The following document is from:

Safe and Responsible Use of the Internet: A Guide for Educators

Nancy E. Willard, M.S., J.D.

Responsible Netizen Institute
474 W 29th Avenue
Eugene, Oregon 97405
541-344-9125
541-344-1481 (fax)
Web Site: http://responsiblenetizen.org
E-mail: info@responsiblenetizen.org

Part II. Safe and Responsible Internet Use Plan

3. Technology Protection Measures

CIPA Requirements

(A) Internet Safety
  (i) IN GENERAL.--...(A)n elementary or secondary school having computers with internet access may not receive services at discounted rates under paragraph (1)(B) unless the school, school board, local education agency, or other authority with responsibility for administration of the school--
  (I) submits to the Commission the certifications described in subparagraphs (B) and (C); ...

...

(B) CERTIFICATION WITH RESPECT TO MINORS.-- A certification under this subparagraph is a certification that the school, school board, local education agency, or other authority with responsibility for administration of the school--

(i) is enforcing a 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;

(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 by minors."[1]

(1) TECHNOLOGY PROTECTION MEASURE.--the term 'Technology Protection Measure' means a specific technology that blocks or filters Internet access to visual depictions that are-- (the prohibited material)[2].

Complying with CIPA Without Using Commercial Filtering Software

It is possible to comply with CIPA and not use commercial filtering software.

In August 2003, the National Telecommunications and Information Administration released a Report to Congress on the Children's Internet Protection Act. This report was a Study of Technology Protection Measures. One of the issues the report addressed was the kinds of technology protection measures that can be used by districts to comply with CIPA. The report noted the following concerns:

> Commenters discussed the difficulty that some educational institutions have interpreting CIPA's "technology protection measure" language. Some commenters claim that many educational institutions default to "filtering" technology only, without researching other types of technology protection options. As a result, many believe that this reliance on mostly filtering products stifles the marketplace and serves as a disincentive for technology companies to invest in the research and development of newer and more sophisticated products. Moreover, as set forth above, filtering and blocking software has not been able to overcome problems of overblocking, inability to generate an updated index for the Internet, and lack of correspondence to statutory definitions and categories. Yet, other technology tools can or have the potential to address better the needs of educational institutions. Thus, NTIA recommends that Congress change the current legislation to clarify that the term "technology protection measure" encompasses not only filtering and blocking software, but also other current and future technology tools. … Alternatively to amending CIPA, NTIA recommends that the FCC and the U.S. Department of Education (DOE) provide further guidance to recipients of E-rate or DOE funds on the meaning of technology protection measures[3].

[1] 47 U.S.C. 254 (h)(5)(B)
[2] 47 U.S.C. 254 (h)(7)(I)
[3] U.S. Department of Commerce, National Telecommunications and Information Administration, http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/.

(The author of this Guide was cited extensively in the NTIA report. The author specifically addressed this issue with the NTIA. The material and arguments presented to the NTIA by the author are included at the end of this chapter.)

NRC Report -- Analysis of Protection Technologies

The NRC committee was charged with the task of conducting a study of "computer-based control technologies" and other approaches to address the concerns of pornography on the Internet[4]. The NRC committee conducted a full study of various technologies that "can be used to *protect* or limit children's exposure to inappropriate sexually explicit material on the Internet[5]." Note the use of the term "protect," which is the same term used in the CIPA legislation.

Table 12.1, of the *NRC Report*, entitled Technology-Based Tools for the End User, is perhaps the most comprehensive list of the types of technologies that function, according to the NRC, to *protect* against access to inappropriate material. Presumably, the types of technologies contained on this list are ones that a school district could consider adopting to comply with CIPA[6].

The NRC committee was charged with the task of conducting a study of "computer-based control technologies" and other approaches to address the concerns of pornography on the Internet[7]. The NRC's conclusion was that while technologies had a role to play in the protection of youth, social and educational strategies must provide the foundation for the protection of children. The NRC committee conducted a full study of various technologies that "can be used to *protect* or limit children's exposure to inappropriate sexually explicit material on the Internet[8]."

Table 12.1, entitled Technology-Based Tools for the End User, a recent comprehensive list of the types of technologies that function to protect against access to inappropriate material. Presumably, the types of technologies contained on this list are ones that a school district can adopt to comply with CIPA[9].

In reviewing the information on technology protection measures, educators should keep in mind the developmental dimensions of the issue. The protection and access needs of elementary students are different from those of high school students. As the *NRC Report* noted:

> The information needs of children that the Internet can and should meet also change with the developmental stage of the child in question. For example, juniors and seniors in high school have a much broader range of information needs (i.e., for doing research related to their education) than do those in the third grade or in junior high school. This, in turn, leads to the question of how to provide older children with access to a broader range of

[4] P.L. 105-314, the *Protection of Children from Sexual Predators Act of 1998*, Title IX, Section 901.
[5] National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002). URL: http://bob.nap.edu/html/youth_internet/.
[6] With the exception of Instant Help, which the NRC indicated was an after-the-fact solution.
[7] P.L. 105-314.
[8] NRC report at Section 11.3.
[9] With the exception of Instant Help.

material while preventing younger ones from accessing material that is deemed not appropriate given their developmental level[10].

Rather than a one-size-fits-all commercial filtering approach, technologies should be analyzed from their perspective of how best they can meet the protection and access needs of students at different levels in their schooling.

One significant concern related to CIPA is the perception of educational decision-makers that the *only* type of technology that will meet the requirements is commercial, proprietary-protected filtering software. If this perception remains unchanged, all future development of alternative technology protection tools will cease. No company could expect to penetrate the marketplace.

NRC Technology-Based Tools Table

The following is Table 12.1 as presented in the *NRC Report*:

Type of Tool	Function	One Illustrative Advantage	One Illustrative Disadvantage	Voluntary versus Involuntary Exposure
1. Filter	Block "inappropriate" access to prespecified content; typically blocks specific web pages, may also block generic access to instant messages, e-mail, and chat rooms	Can be configured to deny access to substantial amounts of adult-oriented sexually-explicit material from commercial web sites	In typical (default) configuration, generally denies access to substantial amounts of Web material that is not adult-oriented and sexually explicit.	Protects against both deliberate and inadvertent exposure for sites that are explicitly blocked; can be circumvented under some circumstances
2. Content-limited access	Allow access only to content and/or services previously determined to be appropriate	Provides high confidence that all accessible material conforms to the acceptability standards of the access provider	May be excessively limiting for those with broader information needs than those served by the access provider	Very low possibility of deliberate or inadvertent exposure given that all of the material is explicitly vetted
3. Labeling of content	Enable users to make informed decisions about content prior to actual access	Separates content characterization (e.g., sexually explicit or not) from decisions to block; multiple	Effectiveness depends of broad acceptance of a common labeling framework	Likelihood of exposure depends on accuracy of labels given by labeling party

[10] NRC, supra at Section 14.1.2.

		content raters can be used		
Monitoring with individual identification	Examining a child's actions by an adult supervisor in real time or after the fact	Rarely prevents child reaching appropriate material that might have been mistakenly flagged as inappropriate	Potential loss of privacy zone for child	Warnings can help to deter deliberate exposure; ineffective against inadvertent exposure
Monitoring without individual identification	Watch the collective actions of a group (e.g., a school) without identifying individual	Can provide useful information about whether or not acceptable use policies are being followed	Does not enable individual accountability for irresponsible actions	Warnings can help to deter deliberate exposure; less effective against inadvertent
Spam-controlling tools	Inhibit unsolicited e-mail containing sexually explicit material (or links to such material) from entering child's mailbox	Can reduce volume of inappropriate e-mails significantly	Among users concerned about losing personalized e-mail, reduced tolerance for false positives that block genuine personal e-mails incorrectly identified as spam	Mostly relevant to inadvertent exposure (i.e. unsought commercial e-mail containing sexually-explicit material)
Instant help	Provide immediate help when needed from an adult	Provide guidance for child when it is likely to be most effective, i.e. at time of need	Requires responsive infrastructure of helpers	Mostly relevant to inadvertent exposure

Technology Protection Measure Recommendations

The following are recommendations related to technology protection measures that can effectively used in the context of a comprehensive education and supervision approach.

Filtering based on first party content labeling

This technology is a combination of categories 1 and 3 above. The Internet Content Rating Association has been leading an international effort to encourage labeling of web sites[11]. Here is what NRC had to say about ICRA:

[11] http://www.icra.org.

> Recognizing that the primary impediment to the success of rating schemes is the extent to which Internet content is currently not labeled, the Internet Content Rating Association (ICRA) has undertaken a global effort to promote a voluntary self-labeling system through which content providers identify and label their content using predefined, cross-cultural categories. ICRA is a global non-profit organization of Internet industry leaders committed to making the Internet safe for children while respecting the rights of content providers[12].

The ICRA filter can then be set to block access to any site that has labeled itself as an adult site or a site with sexually explicit content. There are certainly no constitutional problems with preventing students from accessing sites that have labeled themselves as appropriate only for adults or sexually explicit. The disadvantage of this approach is that the system will only block access to "responsible" adult sites that have voluntarily labeled themselves. Therefore, the underblock rate will continue to be of concern. However, the FCC declined to establish any effectiveness standard for technology protection measures. The ICRA system is free.

Because the underblocking rate with this approach will be of concern, it is necessary for a district to use this approach only as a component of a comprehensive strategy. Using the ICRA system to block access to adult and sexually explicit sites is not effective enough to use as primary means of protecting elementary students. Nor will it deter a student who is intentionally seeking access from accessing some sites. Therefore, it remains important to establish safe spaces for elementary students (the ICRA system can also be used for this purpose, see below), to ensure all students are educated about safe and responsible use, and to establish effective supervision and monitoring. If a district has implemented a comprehensive education and supervision approach, students will gain skills in avoiding sites that have not rated themselves and will know how to handle the situation if such a site is accidentally accessed.

Non-Proprietary-Protected Filtering Software

There are some filtering software companies that provide access to their database of blocked sites. If companies are also willing to provide full and complete information about the criteria they use and the keyword that they use to identify suspicious sites, it is likely that such products are sufficiently "open" to meet the requirements of local control and public accountability.

Because these products are not likely as robust as the commercial, proprietary-protected products, they area likely to underblock and therefore should not be used outside of the context of a comprehensive approach. The products are also likely to overblock. Therefore it is also essential to assess the ease of overriding the software to provide access to appropriate material that has been inappropriately blocked. The authority to override should be widely dispersed throughout the district so that there is rapid turn-around whenever a request for access is made.

Filters That Can Be Set To "Warn" But Not Block.

The NRC described this kind of technology as follows:

[12] NRC, supra at Section 12.1.5.

> Built into any filter is a specification of content that should be blocked. Instead of blocking access, a filter could warn the child of impending access to inappropriate material, but leave it to his or her discretion whether or not to access the material. Because the child does have choices, such a feature would have pedagogical advantages with respect to helping children to make responsible choices, assuming the environment is structured in a way to facilitate such assistance[13]

Products that warn but do not block would certainly provide an advantage related to the concerns of overblocking that frustrates educational activities. However, if the product is blocking access to controversial material based on viewpoint discrimination, the use of such products could still raise concerns. For example, if students seeking information on sexual orientation are constantly informed by the system that sites with such information may contain "inappropriate material" this would be of concern. Students would also be aware that school officials would have access to reports on the functioning of the system and this may have a inappropriate dampening effect of student access of potentially controversial information.

Another consideration of such a system is cost. If the district's comprehensive strategy is working to prevent access to inappropriate material, the costs of this kind of a system would likely be unnecessary.

Content Limited Access

Content limited access systems allow for access to a set of sites that have been reviewed and approved in accord with a set of established criteria. The *NRC Report* discussed this type of technology in terms of content-limited Internet Service Providers and described such services as follows:

> As a feature of their offerings, a number of ISPs provide Internet access to only a certain subset of internet content .... Some content-limited IPSs, intended for use by children, make available only a very narrow range of content that has been explicitly vetted for appropriateness and safety. Thus, all of the Web pages accessible have been viewed -- and assessed -- for content that is developmentally appropriate, educational, and entertaining. (This approach is known as "white listing" -- all content not on a white list are disallowed, ... [14])

The NRC's perspective of content-limiting technologies was incomplete. There are additional technologies, as well as techniques, that can achieve the objective of "content-limited" -- restricting access to sites that have been reviewed and determined to meet certain standards. These include:

- Commercial subscription services established to serve the educational market.
- ICRA system configured to allow access to predefined list of sites.

[13] NRC, supra at Section 12.1.6.
[14] NRC, supra at Section 12.1.1.

- Proxie server that limits access to sites that have been downloaded from the Internet and prevents live Internet access.

The best technique for establishing limited-content access is the establishment of district and classroom web sites that link to educational content. In a well-supervised elementary classroom, with clearly defined limits on Internet use, the best content-limiting access technique is the class web site or set of hot links that the teacher has established that specifically relate to the specific instructional objectives of the current lesson.

Content limiting techniques, facilitated through the use of various technologies, are highly recommended as the primary strategy to address the safety concerns for elementary students. Students of this age do not have the knowledge, skills, or developmental capacity to exercise the kind of judgement necessary to make safe choices in their use of the internet. Free searching on the Internet is a waste of valuable educational time.

For middle school and high school students, educational web pages and search engines can also facilitate access to sites that have been reviewed for educational appropriateness. However, especially with high school students, limiting access to such sites would be unnecessarily restrictive. Students of this age must gain the skills to effectively use the open Internet for research and career development.

Content Labeling

While the NRC considered this a separate topic, essentially content labeling is a technique that can work in conjunction with systems that filter out inappropriate material or limit access to appropriate material. The NRC noted the leadership currently being provided by ICRA to foster content labeling.

Monitoring

The NRC describes monitoring as follows:

> Monitoring, as a way of protecting youth from inappropriate content, relies on deterrence rather than prevention per se. In some cases, it is the threat of punishment for an inappropriate act that has been caught through monitoring that prevents the minor from behaving in an inappropriate manner. In other cases, "catching someone in the act" can provide an important "teachable moment" in which an adult can guide and explain to the child why the act was inappropriate and why this content is on the Internet[15].

It is important to note the language used by the NRC to describe monitoring: "a way of *protecting* youth from inappropriate content." CIPA requires schools to certify that they are using a Technology Protection Measure that "*protects* against access" to unacceptable material[16]. Clearly monitoring should be considered a technology that meets the CIPA requirements for a Technology Protection Measure. Further, the NRC section that addresses

[15] NRC, supra at Section 12.2.1.
[16] 47 U.S.C. 254 (h)(5)(B).

monitoring includes a footnote[17] that references a New York Times article presenting a new filtered monitoring technology wherein it is stated:

> "But the lawmakers who drafted the Child Internet Protection Act, as it is known, said they wanted the law to be flexible enough to allow alternatives to simple filtering, so long as the goal of preventing children from encountering forbidden material can be met[18]."

The NRC chart lists two types of monitoring -- with and without identifying individual users. From an educational perspective, if the focus is on fostering safe and responsible use of the Internet, there is little value in monitoring without identifying the individual user. As the NRC noted:

> Because monitoring tools do not place physical blocks against accessing inappropriate material, a child who knowingly chooses to engage in inappropriate Internet behavior or to access inappropriate material can do so if he or she is willing to take the consequences of such action. However, the theory of monitoring is that knowledge of monitoring is a deterrent to taking such action[19].

Clearly, to fulfill its role as a motivation for deterrence, clear notice of the existence of monitoring is critically important. As is discussed in depth in "Supervision, Monitoring, and Privacy," the use of monitoring technologies fit very will into existing legal principles of school privacy and search and seizure.

The NRC also addressed the use of monitoring as a component of an educational strategy. It stated:

> If monitoring is coupled to explanations and guidance about appropriate and inappropriate behavior, there is some potential that this application can promote the long-term development and internalization of appropriate behavioral norms. But the explanation and guidance are essential. If, as is much more likely in an institutional setting and in many home situations, the primary or exclusive consequence of detection of inappropriate access is punishment, such learning may well not occur. Even more destructive would be punishment resulting from inadvertent access to inappropriate material, as one can easily imagine might be imposed by an adult supervisor who did not believe an assertion by his or her charge that the inappropriate Web page was viewed by accident.

While it is to be expected that detection of inappropriate activities by a student would naturally result in some form of punishment, it could be hoped that the disciplinary encounter would incorporate explanation and guidance. It is also essential that students who have inadvertently accessed inappropriate material are not inappropriately disciplined.

---

[17] NRC supra at Section 12.2 (footnote 38).

[18] Schwartz, J. Schools Get Tool to Track Students' Use of Internet. *The New York Times*, 05/21/2001. The reporter who wrote this story affirmed to the author that one of the lawmakers he interviewed for this story was Senator John McCain, the senator who introduced the CIPA legislation.

[19] NRC, supra at Section 12.2.2.

SPAM Controlling Technologies

"SPAM" is the term that is applied to unsolicited e-mail, some of which might be pornographic in nature or invite the recipient to visit a new pornographic site. An additional concern related to SPAM is the transmission of computer viruses. The manner in which a school district control -- or seeks to control -- SPAM will be dependent on the type of e-mail system it uses. If the district has established its own e-mail system, SPAM control technologies will need to be incorporated into the network. If the district has contracted with subscription communication services, the SPAM technologies will be incorporated into the system at their server level.

Regardless of the use of SPAM control technologies, students and staff must also learn not to open messages from an unknown source -- especially those with the annoying subject lines, such as "You have already won" or "Here is something special for you."

Instant Help

The *NRC Report* suggested the development of "Instant Help" technology that could be present as a component of a browser or desktop. The NRC indicated that this technology, which is not currently available, would not prevent exposure, but would operate after the fact to provide support for the child.

In schools, "instant help" should be in the form of a "real world" caring, knowledgeable teacher.

Commercial, Proprietary-Protected Filtering Software

As outlined in Chapter III-6, the author of this Guide believes the use of these products by public institutions presents significant constitutional concerns. In many schools, the ineffective use of these products is frustrating the educational activities of both students and staff.

These products have also grown quite expensive. While the initial use of these products was to prevent children from accessing material considered inappropriate for them, the market for these products quickly shifted. The vast majority of sales of these companies are to corporations and other employers seeking to manage the inappropriate use of the Internet by their employees. As a result, these products are now frequently referred to as Internet use management systems. The functional requirements for products used by employers are different from the requirements of schools seeking to comply with CIPA. The excessive costs of these products are primarily associated with the meeting the functional requirements of the employers.

Nevertheless, for the time being, if only to satisfy community concerns, many school districts will feel it necessary to use these kinds of products. If this is the case, the following are guidelines for use that will assist in addressing the concerns of overblocking and underblocking.

Conduct a thorough “due diligence” evaluation of the company.

To address concerns over the potential of intentional viewpoint discrimination it is necessary to thoroughly investigate the company to determine its values and biases that may impact blocking decision-making. Information to request should include the database of blocked sites, specific information on blocking criteria for any category you are considering blocking including the

keywords used to search for sites to be blocked, background information on all leading corporate officials, and a detailed list of all major corporate clients.

Because thee companies protect much of this information as confidential, proprietary information, you may or may not have much success. But the manner in which the company responds to this very legitimate request could be very insightful.

The author of this Guide has discovered eight filtering software companies with very close relationships with conservative religious organizations[20]. Relationships such as these could result in significant blocking based on viewpoint discrimination.

Block the least number of categories necessary.

To comply with CIPA, only the categories blocking sexually explicit adult material are required to be blocked. Other categories, which may include material students are prohibited from accessing, do not generally provide graphic images on the screen that are disruptive. The fewer the categories blocked, the less the potential for overblocking.

Recently, the Kaiser Family Foundation reported on its study on the ability to access sites containing health information across a broad range of topics when filtering software has been installed[21]. This study assessed the performance of the top six selling filtering products in public schools. The filters were configured at a least restrictive level, intermediate constrictive level, and most restrictive level. The health information sites included topics unrelated to sex, topics related to sexual body parts, topics related to sex, and sites presenting potentially controversial health information.

Kaiser found across all of the health information that filters set at the least restrictive level blocked only 1.4% of the health information sites. Filters blocked only 5% of such sites at the intermediate level. However, filters blocked 24% of such sites at the most restrictive level.

A closer analysis of the data reveals blocking patterns that present significantly greater concerns of the presence of viewpoint discrimination. Even at the least restrictive level roughly 10% of health sites containing information related to “Safe Sex,” “Condoms,” and “Gay” were blocked.

At the intermediate and most restrictive levels in those categories where the subject area is controversial, the rate of overblocking was significantly higher. The categories that stood out included “Ecstasy” (drug education sites), “Safe Sex,” “Condoms”, “Gay,” and “Lesbian.” At the intermediate restriction level, typical of most school settings, the filters blocked approximately 25% (1 in 4) of the health information sites in these subject areas. At the most restrictive level, the filters blocked approximately 1 in 2 health sites in these controversial subject areas.

As noted in Chapter II-2, any district that feels it necessary to block multiple categories to effectively manage student Internet use should take a long close look at the effectiveness of its

[20] See, Filtering Software: The Religious Connection at http://responsiblenetizen.org/documents/religious1.html.
[21] Kaiser, supra.

professional development supporting the effective educational use of the Internet, education, and supervision.

Do not make the mistake of believing that the use of these products will prevent students from accessing inappropriate material.

The Kaiser Family Foundation, also assessed the effectiveness of proprietary-protected filtering software in preventing access to inappropriate material[22]. As one component of the study, the researchers assessed the ability to intentionally access pornography sites Roughly one in ten porn sites were accessible regardless of how the filters were configured (least -- 87% of pornography sites blocked; intermediate -- 90% of pornography sites blocked; most -- 91% of pornography sites blocked). When the researchers assessed the ability of filters to block access under conditions simulating accidental access at the least restrictive level, only 62% of the pornography sites were blocked.

If one in ten pornography sites are accessible when filtering has been installed, this rather expensive technology will provide approximately five minutes of protection for a curious teen at an unsupervised computer.

Districts must ensure that students understand the policy and its ramifications, provide effective supervision, and appropriate discipline.

Select a product that allows for significant flexibility with respect to the designation of individuals with authority to override the filter and an easy to manage override process. Establish internal procedures that ensure timely, responsive overriding of inappropriately blocked sites. These procedures should allow for anonymous requests to override.

Under the Supreme Court ruling in the ALA case, overriding the filter to provide access to inappropriately blocked sites is the cure for any constitutional concerns. It is absolutely essential to provide for such overriding in timely, responsive, and anonymous manner.

Regularly review the performance of the filtering product.

Evaluate the degree to which the filtering product is blocking access to appropriate material and failing to block access to inappropriate material.

[22] Kaiser Family Foundation (2002), *See No Evil: How Internet Filters Affect the Search for Online Health Information Executive Summary.* http://www.kff.org/content/2002/3294/Internet_Filtering_exec_summ.pdf.

Comments made by NTIA made by author:

Complying with CIPA Without Using Commercial Filtering Software

It appears that is possible to comply with CIPA and not use commercial proprietary-protected filtering software.

However, there are likely to be different legal opinions on this question. Therefore, this issue must ultimately be decided by a school district after consultation with their own legal counsel.

The following is information that supports the position that school districts may use technology protection measures other than commercial proprietary-protected filtering software to comply with CIPA.

Statutory Provisions

CIPA requires that districts certify they are using a Technology Protection Measure. Technology Protection Measure is addressed in two ways in the CIPA statute:

> ... (T)he operation of the 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; (II) child pornography; or (III) harmful to minors; ...[23]

> TECHNOLOGY PROTECTION MEASURE.--the term 'Technology Protection Measure' means a specific technology that *blocks or filters* Internet access to (the prohibited material)[24].

The term "filter" has become a generic term to cover products that seek, in some manner, to screen Internet traffic and block access to material that has been deemed to be inappropriate. A question is whether the term "filter" necessarily includes the concept of "block." The specific terms of the statute are "blocks or filters."

The statute also uses the terms "protect against access" not "prevent access." Presumably, therefore, any technology that either filters traffic or blocks traffic and is used for the purpose of protecting against access to inappropriate material should be considered to meet the statutory requirements.

The NCIPA statute also contains the following provision:

> LOCAL DETERMINATION OF CONTENT.-- A determination of what matter is considered inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination. No agency or instrumentality of the United States Government may--
> (A) establish criteria for making such determination;

[23] 47 U.S.C. 254 (h)(5)(B)
[24] 47 U.S.C. 254 (h)(7)(I)

(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, school board, local educational agency, library, or other authority in the administration of subsection (h)(1)(b)[25].

If the definition of Technology Protection Measure is read in conjunction with the provision for local determination of content, it becomes apparent that school districts should have the ability to select a Technology Protection Measure that allows the district to make a local determination of what material is considered inappropriate. This presumably means that technologies other than ones that protect what they are doing as confidential proprietary information and thereby prevent such local determination would meet the requirements of the law.

FCC Regulations Related to Technology Protection Measures

The FCC also addressed the issue of Technology Protection Measures in the development of regulations for CIPA. With respect to the type and effectiveness of Technology Protection Measures, the FCC stated:

33. Some commenters have requested that we require entities to certify to the effectiveness of their Internet safety policy and Technology Protection Measures. However, such a certification of effectiveness is not required by the statute. Moreover, 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.

34. A large majority of commenters express concern that there is no Technology Protection Measure currently available that can successfully block all visual depictions covered by CIPA. Such commenters seek language in the certification or elsewhere "designed to protect those who certify from liability for, or charges of, having made a false statement in the certification" because available technology may not successfully filter or block all such depictions. Commenters are also concerned that Technology Protection Measures may also filter or block visual depictions that are not prohibited under CIPA.

35. We presume Congress did not intend to penalize recipients that act in good faith and in a reasonable manner to implement available Technology Protection Measures. Moreover, this proceeding is not the forum to determine whether such measures are fully effective.[26]

It is significant that the FCC has specifically stated that there it has not established any effectiveness standards. As noted, the statute uses the terms "protects against access," not "prevent access." This should mean that districts may chose from newer technologies that hold better potential for addressing the underlying concerns, even if those products are not entirely effective in preventing all access, rather are useful in protecting against access.

[25] 47 U.S.C. 254 (l)(2)
[26] FCC Order, supra.

Comments Senator McCain, Chief Sponsor of CIPA

The following are comments made in a press release issued by Senator McCain, the chief sponsor of CIPA in response to the filing of the ALA lawsuit, related to matters of types of technologies that can be used to comply with CIPA.

> Washington, D.C. – Senator John McCain (R-AZ), Chairman of the Committee on Commerce, Science, and Transportation, today made the following statement in response to the American Civil Liberties Union (ACLU) court challenge to the Children's Internet Protection Act:
>
> "The Children's Internet Protection Law, which passed the Senate 95-3 and has consistently enjoyed enormous bipartisan support, simply ensures that schools and libraries across the country have the technology they need to protect children from harmful material on the Internet. *This law gives communities the freedom to decide what technology they choose to use and what to filter out.* It does not dictate any specific actions be taken by communities or apply a federal standard, it simply requires them to have *some technology* in place to protect children if they are using federal funds for Internet access[27].

NRC Report -- Analysis of Protection Technologies

The NRC committee was charged with the task of conducting a study of "computer-based control technologies" and other approaches to address the concerns of pornography on the Internet[28]. The NRC committee conducted a full study of various technologies that "can be used to *protect* or limit children's exposure to inappropriate sexually explicit material on the Internet[29]." Note the use of the term "protect," which is the same term used in the CIPA legislation.

Table 12.1, of the *NRC Report*, entitled Technology-Based Tools for the End User, is perhaps the most comprehensive list of the types of technologies that function, according to the NRC, to *protect* against access to inappropriate material. Presumably, the types of technologies contained on this list are ones that a school district could consider adopting to comply with CIPA[30]. The types of tools and description of function provided by NRC are as follows in columns 1 and 2. Column 3 is additional material the author of this Guide has added to describe more specific technologies of the type noted.

These technologies are discussed more in depth in the chapter "Technology Protection Measures."

Type of Tool	Function	Author's Comment
1. Filter	Block "inappropriate" access to prespecified content; typically blocks	- Filtering based on first party content labeling [e.g., Internet Content Rating Association

[27] URL: http://mccain.senate.gov/intfilt01.htm. Tuesday, March 20, 2002. Emphasis added.
[28] P.L. 105-314, the *Protection of Children from Sexual Predators Act of 1998*, Title IX, Section 901.
[29] National Research Council. *Youth, Pornography, and the Internet* at 11.3. (Dick Thornburgh & Herbert S. Lin, eds., 2002) URL: http://bob.nap.edu/html/youth_internet/
[30] With the exception of Instant Help, which the NRC indicated was an after-the-fact solution.

	specific web pages, may also block generic access to instant messages, e-mail, and chat rooms.	(ICRA) set to block access to sites that have labeled themselves as adult sites -- a combination of technologies #1 and #3. - Filtering software where processes and blocked list are not confidential. - Filters that can be set to "warn" but not block.
2. Content-limited access	Allow access only to content and/or services previously determined to be appropriate.	- Subscription services. - Proxie Server. - ICRA system set to allow access to predefined list of sites.
3. Labeling of content	Enable users to make informed decisions about content prior to actual access.	Content labeling (#3) is an activity that can support filtering (#1) and content limited access (#2). ICRA is leading the effort in content labeling.
4. Monitoring with individual identification	Examining a child's actions by an adult supervisor in real time or after the fact.	- Filtered monitoring tools filter Internet traffic and report on traffic that is suspected to be in violation of policy[31].
5. Monitoring without individual identification	Watch the collective actions of a group (e.g., a school) without identifying individuals.	Without the ability to identify specific individuals, the effectiveness of this technology would be in question.
6. Spam-controlling tools	Inhibit unsolicited e-mail containing sexually explicit material (or links to such material) from entering child's mailbox.	Spam-controlling software is a must at some location within the e-mail communication system.
7. Instant help	Provide immediate help when needed from an adult.	The *NRC Report* indicated that this technology, which is not currently in use, is not designed to prevent exposure, but to operate after the fact.

[31] An argument can clearly be made that since CIPA specifically references monitoring, that monitoring tools are not considered technology protection measures. However, the NRC specifically refers to monitoring as a technology for "protecting youth from inappropriate content" (NRC at Section 12.1.1) which is virtually identical to the language of CIPA requiring a Technology Protection Measure that "protects against access." Additionally, there was an article about a filtered monitoring technology in the New York Times where the issue of CIPA applicability was addressed, as follows: "But the lawmakers who drafted the Child Internet Protection Act, as it is known, said they wanted the law to be flexible enough to allow alternatives to simple filtering, so long as the goal of preventing children from encountering forbidden material can be met." Schwartz, J. Schools Get Tool to Track Students' Use of Internet. *The New York Times*, 05/21/2001. The reporter who wrote this story affirmed to me that one of the lawmakers he interviewed for this story was Senator John McCain, the senator who introduced this legislation.

FCC Order Related to Local Control

There are several provisions in the *FCC Order* that addresses local control, including the following:

With respect to the overall rules:

> 2. We adopt these rules with the goal of faithfully implementing CIPA in a manner consistent with Congress's intent. We have attempted to craft our rules in the most practical and efficacious way possible, while providing schools and libraries with maximum flexibility in determining the best approach. Moreover, to reduce burdens in the application process, we have designed rules to use existing processes where applicable. We conclude that local authorities are best situated to choose which technology measures and Internet safety policies will be most appropriate for their relevant communities.[32]

Conclusion

Given the FCC's regulations, the findings and recommendations of the recent *NRC Report*, and the ruling in the *ALA* case, it can be considered highly improbable, if not inconceivable, that the FCC would intervene at a community level to tell a school district that it had no choice under CIPA but to delegate control to a third party filtering company to decide what its students could or could not access on the Internet.

[32] FCC Order, supra.