

RECEIVED

February 14, 2001

FEB 20 2001

Magalie Roman Salas
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

FCC MAIL ROOM

Subject: [CC Docket No. 96 -45, FCC 01 - 31] Federal-State Joint Board on Universal Service

Dear Ms. Salas:

The following correspondence is in response to the FCC's Notice of Proposed Rule Making regarding the Children's Internet Protection (CHIP) Act. For purposes of clarity, all issue statements are accompanied by the pertinent Sections from the Act.

H.R. 4577

Sec. 1701. Short Title "Children's Internet Protection Act"

Sec. 1703 Study of Technology Protection Measures

(b) Definitions

- (1) Technology Protection Measure ...means a specific technology that blocks or filters Internet access to visual depictions that are (a) obscene; (b) child pornography; (c) harmful to minors
- (2) Harmful to minors ...means any picture, image, graphic image file, or other visual depiction that ---(a)...appeals to prurient interest...(b) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors ...(c) taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.

Issues:

- (3) Reviews of filtering devices have consistently yielded the same results: Filters do not work and can promote a false sense of security. Blocking strategies based upon words do not block images, nor do they accurately and completely block contents described as obscene, harmful

No. of Copies rec'd 0
List A B C D E



City of Chicago
Richard M. Daley
Mayor

Chicago Public Library

Administration

Mary A. Dempsey
Commissioner

Board of Directors

Jayne Carr Thompson
President

Paul H. Dykstra
San Luong O
Martin R. Castro
Melody L. Hobson
Donald Hubert
John W. Jordan II
Cherryl T. Thomas

400 South State Street
Chicago, Illinois 60605
(312) 747-4999 (VOICE)
(312) 747-4314 (TDD)

www.chipublic.org

or child pornography. Infrequent "offensive" images are frequently not blocked while factual, "non-harmful" materials are blocked. Filters do not guarantee that hate speech or other information harmful to minors will be blocked. Filters do not block dangerous speech in chat rooms or e-mail that may put minors in harm's way. Filters can be disabled or circumvented.

- (4) Vendors of filtering packages, a market estimated to reach \$1.3 billion by 2003, have refused to disclose a list of words and sites which they block, citing the need to protect their intellectual property. Library staff is thus unable to exercise professional judgment, make informed decisions as to the efficacy and suitability of competing products and to determine any biases.
- (5) Some vendors of filtering software are using their packages to gather data, which can be sold to marketers and others, interested parties.
- (6) The FCC should convene a panel of experts and develop guidelines and methodology to establish a testing and certification process for filtering packages mandated by this Act.
- (7) Public library is responsible for providing free and equal access to materials regardless of format for all patrons.
- (8) Definitions of standards are subjective and should be developed at the local community level.
- (9) Final authority on serious literary, artistic, political, or scientific value should also be developed at the local, community level.

Sec. 1712. Limitation on availability of certain funds for Libraries

- (i) Amendment – Sec. 224 of the Museum and Library Services Act...

(f) Internet Safety

- (10) (A) (i) has in place a policy of Internet safety for minors that includes operation of a technology protection measure...that protects against access through such computers to visual

depictions that are – (I) obscene; (II) child pornography; or (III) harmful to minors; and

(ii) is enforcing the operation of such technology protection measure during use of such computers by minors; and

(B) (i) ...policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are – (I) obscene; or (II) child pornography; and (ii) is enforcing the operation of such technology protection measure during the use of the computers.

(11) **Disabling During Certain Use.** – An administrator, supervisor, or other authority may disable a technology protection measure under paragraph (1) to enable access to bone fide research or other lawful purposes.

(B) **Harmful to minors.** –(i) ...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 suitable to minors ... (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Issues:

Beyond issues with accuracy of filters and definitions as cited under Sections 1701 and 1703 above, this section includes additional terms subject to local interpretation and definition (i.e. appeal to prurient interest and patently offensive). Further, approach is overly burdensome to staff who are required to determine legitimacy of research needs of individual patrons and disable or engage technology protection measures pursuant to their standards. Staff is requested to make value judgments and to interact with technology at a level which may be beyond their individual proficiency level.

Sec. 1721 Requirement for Schools and Libraries to enforce Internet Safety Policies with Technology Protection Measures for Computers with Internet access as a condition of Universal Service Discounts.

(6) Requirements for Certain Libraries with Computers having Internet Access.—

(A) Internet Safety (iii) Public Notice; Hearing ...shall provide reasonable public notice and hold at least 1 public hearing or meeting to address the proposed Internet safety policy;

(B) Certification with Respect to Minors. – (i) ...operation of a technology protection measure ...that protects against access through such computers to visual depictions that are ---(I) obscene; (II) child pornography; or (III) harmful to minors; and (ii) is enforcing the operation of such technology protection measure during any use of such computers be minors.

(C) Certification with Respect to Adults. –(i) ...operation of a technology protection measure ...that protects against access through such computers to visual depictions that are –(I) obscene; or (II)child pornography; and (ii) is enforcing the operation of such technology protection measure during use of such computers.

(D) Disabling During Adult Use. – An administrator, supervisor or other person authorized ...(A) (i) may disable the technology protection measure concerned during use by an adult, to enable access for bona fide research or other lawful purpose.

(E) Timing of Implementation. – (i) (I) with respect to the first program funding year under this subsection following such effective date, not later than 120 days after the beginning of such program funding year...(II) with respect to any subsequent program funding year, as part of the application process for such program funding year.

Issues:

Requires public hearing on library policy; adds additional burden to local staff and disregards the responsibility of the Library Board. Staff certification that minors and adults are protected from visual access to obscene images by installation of filtering devices, which have been proven to be inaccurate, unreliable and can be disabled. As cited above, requires discretion of staff members to review and decide legitimacy of patron's purpose, a determination that is in direct conflict with the public library philosophy of free and open access to all materials, and which require library staff to render a legal determination for which they are not trained nor which they are eligible to make.

There is a case before the Supreme Court to determine if morphed or computer generated images of what appear to be children engaged in prohibited acts is "child pornography." This open issue regarding the definition of child pornography must be addressed in any certification process.

The application process for Year 4 (July 1, 2001 – June 30, 2002) E-rate funding began on July 1, 2000. Libraries filed forms 470 and 471 before passage of the CHIP Act. The FCC should designate Year 5 as the first program funding year as this is the first application process, which will occur subsequent to the passage of the CHIP Act. This will eliminate the retroactive application of the Act and the need for a separate certification process.

Sec. 1731. ...Neighborhood Children's Internet Protection Act

Sec. 1732 Internet Safety Policy Required

- (1) (A) adopt and implement an Internet safety policy that addresses –
 - (i) access by minors to inappropriate matter on the Internet and the World Wide Web;
 - (ii) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
 - (iii) unauthorized access, including so-called 'hacking', and other unlawful activities by minors online;
 - (iv) unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
 - (v) measures designed to restrict minors' access to materials harmful to minors; and
- (B) provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy.
- (2) Local Determination of Content. – The school board, local educational agency, library, or other authority shall make a determination regarding what matter is inappropriate for minors responsible for making the determination. No agency or instrumentality of the United States Government may –

(A) establish criteria for making such determination;

- (B) review the determination made by the certifying school, school board, local educational agency, library or other authority; or
- (C) consider the criteria employed by the certifying school, school board, local educational agency, library, or authority in the administration of subsection (h) (1) (B).

Issues:

Requires staff to monitor and insure safety of minors in the use of electronic mail, chat rooms and other forms of direct electronic communications. As staff is required to insure safety of use of technology, staff would be required to "look over the shoulder" of minors while they use technology. This violates patron's right to privacy, may have a chilling effect on teens and adolescents using the Internet to meet their informational needs and diverts valuable staff resources from answering reference questions and the performance of their other library related duties (i.e. collection development, user education, etc.)

Computer hacking is a programming skill that can be developed in many different programming languages. As computer programming is not a component of library education, staff must be trained to recognize hacking

Staff must further violate privacy by reviewing information shared by minors and determine if information is personal in nature and therefore inappropriate.

Local determination of content is allowed under this Section.

The Chicago Public Library appreciates the opportunity to comment upon the proposed implementation of the CHIP Act.

Sincerely,



Karen Danczak Lyons
First Deputy Commissioner
Chicago Public Library