on Windows 98/Me/NT/2000/XP PCs. While it targets home users, it has been purchased by a number of small libraries because it is relatively inexpensive. Its list price is \$39 for a one-year subscription. The price includes software updates to CyberList, a "blacklist" of unacceptable sites, and online or telephone support. A 14-day free trial is available for evaluation.

The CyberList sorts sites into a number of content categories, including partial nudity, full nudity, sexual acts/text, gross depictions/texts, sex education, and drugs/drug culture. All categories are blocked by default, but a purchaser can select the categories that are to be accessible without blocking. There are also settings that restrict access to e-mail, chat rooms, and newsgroups. The product also does filtering using keyword analysis in content. It is also possible to enter specific words that are to be filtered.

A server based option is now available to larger libraries. Prices are quoted on request.

[CyberSitter 2003](#) is a client-based blocking and filtering product designed to be run on a PC with Windows 95/98/Me/NT/2000/XP. While it targets home users, it has been purchased by a number of small libraries because it is inexpensive, takes very little disk space, and easy to install. The list price is \$39.95 for a single computer license, \$59.95 for two, \$74.95 for three, \$99.95 for five, and \$199.00 for ten licenses. There are free list updates for one year. A two-year subscription to program upgrades is \$20. The program takes just 3.0 MB of disk space. Even though there are 30 categories of filtering, the menus are simple.

The subscription service not only uses a list of sites that deal with sex, drugs, hate, and violence, but also uses a content recognition system on sites that are not on the list. It filters access or will allow access after deleting words and phrases that appear to be objectionable. This can make a page impossible to read. The content recognition also results in a somewhat higher error rate than with a list of sites that have been examined by a vendor's staff. There is a way to add sites to block and there is a mechanism for overriding blocked sites. It can be set to filter out words in newsgroups, mail, chat, or messaging programs. URLs that have been blocked, but that are deemed suitable for minors, can be added to a "white list" so that they will not be blocked in the future. There is a simple on/off switch that can be accessed by someone with the appropriate password.

CyberSitter has won *PC Magazine's* Editor's Choice award for several years in a row.

A server-based option is available to larger libraries. The company quotes prices on request.

[CybraryN Solutions](#) Libraries that want only the blocking and filtering module and do not have a Dynix or VTLS system should deal directly with [Fast Data Technology](#) as that will result in a lower price. Pricing begins at 25 concurrent users and goes to a site license for more than 1,000 concurrent users. There is no published price list. FastTracker is also available as a hosted service.

FastTracker uses a not only a URL list, but also a content analysis tool. The company estimates that 75 percent of the sites that are blocked are on its list, and 25 percent are filtered as the result of content analysis. There does not appear to be a word list available, nor is there a way of permitting access to sites that contain words that are objectionable for reasons other than pornography. Its 30 categories are unusually broad, including job search and shopping sites. That is due to the fact that the product was developed for organizations that are concerned about staff time lost due to surfing of the Internet that is not work-related. One of the claimed advantages of FastTracker is that policies for staff users can be set differently than for patrons, and extensive reports are provided on where users went and for how long.

[I-Gear 3.5](#) is a server-based blocking and filtering product that can be run on a Windows NT Server 4.0 or later, Sun Solaris 2.x server or later, or Red Hat Linux server 5.2 or later. It groups Web sites it has examined into 27 categories that can be blocked or not blocked. In addition it uses a Dynamic Document Review (DDR) that examines incoming text using key words and phrase that have both positive and negative weights. The resultant points score for a document is compared with threshold to determine whether the document should be filtered. Updates are available online via a single button click or the updates can be set to download automatically as they are released.

Prices are quoted after a library submits information about its size. They are negotiable.

[McAfee Parental Controls 1.0](#) is a client-based blocking and filtering product that can be used on any PC or Mac. It is priced at \$49.99, but is most often sold as part of McAfee InternetSecurity 5.0, a \$79.99 package that includes antivirus, firewall, and privacy features. The price includes free updates and free technical support for life.

The product has both a blocked-sites list and a word filter for detecting inappropriate content. Each can be locally edited. This gives librarians the opportunity to improve the accuracy of the blocking and filtering. It can filter pop-up ads and file sharing services. A unique feature of the product is object analysis. Unfortunately, it does not differentiate very well between famous paintings and pornography.

[NetNanny 5.0](#) is a client-based blocking and filtering product designed to be run on Windows 98/93SE/ Me/ NT 4.2/XP PCs. It targets home, school, and library users. It is

inexpensive at \$39.95 list, but it requires substantially more computer resources than its major competitors. It requires a minimum of 32 MB of RAM and 60 MB of hard drive space. While earlier versions required a tedious manual set-up, the current release is self-installing. It defaults to the most secure setting.

There are built-in lists of URLs and permitted and restricted words that can be modified by someone with an appropriate password. New lists of URLs can be downloaded manually or automatically on a daily, weekly, or monthly basis. It is possible to add URLs locally. Quota-based filtering makes it possible to filter Web pages containing more than a specified number of restricted words from the complete word list. An option allows access to be limited to sites that have been specifically authorized. A "Can Go" list of 3,000 Website recommended for children is available.

One unique feature is that it includes object analysis. As is the case with McAfee Parental Controls 1.0, it does not reliably differentiate between art and pornography. Another unique feature is that it can prevent family names, addresses, phone numbers and credit card numbers being sent from the PC.

[Websense Enterprise](#) is a server-based product that was developed for Fortune 500 companies to enable them to improve productivity and security. It manages Internet access, blocks peer-to-peer file sharing, and blocks undesirable sites using a large database of URLs that is updated daily. There are 88 categories. Particularly useful is the separation of sex and sex education sites. A companion product called Websense Enterprise Reporter has more than 80 pre-defined report templates.

The server can be a Pentium III or greater processor with 512 MB of RAM or a Sun Ultra 10 Processor with 512 MB of RAM. The operating system can be Windows 2000 or 2003 Server, Red Hat Linux 8.0-9.0, or Sun Solaris 2.6-9.

The product is suitable only for libraries that have a large number of workstations because the license fee is \$15,000 a year. A single license covers up to 1,000 workstations.

Questions to Ask of Vendors

The American Library Association's E-rate Task Force has developed a list of questions to ask vendors. There were 70 questions on the list as of March 1, 2004. Each question will not be relevant for all libraries. The list is available at <http://www.ala.org/ala/washoff/WOissues/civilliberties/washcipa/RFI.pdf>

Prepared by Richard W. Boss, April 14, 2004