CIPA: A Brief FAQ on Public Library Compliance

(Updated February 28, 2012)

Bob Bocher, Technology Consultant
608-266-2127, robert.bocher@dpi.wi.gov
Wisconsin Department of Public Instruction

This FAQ and other information on the *Children's Internet Protection Act* (CIPA) are at http://dpi.wi.gov/pld/cipafaq.html. While reasonable efforts were made to ensure the accuracy of this document, the Federal Communications Commission (FCC) or the Schools and Libraries Division (SLD) are the official sources of information. The author is not an attorney and library staff should seek legal advice as needed. Bob Bocher is on the American Library Association's E-rate Task Force and is a member of the State E-rate Coordinators' Alliance (SECA). Permission is granted to reproduce this FAQ with proper attribution.

Background: The 1996 *Communications Decency Act* (CDA) was the first attempt by Congress to regulate content on the Internet. Because its overly broad and vague language infringed on First Amendment rights, the Supreme Court found the CDA unconstitutional in 1997. In follow-up legislative efforts Congress more narrowly focused on protecting children from obscene material on the Internet. This led to passage of the *Children's Internet Protection Act* (CIPA) in December 2001. Shortly thereafter several organizations—including the American Library Association—filed suit claiming that like the CDA before it, CIPA infringed on the First Amendment rights of library patrons. The case eventually went before the Supreme Court which found CIPA constitutional in June 2003.

Q: Under what circumstances does my library have to comply with CIPA?
A: Any public library using E-rate or LSTA (Library Services and Technology Act) funds for the following purposes must comply with the law's filtering requirement. When a library receives both E-rate discounts and LSTA funds, the E-rate language of CIPA takes precedence.

1. *E-rate:* CIPA applies when getting discounts for Internet access or internal connections. Compliance is not required for discounts on telecommunication services, including voice and broadband circuits.
2. *LSTA:* CIPA applies when using LSTA funds to purchase computers used to access the Internet or to pay for Internet access. Compliance is not required for other uses of LSTA funds.

In 2008 Congress passed the *Protecting Children in the 21st Century Act.* This added statutory language to CIPA requiring schools to educate minors "On appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and [on] cyberbullying awareness and response." Schools must be in compliance with this added requirement by July 1, 2012. This act does *not* apply to libraries.

Q: What is the timeframe for complying with CIPA?
A: Compliance is done annually by checking the appropriate box on the E-rate Form 486, #11. Applicants applying for E-rate for the first time have their initial application year to come into compliance.

Q: What has to be filtered or subject to the "technology protection measure" (TPM)?
A: CIPA requires the filtering of certain images, but not the filtering of text or audio. The filter, referred to in CIPA as a "technology protection measure," must protect against access to images that (1) are obscene, (2) contain child pornography, or (3) are harmful to minors. The first two prohibitions are defined in federal statutes. Obscenity is also frequently defined in state statutes and local ordinances using guidelines established in the Supreme Court's 1973 Miller v. California decision. "Harmful to minors" is defined in CIPA. It takes the Miller definition of obscenity and applies it with respect to minors under age 17. In its CIPA order and regulations (released April 5, 2001), the FCC declined to "amplify the statutory definitions" in the law or to provide further guidance in this area. Of interest, only a court can legally determine if an image is obscene. However, librarians must make this decision on a regular basis to uphold the library's Internet use policy and to comply with CIPA.

Q: What computers must have the Internet TPM?
A: The law states that a library must have a TPM in place "with respect to *any of its* (emphasis added) computers with Internet access." This includes library owned computers wherever they are located in the library, even in administrative areas not accessible to the public. During the drafting of the FCC regulations in March 2001, an FCC attorney indicated that it was a plausible interpretation of the law that patron owned laptops—often used to access the Internet via the library's wireless network—did not have to be filtered. This informal opinion is based on CIPA's phrase "its computers" which clearly refers to library owned computers. (There is no reference in

CIPA to non-library owned computers.) In fall 2011 the FCC indicated it plans to seek public comment on the issue of filters and patron (and student) owned devices in a forthcoming 2012 ruling making notice.

Q: Under what circumstances or conditions can the TPM be disabled?
A: The law states that any authorized staff may disable the TPM to allow Internet access for lawful purposes. In the E-rate section of CIPA the disabling provision applies only to adults (age 17 or older), but the LSTA section allows anyone to request that the TPM be disabled. Since authorized staff can disable the TPM, it should be relatively easy to craft a policy to allow staff to turn off the TPM for their own use. The disabling process is an important factor when evaluating any filtering software, in part because the Supreme Court's CIPA decision places considerable emphasis on disabling as a way to avoid First Amendment harm from over blocking. For example, Justice Kennedy's concurring opinion states that if a patron requests unfiltered access to view constitutionally protected content—and such a request is not honored in a reasonable manner—then the library places itself at risk of a possible "as applied challenge." This means a patron may claim that the library has applied CIPA's filtering mandate in such an onerous fashion that it is unconstitutionally blocking access to legally protected content. (Note: Currently a lawsuit is pending against the North Central Regional Library in Washington (Bradburn v. NCRL). The suit claims the library is over blocking and not complying with the unblocking language in CIPA.) The law does not require patrons to state why they want unfiltered Internet access. The Court's ruling supports the position that patrons simply have to request unfiltered access, with no explanation needed. It is important for a library's Internet policy to address the process by which a patron can request unfiltered access.

> CIPA has an important exception that limits speech-related harm. It allows libraries to permit adult patron access to an "over-blocked" Web site or to disable the filter upon request. —Supreme Court decision

In its CIPA regulations the FCC declined to provide any guidance on disabling procedures or policies. Libraries thus have considerable latitude in this area which has resulted in crafting disabling scenarios that are of minimal burden to staff and patrons. For example, one scenario is to allow adult patrons to select unfiltered access by choosing this option on the screen and electronically authenticating this action via the patron's library card. (In providing guidance on this issue an attorney retained by ALA indicated that such a scenario can be reasonably argued to comport with the law.) Further safeguards could include signage indicating "adult only" workstations and the library could require patrons to sign a statement indicating they want unfiltered access.

> FCC rules directing staff when to disable the filter would likely be overly broad, imprecise, and potentially chilling speech. We leave such determinations to local libraries. —*FCC CIPA Order*

Q: How effective does the TPM have to be?
A: The law states that the TPM must *protect* against visual depictions outlawed by the legislation. No TPM is 100% effective in *preventing* all such access. In its CIPA regulations, the FCC declined to further define the TPM requirements or to adopt any type of definition or certification on how effective a TPM must be, beyond the general "protect" language in the law. Thus, a vendor's claim that its TPM is "CIPA compliant" or that it meets "CIPA requirements" are of little value. In deference to local control, the FCC further stated, "We conclude that local authorities are best situated to choose which technology measures will be most appropriate."

> Adding a filter effectiveness standard does not comport with our goal of minimizing the burden we place on schools and libraries. Thus we will not adopt an effectiveness requirement. —*FCC CIPA Order*

Q: What are the legal implications if the TPM fails?
A: The FCC presumes that Congress did not intend to penalize libraries that act in good faith and in a reasonable manner to implement TPMs. The FCC also notes that failure to comply with the law's requirements could "engender concern among library patrons," and it believes that libraries will act to avoid such situations. A library *must have* policies and procedures to address any complaints in an expeditious manner. If a patron claims that too many allegedly illegal images are getting through the TPM, CIPA does not provide a venue for patrons to take legal action against the library. Rather, patrons can file a complaint with the FCC which will then initiate an investigation. The FCC can require a library to reimburse its E-rate discounts for any time it is out of compliance, but the Commission assumes that it "will rarely, if ever," be called upon to take such action. For LSTA, the Institute of Museum and Library Services (IMLS) can withhold future payments to the library but it cannot retroactively recoup funds for any time a library is out of compliance. To date, the author knows of no actions taken by the FCC or IMLS to penalize a library for noncompliance.

Q: Does it make any difference where the filtering takes place?
A: It makes no difference where the filtering is done. It can be done centrally by an Internet Service Provider, at the server level on the library's LAN or WAN, or the filter can be individually installed on each workstation. This latter option is practical only when the number of workstations is quite small.