

CIPA QUESTIONS AND ANSWERS

JULY 16, 2003

Contents of Q&A:

- I. CIPA in General
- II. Applicability and Scope
- III. “Technology Protection Measure”; Disabling
- IV. Certification and Enforcement
- V. Timing of Certification and Enforcement

I. In General.

Q: *Three agencies – the Federal Communications Commission (FCC), the Department of Education (D. of Ed.), and the Institute of Museum and Library Services (IMLS) – have responsibilities under this new law. Will my library need to make multiple certifications to multiple agencies?*

A: No. Covered libraries are required to file only one certification with one agency to avoid conflicting or duplicative requirements, among the three federal agencies involved.

- Every library receiving E-rate discounts for Internet access, Internet service, or internal connections must comply with the new amendments to section 254 of the Communications Act (as added by sections 1721 and 1732 of the new statute) and certify compliance with Children’s Internet Protection Act to the FCC. That is the only agency to which these entities are responsible, even if they receive Elementary and Secondary Education Act (ESEA) title III or Library Services and Technology Act (LSTA) (state grants) funds.
- School libraries receiving ESEA title III funds for computers or accessing the Internet, but *no* E-rate discounts, must provide their certification to the Department of Education.
- Libraries receiving LSTA state grant funds for computers or accessing the Internet, but *no* E-rate discounts, must provide their certification under Museum and Library Services Act.

Q: *Do CIPA and the Neighborhood Act cover the same ground? What is the relationship between the two different “acts”?*

A: CIPA and the Neighborhood Act cover different ground and are not in conflict. Both acts comprising the new law set forth requirements concerning the "protection" of minors from certain materials.

The CIPA requires the filtering or blocking of certain visual depictions and requires libraries to adopt and implement an Internet safety policy and operate "technology protection measures" (blocking and filtering) if they receive--

- E-rate discounts for Internet access, Internet service, or internal connections;
- Funds under title III of ESEA to purchase computers used to access the Internet or to pay the direct costs associated with accessing the Internet; or
- Funds under the state grant programs of LSTA to purchase computers used to access the Internet or to pay the direct costs associated with accessing the Internet

The Neighborhood Act covers a broader range of content and certain prohibited activities, pertains to the universal service discounts only, and requires libraries to adopt and implement an Internet safety policy – essentially an "acceptable use" policy – addressing various specific issues and to do so with local participation. One of a number of elements of the Internet safety policy is the use of blocking or filtering technology (referred to in the legislation as a "technology protection measure." (The specific requirements relating to blocking or filtering technology and the timing and procedures for certifying their use are contained in the CIPA.)

II. Applicability and Scope.

Q: *Does the new law apply to academic or college libraries?*

A: No. Academic and college libraries are not covered under the E-rate provisions because they are not eligible for E-rate discounts and they are not covered under the LSTA provisions because those sections apply only to public libraries and libraries in public elementary and secondary schools.

Q: *Does CIPA apply to my library?*

A: CIPA applies to public libraries that receive—

- E-rate discounts for Internet access, Internet service, or internal connections;
- Funds under title III of ESEA to purchase computers used to access the Internet or to pay the direct costs associated with accessing the Internet; or

- Funds under the state grant programs of LSTA to purchase computers used to access the Internet or to pay the direct costs associated with accessing the Internet.

All public libraries covered by virtue of their use of E-rate discounts for Internet access, Internet service, or internal connections must certify compliance to the Federal Communications Commission. School libraries covered through use of title III funds certify to the Department of Education; public libraries covered through use of LSTA state grant funds certify to IMLS. (See also the discussion on Certification below.)

Q: *My library does not receive E-rate discounts. Will CIPA (or the Neighborhood Act) apply if we receive an LSTA grant that is for activities other than purchasing computers for accessing the Internet or for other Internet access costs?*

A: No, the requirements of CIPA are specifically tied to use of LSTA funds “to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet.” If no LSTA funds are received by the library, or if those received are used for purposes other than those quoted, then CIPA simply does not apply. (The Neighborhood Act applies only to E-rate recipients.)

Q: *Does the new law apply to libraries that do not have children’s collections or programs, or one located in a retirement community? What about Braille and Talking Book Libraries for blind children – are they covered?*

A: Yes, in each instance. Under the plain language of the statute, libraries must have safety policies that include the operation of blocking or filtering technology “with respect to any . . . computers with Internet access that protects against [even theoretical] access through such computers to visual depictions that are . . . obscene,” etc. The statute requires that libraries receiving E-rate discounts or LSTA or ESEA funds for computers or Internet access adopt a policy for minors *and* adults that includes blocking or filtering technology, even if minors are unlikely to use their computers.

Q: *Will the required use of blocking or filtering technology apply where computers were purchased in the past with ESEA or LSTA funds, but such funds are not being used for Internet access and no E-rate discount is being received by the school or library?*

A: No. While Congress might have applied the requirements of CIPA to attempt to require that any computer purchased with federal funds in the past must be subject to use of blocking or filtering technology, it did not do so. The law states that “no funds . . . may be used to *purchase* computers used to access the Internet, or to pay for direct costs associated with accessing the Internet . . .” unless the safety policy is in place and certification is made [emphasis added].

III. “Technology Protection Measure”; Disabling.

Q: *What is a “technology protection measure”?*

A: The law defines a “technology protection measure” as “a specific technology that blocks or filters Internet access to visual depictions that are—(A) obscene . . .; (B) child pornography . . .; or (C) harmful to minors . . .” Although the law clearly requires the use of filtering or blocking technology, it does not require the use of specific filtering software or services. Instead, CIPA requires schools or libraries covered by the new requirements to certify that they are using technology that blocks or filters access to visual depictions of the type specified in the legislation.

Q: *The new law appears to require only use of technology protection measures that block or filter Internet access to “visual depictions”; does that mean that I do not need to take steps to block or filter text, whatever the content?*

A: Yes. CIPA requires only that covered libraries block or filter “Internet access to visual depictions . . .” Therefore, the blocking or filtering technology need not affect text, whatever the content, and setting a browser to “text only” would satisfy this requirement.

Q: *What kind of “visual depictions” must be blocked or filtered?*

A: For adults, the recipient of funds must block or filter access to visual depictions that are obscene (as defined by the federal obscenity statute, 18 U.S.C. § 1460 et seq.) and child pornography (as defined by 18 U.S.C. § 2256). For minors, the recipient of funds must block or filter visual depictions that are obscene and child pornography, as well as visual depictions that are “harmful to minors.”

Q: *What is “obscenity”?*

A: The federal obscenity statute cited in CIPA does not itself contain an express definition of obscenity. However, the Supreme Court (in *Miller v. California*, 413 U.S. 15 (1973)) has established a test for obscenity that is now implicitly incorporated into the federal statute:

- (a) Whether “the average person, applying contemporary community standards,” would find that the material, taken as a whole, appeals to the prurient interest;
- (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state or federal law to be obscene; and
- (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Q: *What is “child pornography”?*

A: The federal child pornography statute, 18 U.S.C. § 2256, defines “child pornography” as “any visual depiction” of a minor under 18 years old engaging in “sexually explicit conduct,”

which includes “actual or simulated” sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or “lascivious exhibition of the genitals or pubic area.” The statute’s definition includes not only actual depictions of sexually explicit conduct involving minors, but also images that “appear to be” minors engaging in sexually explicit conduct.

Q: *What is “harmful to minors”?*

A: The act defines “harmful to minors” as “any picture, image, graphic image file, or other visual depiction that—

“(A) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

“(B) depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, 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 as to minors.”

Q: *What is a “minor”?*

A: The act defines “minor” as an individual who has not attained the age of 17.

Q: *Is there blocking or filtering technology available that actually filters or blocks access to obscenity, child pornography, and material harmful to minors without also restricting access to constitutionally protected speech falling outside these defined terms?*

A: No. At this time we are aware of no filtering technology that will block out all illegal content, but allow access to constitutionally protected materials.

IV. Certification and Enforcement.

Q: *What kind of “certification” will be required by the FCC, D. of Ed., and IMLS?*

A: CIPA requires annual certification of compliance with the statute’s requirements that the covered library has in place the required Internet safety policy, which includes the operation of blocking or filtering technology, and is enforcing the operation of that technology during use of its computers.

Q: *To which agency will libraries be required to make this certification?*

A: Certification must be made only to one agency, depending on the category into which each covered library falls:

- Every public library receiving E-rate discounts for Internet access, Internet service, or internal connections must certify compliance with CIPA to the FCC. That is the only agency to which these entities are responsible, even if they receive ESEA (title III) or LSTA (state grants) funds.
- School libraries receiving ESEA title III funds for computers or accessing the Internet, but *no* E-rate discounts, must provide their certification to the Department of Education.
- Libraries receiving LSTA state grant funds for computers or accessing the Internet, but *no* E-rate discounts, must provide their certification under Museum and Library Services.

A detailed specification of CIPA’s certification requirements follows:

Institution & Type of Support	Applicable CIPA Requirements
Library receives E-Rate support <i>only</i>	Comply with E-Rate provisions <i>only</i>
Library receives LSTA support <i>only</i>	Comply with LSTA provisions <i>only</i>
Library receives <i>both</i> E-Rate <i>and</i> LSTA support	Comply with E-Rate provisions <i>only</i>
Library receives <i>no support</i> from E-Rate or LSTA	No requirements under CIPA

Q: *Who makes the certification if the library that ultimately receives the funds or E-rate discount is not the “applicant,” as is the case where there are state agencies or consortia who apply for the funds from the federal agencies and pass them on to other entities?*

A: We do not know the answer at this time.

V. Timing of Certification and Enforcement.

Q: *If a library certifies that it is in compliance, how would the responsible agency determine otherwise?*

A: If the library has in place an Internet safety policy that involves use of any blocking or filtering technology, and if it certifies that it is enforcing the operation of that technology, then noncompliance could be determined if the responsible agency receives a complaint and through investigation concludes that the certification was inaccurate or false. Otherwise, the failure to certify would constitute the most likely ground for noncompliance.

Q: *Can my library be sued to challenge noncompliance with CIPA or otherwise to enforce the statute's new requirements?*

A: While this issue is not entirely free from doubt, it is the conclusion of ALA's counsel that only a responsible government agency can enforce the statute as specified in the statute itself, and that CIPA authorizes no private right of action against a library for failure to comply.