FAQ on E-rate Compliance with the Children's Internet Protection Act
and the
Neighborhood Children's Internet Protection Act
(http://www.dpi.state.wi.us/dltcl/pld/cipafaq.html)

February 19, 2004

Bob Bocher
Wisconsin Department of Public Instruction
Division for Libraries, Technology, and Community Learning

CIPA Lite FAQ: A two-page version of this FAQ is available at http://www.dpi.state.wi.us/dltcl/pld/cipafaqlite.html. It focuses on library compliance with CIPA in light of the Supreme Court's June 2003 ruling that the filtering language in CIPA was constitutional for public libraries.

The following questions have substantive updates since the Supreme Court's decision.

- What is the impact of the Supreme Court's decision…?
- How do we certify for 2003 that we are meeting the law's requirements?
- What does the law mean by "technology protection measure" (TPM [e.g., filter])?
- What computers must have the Internet TPM?
- Under what circumstances or conditions can the TPM be disabled?
- What are the legal implications if the TPM fails…?

This FAQ is divided into the following areas:

While reasonable efforts have been made to ensure the accuracy of this FAQ, only information from the Federal Communications Commission (FCC) or the Schools and Libraries Division (SLD) should be considered official. Schools and libraries are also encouraged to seek legal advice in relation to CIPA and NCIPA compliance issues. The author is a member of the American Library Association's E-rate Task Force and of the Chief Council of State School Officers' State E-Rate Coordinators' Alliance. This FAQ is not, however, associated with these two organizations. If you have any questions on this FAQ, contact Bob Bocher, Technology Consultant, Wisconsin Department of Public Instruction, 125 S. Webster St., Madison WI 53707-7841, phone 608-266-

2127, fax 608-266-2529, robert.bocher@dpi.state.wi.us. Permission is granted to use any of the information in this FAQ with proper attribution.

I. Background on CIPA and NCIPA

The Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA) passed Congress in December of 2000. Both were part of a large federal appropriations measure (PL 106-554). The Federal Communications Commission released its regulations for CIPA and NCIPA covering the E-rate program in April 2001. This FAQ focuses primarily on compliance related to the E-rate program. See the Sources section at the end of this document for references to the Commission's regulations and more information on this legislation.

CIPA and NCIPA: There is some overlap in language between these two sections of PL 106-554 but they do address different areas. The Children's Internet Protection Act addresses what has to be filtered and the need for an Internet safety policy. The Neighborhood Children's Internet Protection Act focuses on what has to be included in a school or library's Internet safety policy. Moreover, NCIPA is applicable only to the E-rate program.

Federal programs: CIPA compliance is required when using funds for particular purposes from three federal programs: E-rate, ESEA Title II D (Ed Tech), and LSTA. When a school or library receives discounts from the E-rate program, its CIPA requirements take precedence over the requirements in the ESEA or LSTA sections of CIPA.

Public library filtering: The report *Public Libraries and the Internet 2002: Internet Connectivity and Networked Services* (http://www.ii.fsu.edu/Projects/2002pli/2002.plinternet.study.pdf) showed that 24.4% of public libraries nationwide had filters on all public Internet workstations, 17.5% of the libraries had filters on some public workstations, and the remaining 58.1% reported not filtering any public access workstations. The report did not address the filtering of staff workstations.

Previous Congressional actions on filtering: CIPA was not the first attempt by Congress to regulate Internet content or Internet access. The Communications Decency Act (CDA) was part of the Telecommunications Act of 1996, the same act that included the E-rate program. The CDA was subject to an immediate lawsuit and was ultimately found unconstitutional on First Amendment grounds by the Supreme Court in 1997. Following failure of the CDA to pass constitutional muster, Congress passed the Child Online Protection Act (COPA) in October 1998 (not to be confused with the Children's Online Privacy Protection Act, COPPA). Compared to the broader CDA, COPA more narrowly focused on Internet content deemed harmful to minors. It too was subject to a lawsuit and was found unconstitutional by the federal Third Circuit Court of Appeals in June 2000. After a hearing before the Supreme Court, the case was remanded back to the Third Circuit which again found COPA unconstitutional a second time in March, 2003. The federal government again appealed to the Supreme Court which will hear the case on March 2, 2004.

II. E-rate Compliance and Certification with CIPA and NCIPA

Q: Under what circumstances does my school or library have to comply with CIPA and NCIPA?

A: To receive E-rate discounts your school or library has to comply with CIPA/NCIPA as shown below.

Program	*Must Comply with CIPA Requirements*	*CIPA Requirements Do Not Apply*
E-rate	When getting discounts for • internal connections • Internet access	When getting discounts for • telecommunication services (voice or data)
ESEA Title IId and LSTA	When using funds for • purchasing computers that access the Internet • direct costs for accessing the Internet	When using funds for • any other purposes allowed by the program and state program guidelines

NCIPA is applicable only when getting E-rate discounts for internal connections or Internet access.

> We have attempted to craft our rules in the most practical way possible, while providing schools and libraries with maximum flexibility in determining the best approach. We conclude that local authorities are best situated to choose which technology measures will be most appropriate for their relevant communities.
> —FCC regulations, April 2001

The Federal Communications Commission (FCC) is charged with enforcing CIPA/NCIPA for the E-rate program. The federal Department of Education (USDoE) and the federal Institute for Museum and Library Services (IMLS) are charged with ESEA and LSTA CIPA enforcement respectively. A school or library getting E-rate discounts and ESEA or LSTA funding needs to comply with CIPA's E-rate requirements. The FCC released detailed CIPA/NCIPA regulations in April 2001. Those regulations are cited throughout this FAQ. The regulations give schools and libraries considerable latitude on how to implement the mandates in the law. Neither the USDoE nor the IMLS have developed detailed regulations.

To determine whether an E-rate eligible service falls under the purview of the act, consult the SLD's Eligible Services List (ESL). In general, applicants with services that are defined in the Internet or internal connections part of the ESL must comply with the law. Applicants with services defined in the telecommunication services area of the list are exempt from compliance for telecommunication services only. If your telecommunications provider is also providing your school or library's Internet access, you must still comply with CIPA's filtering provision if you get E-rate Internet discounts from your provider. If a telecommunications provider bundles the cost of the circuit with its Internet service, and you want to get discounts on the circuit without needing to comply with CIPA, it will be necessary to have the circuit costs broken out (e.g., separate line item on the bill) to be able to get discounts only on the circuit.

Q: What is the impact of the Supreme Court's decision and the FCC's follow-up Order on library compliance with CIPA's filtering requirement?

A: On June 23, 2003, the Supreme Court ruled 6–3 that the filtering requirement in CIPA is constitutional for public libraries. This action reversed a 2002 federal district court ruling that had found the filtering mandate unconstitutional on First Amendment grounds. This decision means that any public library using E-rate funds for purposes outlined above will need to comply with CIPA's filtering requirement. Following the Court's ruling the FCC released its Order on library compliance with CIPA on July 24. Especially critical in the Order are paragraphs 11-13 which have information on the timeframe for 2003 certification and the filing of the newly revised E-rate forms. (See also the following question on 2003 certification.)

> Especially because public libraries have traditionally excluded pornographic material from their other collections, Congress could reasonably impose a parallel limitation on its Internet assistance programs. As the use of filtering software helps to carry out these programs, it is a permissible condition.—Supreme Court ruling, June 2003

Highlights of the July 24 FCC Order.

- In part, because the FCC recognized the need of libraries to budget for costs associated with filtering technology and to plan for its implementation, the Commission has given libraries until the start of 2004 services to comply with CIPA's filtering mandate. For most libraries this will be July 1, 2004.
- The Order is clear that during the current 2003 E-rate funding year libraries need to (A) be already compliant with CIPA's filtering provision, or (B) be undertaking actions to comply with the filtering provision by start of 2004 services.
- The Order also references the need for libraries to develop a policy and procedure to unblock sites when requested to by an adult patron. This reinforces the language in the Supreme Court's ruling that libraries that do not unblock sites when requested by adult patrons face an increased risk of legal challenges by patrons. (See the question on unblocking below.)
- It is important to note that the Order focuses on issues associated with the timeframe for compliance by libraries. Most of the FCC's original CIPA regulations, issued in April 2001, are still valid.

IMLS action: On August 1 the federal Institute of Museum and Library Services (IMLS) released its guidelines for complying with CIPA when using LSTA funds. When receiving FY 2004 LSTA funds public libraries must certify either that (A) the library is in compliance with CIPA's provisions, or (B) the library is undertaking actions to comply by the time it starts using 2005 funds. The date by which libraries start receiving FY 2004 LSTA funding varies from state-to-state. State library agencies will be providing their libraries with information on the time frame for compliance.

Schools were not part of the CIPA lawsuit. Most schools needed to comply with the law's filtering requirement as of July 1, 2002.

Q: How do we certify for 2003 that we are meeting the law's requirements?

> **Note:** As of this FAQ's update (2-19-04), it is assumed that almost all schools and libraries have certified for 2003.

A: The FCC's July 24, 2003 Order has important 2003 certification information related to library compliance with CIPA's filtering mandate. Consult the Order, especially paragraphs 11-13, for details.

Certification of compliance is made by an appropriate "Administrative Authority" on the E-rate Form 486. This can be the school or library board, superintendent, principal, library director, or any other staff member with the authority to make such a certification. There are three certification options on Form 486, #11. In brief, these are:

A. My school or library has complied with the requirements of CIPA and NCIPA.
B. My school or library is "undertaking actions" to comply with requirements of CIPA and NCIPA.
C. CIPA and NCIPA do not apply because my school or library is receiving discounts only for telecommunications services.

Applicants must select the option that describes their state of compliance. For most applicants this will be either option A or C above. To prevent the loss of E-rate discounts, the Form 486 must be postmarked no later than

- 120 calendar days after the Service Start Date listed on your Form 486 or
- 120 calendar days after the date of the Funding Commitment Decision Letter whichever is later. Most applicants with services starting July 1 of the funding year must file the 486 generally by October 28 of the same funding year. Monitor the SLD Website for the exact 486 deadline date.

Undertaking actions, option B:

> *For Libraries:* Use of this option is covered in the FCC's July 24 Order. See the Order, especially paragraph 12, for details. In sum, during the 2003 E-rate year libraries covered by CIPA's filtering requirement must already be compliant with the law or be undertaking actions to be compliant by the start of services for the 2004 E-rate year. Undertaking actions can include various activities such as the library board directing staff to review filtering options and products, prepare a preliminary budget, develop a plan for implementation, etc. Be certain to document any activities taken in this area.
>
> *For Schools:* For most school applicants option B is no longer valid. The undertaking actions option is valid only the first time the school files for E-rate discounts (most often 2001) after passage of CIPA/NCIPA. This is known as the "first funding year" and is triggered when a Form 486 is filed for Internet or internal connections and the 486 has been processed by the SLD. Therefore, if your school filed a 486 for discounts on Internet or internal connections in 2001 or 2002, the "undertaking actions" does not apply for discounts in subsequent years. In such cases your school must now be in compliance with the law.

Certification for consortium applications:

> **Note:** Paragraph 13 of the FCC's July 24 Order has specific instructions on certification of library consortia, which include the need for library consortium members to file a newly revised Form 479 with the billed entity and the need for the billed entity to file the newly revised Form 486. Consult the Order for more details.

For schools and libraries that are part of a consortium application, the Form 486 certification is submitted to the SLD by the Billed Entity. This is usually the consortium itself which filed the Form 471. Each member of the consortium (the "administrative authorities") must complete Form 479 declaring compliance with CIPA. The 479 forms are not submitted to the SLD but are collected and kept on file by the Billed Entity. For consortium applications that are only for telecommunication services, no 479 forms are required. Under such circumstances the Billed Entity simply checks the CIPA "does not apply" box on Form 486, #11c. If a consortium application includes some applicants that are getting Internet discounts and some that are getting telecommunication discounts, then all applicants that are part of the consortium must file Form 479 with the Billed Entity. See the Form 486 instructions for more information on consortium applications.

The FCC has ruled that if any member of a consortium application is not in compliance with the law, only the non-complaint members shall be subject to reimbursement of their proportional share of E-rate discounts. The other compliant members can continue to receive discounts (FCC regulations, ¶27).

III. The Basic Requirements of CIPA and NCIPA

Q: What are the basic requirements of the law?

A: There are two basic requirements in the legislation. In brief they are:

1. A school or library must have some type of filter or blocking technology on all of its computers with Internet access. The filters must protect against access to certain visual depictions described in section III A below (CIPA requirement).
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 section III B below (NCIPA requirement).

III. A. CIPA: Technology Protection Measure, TPM (Filtering)

Q: What does the law mean by "technology protection measure" (TPM)?

A: The term "technology protection measure" appears throughout the law. The best way to define this is to review the actual text of the act itself which says, "The term 'technology protection measure' means a specific technology that blocks or filters Internet access to visual depictions" defined in the act. In this FAQ Technology Protection Measure and filter are used interchangeably. A TPM may include other options, besides commercial Internet blocking and filtering software. For example, newer versions of Netscape and IE have their own content rating or labeling systems integrated into the browser (Content Advisor in IE and NetWatch in Netscape). Whether such browser content rating systems meet the letter of the law is open to interpretation.

Q: What has to be filtered or subject to the TPM?

A: The law does not require the filtering of text. But the TPM must protect against access to visual depictions that are:

1. *Obscene:* This is defined in a reference to section 1460 of title 18, U.S. Code.
2. *Child pornography:* This is defined in a reference to section 2256 of title 18, U.S. Code.
3. *Harmful to minors:* This is applicable only to Internet access by minors. It is defined in CIPA and means any picture, image, graphic image file, or other visual depiction that:
   a. taken as a whole, appeals to a prurient interest in nudity, sex, or excretion;
   b. depicts, describes, or represents, in a patently offensive way, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
   c. taken as a whole, lacks serious literary, artistic, political, or scientific value.

In its April 2001 rules, the FCC declined to elaborate on the banned visual depictions beyond what is already stated in the law (FCC regulations, ¶48). In addition to sexually explicit content, most commercial filtering programs have a variety of categories by which they can filter, including Web content related to games, gambling, drug use, violence, etc. Whether a school or library filters any content besides the visual depictions defined in the law is a local decision. However, libraries that filter other content open themselves to potential legal challenges based on the blocking of constitutionally protected content.

> We decline to follow the suggestions of commenters to incorporate within our regulations layman's explanations of obscenity, child pornography, and the term "harmful to minors." We decline to amplify the statutory definitions.
> —FCC regulations, April 2001

The law, while defining the type of images that need to be blocked, does not specify any particular software (client) programs, such as a Web browser, email, or chat software which must come under the scrutiny of the TPM.

Q: What computers must have the Internet TPM?

A: The law states that a TPM that protects against access to the visual depictions referenced in the act must be on *any* of its computers with Internet access (CIPA section 1721 (a) (C)(i)). This includes student, staff, and patron computers accessed by minors or adults. The law makes no distinction between computers used only by staff and those accessible to the public. Therefore, even Internet connected computers located in administrative areas not accessible to the public or students must still have filters (FCC regulations, ¶30), but the TPM can be disabled. The FCC declined to make a specific filter exception for text-only terminals connected to the Internet. However, since such terminals cannot access the visual depictions outlawed by CIPA, this in itself probably constitutes compliance with the law (FCC regulations, ¶29). As described in the next question, a provision in the law allows the filter to be disabled under certain circumstances for adult Internet access.

> Under this statute, if a library attempts to provide Internet service for even *one* computer through an E-rate discount, that library must put filtering software on *all* of its computers with Internet access.
> —Justice Stevens' dissent.

Patron PCs: An increasingly popular option in libraries is to allow patron owned laptops to access the Internet through the library's wireline or wireless network. CIPA references the need for the library to have a TPM in place, "with respect to any of *its* computers with Internet access [emphasis

added]." It is very reasonable to assume that "its" refers to the library's PCs and that patron laptops need not be filtered. Officials at a federal agency have indicated, off the record, that they agree with this assumption.

The FCC has also stated that a school or library cannot prorate its E-rate discount to allow some computers to be unfiltered. For example, a library cannot say it will take only 50% of its authorized E-rate Internet discount and then leave 50% of its computers unfiltered.

Q: Under what circumstances or conditions can the TPM be disabled?

A: The law states that any authorized school or library staff may disable the TPM to allow adults to have unrestricted Internet access for any lawful purpose (CIPA section 1721 (6) (D)). Such staff authorization is granted by the school or library's governing body. The disabling language for the E-rate is applicable to adults only (age 17 or older). Note: Even without CIPA, there is no constitutional protection for anyone to view obscene images, and child pornography, regardless of its medium, is clearly illegal.

The FCC in its April 2001 regulations stated that the method or procedures used to disable the TPM for adults is a matter of local school or library policy. The law provides no guidance in this area, and the FCC declined to provide any further clarification. Thus staff have considerable flexibility on how to implement the disabling provision. The Supreme Court's ruling notes "the ease with which patrons may have the filtering software disabled." However, frequent requests for disabling can be time consuming for staff to administer, and may be technologically difficult and costly to implement. The FCC regulations say that if there are concerns about "costs associated with maintaining filtering or blocking systems that may frequently be disabled" then libraries should take the cost considerations into account when evaluating any technology protection measures (FCC regulations, ¶30).

FCC rules should allow a library to offer unfiltered access for adults without their always asking staff to turn off the filters. Requiring this is likely to have a chilling effect on adults' Internet use and is cumbersome to administer.
—Wis Dept of Public Instruction, Comments to FCC, Feb. 2001.

Federally-imposed rules directing school and library staff when to disable technology protection measures would likely be overbroad and imprecise, potentially chilling speech. We leave such determinations to the local communities.
—FCC regulations, April 2001.

The Supreme Court's plurality opinion and the concurring opinions of Justices Kennedy and Breyer place considerable emphasis on CIPA's unblocking option. The optional "may disable" language in the law has on taken on a "must disable" interpretation by the Court's ruling. For example, Justice Kennedy's concurring opinion indicates that if a patron requests unfiltered access to view constitutionally protected Internet material, and the library (1) refuses such a request, (2) does not have the technical ability to grant such a request, or (3) places some other undue burden on the patron, then the library places itself at risk of an "as-applied" challenge by the patron. "As-applied" meaning that as the library has applied CIPA's filtering mandate, the patron contends it is unconstitutionally blocking access to legal content. (See also the question, "What are the legal implications…?")

The law does not address the issue of requiring patrons to state why they are seeking unfiltered Internet access or the type of information they are seeking. (Of interest, there is no language in CIPA that states patrons need to ask staff to disable the filter.) During the Supreme Court's oral argument, the Solicitor General stated that a patron does "not have to explain any reason why he was asking a site to be unblocked or the filtering to be disabled." This phrasing is quoted in the Court's plurality decision. Thus there is considerable legal support that says patrons simply have to

request unfiltered access to legal content on the Internet, with no explanation needed. Considering this, a library policy of having staff ask patrons why they want unfiltered access is very questionable from the Court's perspective and, in addition, such questions raise obvious issues of privacy and confidentiality. A library's AUP should address the issue of what constitutes a patron's acceptable or unacceptable use of the Internet without the need for intrusive staff interference.

Staff workstations: Since authorized staff can disable the TPM for adult patrons, it should be easy to craft a policy to allow adult staff to turn off the TPM for their own use. Unlike a patron request for unfiltered access, which is based on the First Amendment, a staff request for unfiltered access is more of a management or board decision.

Passive disabling: This is defined as establishing polices or taking measures so that staff need not be constantly taking time disabling and re-enabling the filter, and patrons need not be constantly asking staff to disable the filter. The FCC's latitude given to libraries (and schools) on disabling has generated considerable discussion on this issue. For example, one scenario is to have a TPM on workstations but have the patron select unfiltered access by choosing this option on the screen, entering a password, or by use of a smart card process. To provide practical guidance in this area, but not a formal legal opinion, an attorney retained by ALA indicated that such a scenario could be reasonably argued to comport with the law. This assumes that the library makes a good faith effort to enforce a policy that only adults can select the unfiltered option and use the unfiltered PCs. Examples of further safeguards could include signage indicating "adult only" workstations, and the library has the patron sign an AUP which states that he/she wants unfiltered access. In this scenario there is no direct intervention by staff, and adult patrons do not need to request staff to disable the filter.

The procedure for disabling the TPM is a decision to be made by each library in close consultation with the board and legal counsel as needed. And considering the importance that the Court has placed on disabling, this should be a key factor in any filter evaluation.

Q: How effective does the TPM have to be? Is there any type of TPM effectiveness certification?

A: It is important to note that the law states that the TPM must *protect* against visual depictions outlawed by the legislation. The TPM does not have to *prevent* access to all such depictions. (No TPM is 100% effective in preventing all such access.) In developing its CIPA regulations, the FCC declined to further define the filter requirements or to adopt any type of definition or certification on how effective a filter must be, beyond the very general "protect" language of the law. Thus, there is no such thing as an FCC certified TPM or a CIPA certified TPM. And, considering the broad interpretation of the word "protect," any statements by vendors that their filtering software will help schools and libraries be CIPA compliant are of limited value.

> Some commenters have requested we require entities to certify to the effectiveness of their technology protection measures. Adding an effectiveness standard does not comport with our goal of minimizing the burden we place on schools and libraries. Therefore, we will not adopt an effectiveness certification requirement.
> —FCC regulations, April 2001

The FCC regulations do not require schools or libraries to track the number of attempts made to access prohibited visual depictions or the number of times the TPM succeeds or fails. The regulations also do not require schools or libraries to collect any complaints filed by staff, students, or the public on what was or was not blocked (FCC regulations, ¶42). The school or library's Internet policy may indicate that it will track and collect such statistics, but there is no mandate to

do this in the law or regulations. (During the open public comment period before release of its regulations in April 2001, some organizations requested the FCC to mandate such tracking and compiling of complaints.)

Q: What are the legal implications if the TPM fails and allows banned images to appear on the screen?

A: The FCC presumes that Congress did not intend to penalize schools or libraries that act in good faith and in a reasonable manner to implement filters. The FCC also notes that failure to comply with the law's requirements "could also engender concern among library patrons and parents of students at the school. We believe that schools and libraries will act appropriately in order to avoid such outcomes." (FCC regulations, ¶47) In other words, the FCC will rely, in part, on community "concern" to serve as one mechanism to enforce compliance.

There may still be instances in which a patron claims that too many allegedly obscene images are getting through the TPM. A library *must have* policies and procedures in place if it is to address any such complaints expeditiously. It is possible that a patron could initiate a complaint with the FCC that would prompt an investigation. Under CIPA, the FCC can require a library to reimburse its E-rate discounts for any period of time it was out of compliance. However, the FCC has stated that it is not in a position to make a legal determination that an image is obscene. This can only be done as part of a formal court procedure following legal standards, such as those established by the Supreme Court in Miller v. California. To reemphasize: Having a library policy to address complaints can help minimize any possibility of more formal legal action.

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 (ISP) or at the server level on the school or library's LAN or WAN, or the filter can be individually installed on each PC workstation. Installing filtering software on each individual PC works best with a very limited number of PCs. The option to filter at the ISP level or some point on the LAN/WAN is more efficient when filtering a large numbers of workstations, but you may then have a limited ability to customize settings for each workstation. In addition, it may be more difficult to disable the filter on individual PCs when requested by adults. The technical and staff processes and procedures needed to disable the filter or unblock sites should be a key issue when evaluating filters.

III. B. Internet Safety Policy and Public Meeting (NCIPA)

NCIPA's requirements apply only when getting E-rate discounts for services referenced under CIPA. NCIPA does not apply when using just LSTA or ESEA funds for purposes referenced in CIPA.

> **Note:** Assuming 2003 and any subsequent year is not the library or schools first E-rate year in reference to NCIPA (see *undertaking actions* paragraph above) your school or library must already have an Internet Safety Policy that meets the requirements of the law and must have already held a public meeting on the policy.

Q: Can we use our current Internet safety policy as the CIPA/NCIPA Internet safety policy?

A: You can use your current Internet policy if it meets all the requirements stated in the legislation. If, after reviewing your policy, you determine that it does not meet the law's requirements, then you will have to initiate a process to revise it so that it is in compliance.

Q: What must be included in our policy to be in compliance with the law?

A: The CIPA section of the law says that a school or library must have an Internet safety policy and this policy must include the use of filters to protect against access to the visual depictions outlawed in the act. The school's Internet policy must also indicate how it plans to monitor the Internet activities of minors. The law does not require this monitoring provision in the public library's policy. Note: Neither the law nor the FCC rules require the actual online tracking of Internet use by minors or adults.

The NCIPA section of the law is much more specific in its safety policy requirements. NCIPA requires that schools and libraries participating in the E-Rate program adopt and implement an Internet safety policy that addresses

1. Access by minors to inappropriate matter on the Internet and the Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors' access to materials harmful to minors.

The Internet Safety Policy must be adopted after holding at least one public hearing or meeting as described below.

Q: One of the requirements refers to access by minors to "inappropriate matter" and another refers to access to "materials harmful" to minors. What's the difference?

A: The term "harmful to minors" is defined in CIPA as cited above. The definition of "inappropriate for minors" is to be made by the school or library board or administration. The law states that the federal government is not to make any determination on what is or is not "inappropriate for minors." CIPA defines a minor as any person less than 17 years of age.

Q: Does the Internet Safety Policy have to be adopted by the school or library board, or can it be done as an administrative procedure?

A: The law says the "school or library" shall adopt and implement a policy that meets the requirements of the law. Though the law does not state specifically that the board must pass the policy, it is prudent to have your board take such action.

Q: Can a regular meeting of the school or library board be used as the required public meeting?

A: The law and the regulations give schools and libraries considerable flexibility in meeting the public hearing mandate. The law says simply that schools or libraries must "provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy." Considering this general language, the hearing can be part of a regular board meeting, assuming such a meeting allows for public comments. Notices of such a meeting must comport with any local or state open meeting laws. Be certain to document fully the public meeting by keeping a copy of the notice, noting any actions taken, etc.

IV. Sources for More Information

> **Note:** See the Web version (http://www.dpi.state.wi.us/dltcl/pld/cipafaq.html) for a more detailed list.

1) The law, court decisions and related legal papers.

Children's Internet Protection Act (CIPA) (http://www.fcc.gov/wcb/universal_service/chipact.doc)

- The text of the legislation, both CIPA and NCIPA.

FCC April 2001 CIPA Regulations (http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc)

- These are the FCC's regulations released April, 2001. The regulations outline the specific actions schools and libraries must take to comply with CIPA and NCIPA.

FCC July 2003 CIPA Regulations for Libraries (http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-188A1.doc)

- These are the FCC's regulations specifically related to the timeframe for library compliance with the Supreme Court's ruling on CIPA's filtering mandate.

SLD CIPA and Form 486 Frequently Asked Questions
(http://www.sl.universalservice.org/reference/CIPAfaq.asp)

- A good, detailed FAQ on the key relationship of CIPA to the E-rate's Form 486.

Supreme Court Decision (http://www.supremecourtus.gov/opinions/02pdf/02-361.pdf)

- The text of the Court's June 23, 2003 decision.

CIPA Challenge Documents (http://archive.aclu.org/features/f032001a.html)

- Extensive repository from the ACLU with links to many documents related to the legal challenge to CIPA.

2) Resources on CIPA, filters, and related issues.

ALA CIPA Site (http://www.ala.org/cipa)

Good site with the latest legal and regulatory information, etc. See also the memo on filter disabling options at http://www.ala.org/ala/washoff/WOissues/civilliberties/washcipa/qanda/q.htm which outlines several possible scenarios that involve take minimal staff involvement.

Coping with CIPA: A Censorware Special (http://cites.boisestate.edu/civ3i9.pdf)

- A special CIPA issue of Walt Crawford's Cites and Insights. A very good review with many quotes from newspaper editorials and perspectives, both supporting and opposing the Court's decision.

CIPA Update (http://www.infopeople.org/training/webcasts/handouts/2003/7-17-03_handout_files/CIPAsent.pdf)

- This is the handout used as part of a July 2003 CIPA update from Mary Minow. It provides a good overview of the law and the Court's decision.

Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries (http://e-ratecentral.com/CIPA/cipa_policy_primer.pdf)

- In addition to a review of the act, this paper contains Internet Safety Policy guidelines and a sample compliant Internet Safety Policy. From E-rate Central.

Analysis of the CIPA Decision

- FindLaw columnist, attorney, and author Julie Hilden argues the recent CIPA Court decision is less destructive to free speech rights than it seems.

ALA Libraries & the Internet Toolkit (http://www.ala.org/ala/oif/iftoolkits/litoolkit/librariesinternet.htm)

- A good variety of background papers, policies, FAQs, etc., to help librarians manage and communicate about the Internet.

Plain Facts About Internet Filtering Software.
(http://www.ala.org/ala/pla/plapubs/technotes/internetfiltering.htm)

- Provides a good overview of how filters work, a filter check list and a good bibliography. (This is a PLA Tech Note authored by Karen G. Schneider.)

Loudoun County (VA) Library Internet Filters Case Summary
(http://www.eff.org/Legal/Cases/Loudoun_library/)

- This was the first legal challenge to filters in libraries to reach the federal courts.