CHILDREN'S INTERNET PROTECTION:
AN ANALYSIS

Prepared by Legal Counsel for the American Library Association

Under a new federal law, passed as part of the Omnibus Consolidated Appropriations legislation at the end of the last Congress (Public Law 106-554), libraries and schools that take advantage of E-rate discounts for Internet access or receive certain funding under the Library Services and Technology Act or the Elementary and Secondary Education Act will have to adopt an Internet safety policy that incorporates use of filtering software on computers with Internet access.

Requirements for E-rate Recipients

The CIPA and Neighborhood Act both establish requirements for E-rate recipients. The Federal Communications Commission is required by these acts to develop regulations; Notice of Proposed Rulemaking was released by the FCC January 23 and is likely to be published January 2001. Comments (and reply comments) are being solicited; a final rule will be issued before April 20, 2001. [1]

1. Internet Safety Policy

Every school and library that receives E-rate discounts for Internet access, Internet service, or internal connections must develop an Internet safety policy that meets a number of specific requirements that are spelled out below. Those libraries and schools that receive E-rate support only for non-Internet-related "telecommunications services" - services that fall outside the terms "Internet access, Internet service, or internal connections - do not need to comply with CIPA or the Neighborhood Act if they do not receive funding under ESEA title III or MSLA state grants.

The deadline by which a library or school must meet these requirements is unclear. Portions of the statute suggest a deadline as early as April 20, 2001[2], while other portions suggest that certification of compliance is not required until October 28, 2001[3]. The FCC has indicated an intent to harmonize certification deadlines within CIPA and the Neighborhood Act. *It appears as if the FCC's proposed rule will require certification of compliance with the law by October 28, 2001*,

---

[1] CIPA sec. 1733 requires the FCC to prescribe regulations for CIPA and shall ensure that the regulations take effect "120 days after the date of enactment." CIPA was signed by the President on December 21, 2000. The Neighborhood Act sec. 1732(4) prescribes the same deadline for FCC regulations implementing that act. However, section 1732(3) of the Neighborhood Act states that the
Neighborhood Act "shall apply with respect to schools and libraries" developing Internet safety policies "on or after the date that is 120 days after the date of enactment" of CIPA. This means that it is theoretically possible that the FCC rulemaking process could result in deadline for compliance with the Neighborhood Act's Internet safety policy requirements that is earlier than CIPA's deadline for utilizing blocking or filtering technology. That result is not likely to occur, in practice, since the statute says that the Neighborhood Act may be complied with "on or after" 120 days, and the Commission's NPRM makes no suggestion that there will be two separate compliance deadlines.

[2] Neighborhood Act 47 U.S.C sec. 254 (l)(4) added by N-CIPA sec. 1732 reads, "This subsection shall apply with respect to libraries and schools on or after the date that is 120 days after the enactment of CIPA." (April 20, 2001)

[3] 47 U.S.C. sec. 254(h)(5)(E)(i)(I) as added by CIPA sec. 1721(a) and 47 U.S.C. sec 254(h)1721(b)(6)(E)(i)(I) as added by CIPA sec. 1721(a) indicate that in general, during the first program year in which CIPA applies, E-rate recipients must certify compliance "not later than 120 days after the beginning of such program funding year" (October 28, 2001)

for libraries and schools receiving E-rate support during program year four. Libraries and schools that do not yet have the required type of Internet safety policy in place may certify that they are taking steps to have the policy in place by the next program year.

The FCC has suggested that it intends to make compliance with the Children's Internet Protection acts minimally burdensome, meaning that it is unlikely that the FCC will request specific details about Internet safety policies. (Under the Neighborhood Act, the Internet safety policy must be made available to the Commission for review, upon request.) It is thus possible that the FCC will adopt a check-off certification on Form 486, the "Receipt of Service Confirmation Form,"[4] although verification of this conclusion must await the final FCC regulations.

2. Requirements of the Internet Safety Policy

The new law includes both procedural and substantive requirements for the Internet safety policy, although it does not prescribe any specific form or format. The procedural requirements focus on public notice and a public meeting or hearing. The substantive requirements address Internet content and "unacceptable" activities minors might engage in online.

Many libraries and schools already have policies addressing some or all of the issues required to be addressed in an Internet safety policy under this new statute. *If current Internet policies do not meet both the procedural and substantive requirements of the new law, they will need to be revised.* It is possible that even existing acceptable use policies that conform to the requirements of the new law must be reconsidered, since the Neighborhood Act liberally requires that libraries and schools "shall adopt" a policy and that the "proposed" policy be subject to public notice and a meeting or hearing. FCC rules may clarify this issue.

guidance; otherwise, libraries should consult their counsel before deciding how to proceed with a public notice and hearing.[7]

b. Substantive Requirements of the Internet Safety Policy

The Neighborhood Act specifies the topics that must be addressed in the Internet safety policy *other than Internet filtering, which is addressed in CIPA*. Libraries and schools receiving E-rate discounts for Internet access, Internet service, or internal connections must "adopt and implement" a policy that addresses all of the following issues

While the definition of "inappropriate matter" is thus left to local communities, institutions should proceed carefully. School and library policymakers should involve their legal counsel in the drafting of any definitions or policies aimed at limiting access to materials on the Internet, in order to avoid running afoul of the First Amendment. Since the policies must also address "materials harmful to minors" (see below), the term "inappropriate matter" appears to anticipate limiting access to material that may nonetheless be constitutionally protected as to minors.

Access to "Materials Harmful to Minors": In their Internet safety policies required by the Neighborhood Act, libraries and schools must address "measures designed to restrict minors' access to materials harmful to minors." Because the filtering or blocking of material harmful to minors by the use of blocking or filtering technology is addressed in detail in the CIPA, this requirement possibly suggests that libraries and schools must implement *other measures beyond Internet filtering or blocking* to limit minors' access to material harmful to minors, although it may be argued that the same term used in two places under the bill's title of Children's Internet Protection should be read as meaning the same in both places. The law provides no guidance on what those measures are - if not the technology protection measures used under CIPA - implicitly leaving any determination to the local authority.

"Harmful to minors" is defined in CIPA (which is specifically limited in its application to the required blocking or filtering of "visual depictions") as:

> Any picture, image, graphic image file, or other visual depiction that--
>
> (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
>
> (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suit able 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
>
> (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.[9]

Libraries and schools should consult their counsel before they attempt to implement this provision. Many

service, or internal connections are *not* required to comply with these requirements unless they are recipients of ESEA title III funds or LSTA state grant monies.

CIPA uses the phrase "technology protection measures" throughout the legislation and defines "technology protection measure" as "a specific technology that *blocks or filters Internet access* to" specified material.[10]

a. Whose Access Must Be Filtered?

i. General Rule

All Internet access must be filtered, whether minors (under 17) or adults are using the computer, and regardless of how many computers with Internet access the library or school provides. However, CIPA's requirements for what must be filtered are more restrictive for minors than adults, so libraries and schools may choose to implement different settings for the filters depending on whether adults or minors are using the computer.

When minors are using the Internet, access to visual depictions that are any of the following must be blocked or filtered:

- obscene; [11]
- child pornography; [12] or
- harmful to minors. [13]

---

[10] CIPA sec. 1703(b)(1) and 47 U.S.C. sec 254(h)(c)(I) as added by CIPA sec. 1721(a). The definitions are not identical. Sec. 1703(b)(1) defines "technology protection measure" as "a specific technology that blocks or filters Internet access to visual depictions that are" obscene, child pornography, or harmful to minors. 47 U.S.C. sec 254(h)(c)(I) as added by CIPA sec. 1721(a) defines "technology protection measure" as "a specific technology that blocks or filters Internet access to the material covered by a certification" made to the FCC as required by CIPA.

[11] CIPA indicates that the term obscene is defined in 18 U.S.C. 1460. However, no definition appears in that section. A definition of obscenity was set out in the landmark case Miller v. California, 413 U.S. 15 (1973), as a three-part test: (1) Whether the average person, applying contemporary community standards, would find the work (taken as a whole) appeals to the "prurient" interest; (2) whether the work depicts sexual conduct in a patently offensive way; and (3) whether the work (taken as a whole) lacks serious literary, artistic, political, or scientific value. This test is generally applied by courts in evaluating whether material is obscene.

[12] CIPA refers to the definition of child pornography set forth in 18 U.S.C. 2256:
"child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where--

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
(B) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;
(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or
(D) such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

[13] Defined and discussed above.

However, when adults are using the Internet, only material that is obscene or child pornography must be filtered or blocked.

The requirement that a TPM limit access to content that meets specific legal standards presents special concern, since no commercially available filtering or blocking technology or services can do so with precision. Libraries and schools will have to work with counsel to determine what choices, within the filtering products available, best meet the standards of their community.

ii. Exception to the General Rule: Disabling for "Bona Fide Research"

The E-rate program explicitly permits an institution to "disable the technology protection measure concerned, during use by an *adult*, to enable access for bona fide research or other lawful purpose." (Emphasis added.) The law provides no definition of this phrase.

This is one of the areas in which the restrictions on E-rate funding differ from the those imposed on title III or LSTA funding. The title III and LSTA funding restrictions also permit institutions to "disable a technology protection measure under paragraph (1) to enable access for bona fide research or other lawful purposes," but *do not limit that exception to adults*. Because the title III and LSTA portions of CIPA only apply to institutions that are not covered by the E-rate provisions, an institution receiving funding through multiple sources covered by CIPA must comply with the more restrictive E-rate standards.

There are no exceptions to the CIPA E-rate requirement that Internet access be filtered at all times rule for minors. When adults use computers in libraries and schools subject to CIPA's E-rate provisions, a librarian or administrator may disable the filtering software "to enable access for bona fide research or other lawful purposes."

b. Paying for Filtering Technology

E-rate funding is not available to pay for Internet filtering software. However, funds available under section 3134, part A of title VI of ESEA, or section 231 of LSTA may be used for the purchase or acquisition of the "technology protection measures" required by CIPA.[14]

c. E-rate Filtering Deadlines

The deadlines that libraries and schools must meet to comply with CIPA are confusing, conflicting, and vague. Those deadlines applicable to the E-rate program will be clarified as part of the FCC rulemaking.

Currently, E-rate funding applications are being accepted for Program Year 4, which begins on July 1, 2001. It appears as if the FCC will consider Program Year 4 to be "the first program funding year . . . following [the] effective date" of CIPA. CIPA recognizes that local procurement rules may not conform with the certification requirements of CIPA and thus allows for certification that a library or school is "undertaking such actions, including any necessary

---

[14] 47 U.S.C. sec. 254(h)(g)(1) as added by CIPA sec. 1721(a).

procurement procedures, to put in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification"[15] during the first program funding year. Specifically, the filtering requirements in CIPA appear to establish the following deadlines; these will be further clarified in the FCC rulemaking:

* April 20, 2001: 120 days after the enactment of CIPA. This is the deadline by which the FCC "shall prescribe regulations" to implement CIPA.[16]
* July 1, 2001: Beginning of E-rate Program Year 4 and first program funding year in which the CIPA fil tering mandate applies.
* October 28, 2001: 120 days following the beginning of the first program funding year in which the CIPA filtering mandate applies. This will be the deadline for certification that a library or school is filtering pursuant to the requirements of CIPA, or is in the process of becoming compliant, including procuring filtering software or services.
* July 1, 2002: Beginning of E-rate Program Year 5 and second program funding year in which the CIPA filtering mandate applies. Waivers are possible during this program year for institutions that are engaged in procuring Internet filtering, but, because of local procurement procedures, have not yet been able to implement filtering.
* July 1, 2003: Beginning of E-rate Program Year 6 and third program funding year in which the CIPA filtering mandate applies. Waivers are no longer possible during this program year.

d. Certification Options During the First Three Program Years

i. E-rate Program Year 4/CIPA First Year:

At whatever deadline the FCC determines to be the certification deadline (most likely October 28, 2001) libraries and schools must certify that they are either:

· Already filtering or blocking obscene material, child pornography

CIPA third year.

iii. E-rate Program Year 6/CIPA Third Year:

As part of the application process for E-rate funding during Program Year 6 (approximately two year from now), libraries and schools must certify that they are filtering or blocking obscene material, child pornography, and material that is harmful to minors.

Waivers will no longer be available beginning with E-rate Program Year 6. Libraries and schools that do not comply with CIPA will no longer be eligible for E-rate discounts.

e. Penalties for Noncompliance

Failure to Submit Certification. Any library or school that fails to submit the certification requirements described above shall be ineligible for funding under the E-rate program.[17]

Failure to Comply with Certification. Any library or school that "knowingly fails to ensure the use of its computers"[18] in compliance with these requirements not only loses eligibility for funding, but must reimburse the E-rate fund for discounts received during the period covered by such certification.
Additionally other laws, including criminal laws, provide serious penalties for providing false statements to the federal government.

f. Remedies

Libraries and schools that lose funding eligibility because of failure to certify or to comply with certification can regain eligibility for E-rate funding if they become compliant with CIPA requirements and certify to the FCC that they have done so.

Requirements Under the Elementary and Secondary Education Act of 1965 and Under the Museum and Library Services Act

The CIPA requirements for institutions receiving ESEA title III funds and LSTA funding are substantially similar, and implementing each raises similar challenges. (It should be kept in mind that the Neighborhood Act's requirement for a broad Internet safety policy - addressing, among other things, safety and security of minors when using email, unlawful activities by minors, and personal privacy of minors on the Internet - does not apply to libraries and schools that do not receive E-rate or do not use E-rate discounts for Internet access, Internet service, or internal connections. Thus, only CIPA's requirements relating to the use of blocking or filtering technology applies to these institutions, which are covered by virtue of their receipt of title

---

17 47 U.S.C. sec. 254(h)(6)(F)(i) as added by CIPA sec. 1721(a).

18 47 U.S.C. sec. 254(h)(6)(F)(ii) as added by CIPA sec. 1721(a).

III or LSTA funds that are used for computer purchases or Internet access.)

The CIPA requirements are slightly different for institutions that only receive ESEA or LSTA funding, but do not participate in the applicable portions of the E-rate program. This section analyzes the CIPA requirements that apply to libraries and schools that receive ESEA or LSTA funds for computers used to access the Internet, or to pay for direct costs associated with accessing the Internet, but that do not participate in the E-rate program.[19]

1. Internet Filtering Requirements

The general filtering requirements on funding under title III of ESEA and LSTA, for "computers used to access the Internet, or to pay for the direct costs associated with accessing the Internet,"[20] are the same as those for the E-rate. Libraries and schools that receive ESEA title III funds or LSTA state grants must block or filter all access to visual depictions that are obscene, child pornography, or harmful to minors. The rules do not apply to text.

language has a uniform meaning under the E-rate, it does not for programs under title III or LSTA. Program years may vary from state to state and, under ESEA, even from program to program.

As with the E-rate program, libraries and schools receiving funding under LSTA and ESEA have another full year to come into compliance if they are not able to do so during the first year. **However, by the third year after CIPA goes into effect, no more waivers are available.**[25]

It is possible to read the statute as equating "program years" with "annual program application cycles,"[26] as referenced with regard to libraries and schools that already have Internet safety policies and Internet filtering or blocking technology in place. However, it is not absolutely clear that these are the same, and "annual program application cycle" also lacks a uniform meaning for programs under title III and LSTA.

The Department of Education and the IMLS should provide guidance for libraries and schools on the deadlines that apply to title III and LSTA programs. This issue may be particularly complicated for recipients of LSTA funding, which is distributed on behalf of IMLS by 59 separate grantmaking authorities, each with its own "annual program application cycle."

4. Paying for Filtering Technology

Funds available under section 231 of LSTA and under section 3134, part A, of title VI of ESEA may be used for the purchase or acquisition of the "technology protection measures" required by CIPA, namely filtering and blocking technology. [27]

5. Penalties for Noncompliance

The primary difference between E-rate CIPA provisions and those applying to ESEA and LSTA funding is that funds already received under ESEA and LSTA cannot be recovered from schools or libraries that are found to be noncompliant. [28]

In the event that a library or school receiving ESEA or LSTA funding does not comply with CIPA's requirements, the law authorizes use of penalties available under the General Education Provisions Act, including withholding of further payments and issuance of a complaint to require compliance through a cease and desist order.[29] It also permits the Department of Education or the IMLS to enter into a compliance agreement with a funding recipient.[30] Additionally other laws, including criminal laws, provide serious penalties for providing fraudulent information or false certifications to the federal government.

6. Remedies

[25] 20 U.S.C. sec. 3601(a)(2)(B)(ii) & (iii) as added by CIPA sec. 1711 and sec. 1712(a)(f

Libraries and schools that lose ESEA or LSTA funding because of noncompliance with the filtering mandate can regain the ability to apply for grants in the future it by coming into compliance. Those libraries and schools must submit certification or other appropriate evidence that they have "cured the failure providing the basis for the withholding of payments" to the Department of Education or the IMLS for the agency to resume payments.