

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

Copyright © 2002-03 Nancy E. Willard. This document is distributed as “Honor Text.”

The purpose of the “Honor Text” approach is to allow for the wide dissemination of information, while providing financial support for continued policy research and dissemination. The following are the “honor text” guidelines:

- If you are a student or other researcher and are using one copy of this material for personal research, you are not requested to provide compensation.
- If you have established a web site or web page listing information resources for educators, you may freely link to this site or any individual document on this site and are not requested to provide compensation.
- If you are a faculty member, professional development coordinator, or the like and have assigned material on this site as readings for your students (whether provided in hard copy or linked to as an online component of course resources), you are requested to provide compensation for such use. The standard rate for the reproduction of copyrighted materials for courses is \$.10/page/student. If you are using substantial sections, please make contact to arrange for discounts.
- If you are a school or a district and have used these materials for planning and/or policy development, you are requested to provide compensation in a manner that reflects the perceived value.
- For all other uses or further information, please e-mail us at info@responsiblenetizen.org.

Although the author has made every effort to ensure the accuracy and completeness of the information contained in this book, the author assumes no responsibilities for inaccuracies or omissions. Although this book discusses legal issues, nothing contained in this book should be interpreted as the provision of legal advice to any individual, district, or other entity..

Part III. Legal Issues – Internet Use in School

6. The Constitutionality of the Use of Proprietary-Protected Filtering Software in U.S. Public Schools

NOTE: This document has not been rewritten in light of the recent Supreme Court decision in the ALA case. It will be – when the author has the time. However, Justice Kennedy’s opinion in the ALA case, which concurred with the ruling, noted that his decision was based on the CIPA statute itself and did not address implementation actions that might be taken under CIPA. While CIPA itself has been determined to withstand constitutional scrutiny, clearly issues of concern with respect to the implementation of the use technology protection

Safe and Responsible Use of the Internet – Part III, Chapter 6, page 1

measures remain. While the author recognizes the need to rewrite this chapter to address the recent decision, the author maintains that there are significant constitutional concerns raised by the use of proprietary-protected filtering software by public institutions.

Overview

In light of the recent ruling in the case brought by the American Library Association and others challenging the Children's Internet Protection Act, it is likely that the use of proprietary-protected Internet filtering software in schools will ultimately be found to be unconstitutionally restricting student access to material on the Internet. More importantly, rather than placing primary reliance on technology quick fixes, schools should be focusing their efforts on preparing students to use the Internet in a safe, responsible, and effective manner.

The Internet has emerged in the last decade as an extremely important conduit for information and communications. The objective of schools is to prepare students for active and effective participation in society. The information and communication resources of the Internet have become an essential component of this preparation.

Schools are uniquely positioned to serve as the primary vehicle through which young people can develop the knowledge, skills, and motivation to use the Internet in a safe, responsible, and effective manner. Many schools are placing primary reliance on technology quick fixes in the false hope that by installing filtering software they have done their job in this area. They have not. Many school officials are using filtering as a surrogate to fulfill important responsibilities of education and supervision.

Two events occurred during the month of May 2002 that have a direct impact on questions related to the constitutionality and the advisability of the use of proprietary-protected filtering software¹ in U.S. public schools.

On May 8, 2002, the National Research Council (NRC) released its report entitled *Youth Pornography and the Internet*². This report was the culmination of a two year research effort conducted by a distinguished committee of experts, led by committee chair Dick Thornburgh, former U.S. Attorney General. A major conclusion of this report was:

While both technology and policy have important roles to play, social and educational strategies to develop in minors an ethic of responsible choice and the skills to effectuate these choices and to cope with exposure are foundational to protecting children from

¹ The term "proprietary-protected filtering software" refers to those filtering software products provided by private companies that protect information regarding blocking criteria, blocking processes, the actual list of blocked sites, and other relevant corporate information as proprietary trade secrets. This includes all of the most commonly used filtering products in US schools today, including products provided by N2H2, CyberPatrol, WebSense, Secure Computing, Symantec, 8e6 Technologies and others.

² National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002), available at URL: http://bob.nap.edu/html/youth_internet/.

negative effects that may result from exposure to inappropriate material or experiences on the Internet.³

In the preface to the report, Dick Thornburgh, indicated that the report would "disappoint those who expect a technology 'quick fix'" and chided school officials and others for seeking "surrogates to fulfill the responsibilities of training and supervision needed to truly protect children from inappropriate sexual materials on the Internet."⁴

On May 31, 2002, the US District Court for the Third Circuit issued its ruling in a case that the American Library Association, American Civil Liberties Union, and others brought challenging the constitutionality of the Children's Internet Protection Act⁵ (CIPA), *ALA v. US*⁶. CIPA, enacted by Congress in December 2000, requires all schools and libraries receiving federal funds for technology to install a "technology protection measure," which is a specific technology that will filter or block access to obscene material, child pornography, and material that is considered harmful to minors.

The court ruled that CIPA was unconstitutional because the actions required under the law would violate the constitutional rights of library patrons, adults and minors, to access constitutionally protected material on the Internet⁷. The court considered access to the Internet in public libraries to be so intrinsically linked to basic First Amendment values, that they applied the most strict level of scrutiny to the restriction placed on its use by filtering software. Although there was a compelling interest in protecting children and adults from accidental or intentional access to inappropriate material, proprietary-protected filtering systems are not narrowly tailored to address this concern because they block access to substantial amounts of material that is constitutionally protected. Additionally, the court found that there were less restrictive alternatives that can be used to address the concerns. The ability to override the filter to provide access does not cure the constitutional deficiency.

The ruling in *ALA* is not directly applicable to the situation of the use of proprietary-protected filtering software in public schools. It is probable, given the environment of schools, that the standard of analysis that will be applied will be that such use must be reasonably related to legitimate pedagogical concerns and not result in viewpoint discrimination. However, the findings and analysis of the *ALA* case provide important insight into the question of the constitutionality of the use of proprietary-protected filtering software in schools.

³ *Id.* at Section ES-9 (The references in the NRC report will be to the section of the report, rather than page numbers because of the assumption that many people seeking access to more in-depth information will access to online version.)

⁴ *Id.* currently at xii.

⁵ Pub. L. No. 106-554.

⁶ *American Library Association, et. al. v. United States*, No. 01-1303 and 01-1332. In the United States District Court for the Eastern District of Pennsylvania. URL: <http://www.paed.uscourts.gov/documents/opinions/02D0415P.HTM>.

⁷ In *ALA*, the issue before the court was the constitutionality of CIPA. When courts consider the constitutionality of a federal requirement that is tied to funding, they use a 4-part analysis that was first enunciated in *South Dakota v. Dole*, 483 U.S. 203 (1987). Only one part of this analysis was relevant in the case--that was the question of whether CIPA requires libraries to violate the constitutional rights of their patrons. Therefore, it was necessary to consider whether or not the use of filtering violated the constitutional right of free speech of library patrons. For this reason, the ruling can provide insight into the issue of the use of filtering in schools violates the constitutional rights of students.

Courts generally grant significant deference to the authority of school officials to make decisions for their local school community. This deference is grounded in the perspective that the business of school is conducted in an open environment, where information about how decisions are made is readily available, and that school officials can be held publicly accountable to their local community for their decisions.

When school officials delegate authority to filtering software companies to make the determinations of what material students can and cannot access on the Internet there is no access to information about how decisions are made and there is no public accountability on the part of the company for such decisions. Such delegation of authority is made under the following conditions:

- Blocking decisions are not being made by professional educators or librarians.
- Category definitions and categorization decisions of the companies are made without reference to local community or school standards.
- Lists of blocked sites, as well as the specific methods that filtering software companies use to compile and categorize lists, including search/block keywords and blocking processes, are considered proprietary protected information.
- There is no vehicle to ensure public accountability on the part of the filtering software companies. Such companies are not subject to freedom of information/access to public records laws. Their board of directors cannot be held accountable to the citizens of a community through an election process.
- Several filtering companies have extensive marketing relationships with conservative religious organizations. Other markets for these products include repressive third world governments and employers in government and business. It is unknown how the existence of such other markets may be impacting the blocking decision-making of these companies.

Under such circumstances, the delegation of authority and abdication of responsibility by school officials will likely not be considered to be reasonably related to legitimate pedagogical concerns. This is especially true in light of the conclusions in the NRC report regarding the concerns of inappropriate reliance on technology quick fix solutions, rather than a strong focus on education and supervision. What the *ALA* court considered "less restrictive alternatives," are, in the eyes of the NRC, the foundation of an appropriate response to the concerns.

Further, there is ample evidence from multiple sources that proprietary-protected filtering software is restricting student access to materials based in inappropriate viewpoint discrimination. In some cases, such viewpoint discrimination is evident on its face--the inclusion of information related to sexual orientation in the same category as sexual technique and swinging, or the inclusion of non-traditional religious topics in the same category as Satanism. The companies may also be engaging in intentional viewpoint discrimination that would not be detectable without full and complete access to information the companies protect as proprietary.

The fact that some companies have marketing relationships with conservative religious organizations clearly provides compelling reasons to be concerned about the blocking decisions made by these companies. Finally, it is virtually certain that overzealousness and a desire to err on the side of caution on the part of employees who are making blocking decisions is resulting in the prevention of access to material based on viewpoint discrimination.

The fact that school officials can override the filter to provide access to inappropriately blocked sites does not cure the constitutional deficiencies. Given the excessive demands placed on technology staff in schools, it is simply not possible to override the filter to provide access to desired appropriate information in a timely manner. Further, students are likely to be reticent to request access to inappropriately blocked material that is controversial or sensitive in nature. Students simply do not request that the filter be overridden because they know that they can more rapidly access such material through their unfiltered Internet access at home. The students who do not have such access are being placed at a significant disadvantage.

The question of the constitutionality of CIPA is less clear. If CIPA is construed to require the use of proprietary-protected filtering software, then it is likely to eventually be ruled unconstitutional. If the requirements of CIPA are construed more liberally--to encompass the use of technologies that do not require the delegation of authority to companies that cannot be held public accountable--then CIPA may be considered to be constitutional.

The bottom line is that school officials simply cannot be allowed to abdicate their important responsibility of preparing students to use the Internet in a safe, responsible, and effective manner by placing primary reliance on technology quick fixes. And Congress should certainly be criticized for the promotion of this quick fix solution. It is vitally important for schools to develop and implement a comprehensive strategy to address these concerns. This strategy must include:

- A strong focus on the effective, educational uses of the Internet, well-supported through professional and curriculum development.
- A clear Internet use policy that is well-communicated to students, staff, and parents.
- Education to students, staff, and parents about issues related to the safe and responsible use of the Internet.
- The establishment of "safe Internet spaces" for younger students.
- Effective supervision and monitoring sufficient to deter and detect misuse.
- Appropriate educationally based discipline.

By developing a comprehensive strategy to address concerns related to the use of the Internet, educators can help young people develop effective filtering and blocking systems that will reside in the hardware that sits upon their shoulders.

Analysis of Constitutionality of Restrictions Placed on Speech

The determination of the constitutionality of government actions which place restrictions on speech, including both expressive speech and access to information, is a two-part process. The first level of analysis relates to the type of forum in which the restriction has been placed. Once the forum has been established, the court applies the appropriate rules of analysis to determine whether the restriction is constitutional.

The Supreme Court has identified three types of forum for purposes of identifying the level of scrutiny applicable to content-based restrictions on speech on government property.

1. Traditional public forum--which includes sidewalks, squares, and public parks and other locations that have traditionally been places that have been used for the purposes of public assembly, communication, and discussion. For the government to enforce a content-based restriction in a traditional public forum, it must show that its regulation is necessary to serve a compelling state interest and that it is narrowly drawn to achieve that end and are these no less restrictive alternatives. This standard is referred to as "strict scrutiny."
2. Designated (or limited) public forum--public property which the government has opened for use by the public as a place for expressive activity. The government is generally permitted, as long as it does not discriminate on the basis of viewpoint, to limit a designated public forum to certain speakers or the discussion of certain subjects. Once it has defined the limits of a designated public forum, however, any other regulations related to speech are subject to the same strict scrutiny standard of the traditional public forum.
3. Nonpublic forum--consists of all remaining public property. Limitations on speech conducted on this last category of property are evaluated under a more limited review. The regulation need only be reasonable in light of the forum as long as the regulation is not an effort to suppress the speaker's activity due to disagreement with the speaker's view, also referred to as "viewpoint discrimination."

In *ALA*, the court ruled that access to the Internet in public libraries should be considered a designated public forum. The court further noted that the provision of Internet access in public libraries "uniquely promotes First Amendment values in a manner analogous to traditional public fora."⁸ Therefore, the court found it highly appropriate to apply the strict scrutiny standard.

Analysis of Students' Constitutionally Protected Rights of Speech and Access to Information

Students in the public schools do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gate"⁹. However, the courts have recognized that the First

⁸ *ALA* at I.

⁹ *Tinker v. Des Moines Independent Community School Dist.*, 393 U.S. 503, 506 (1969).
Safe and Responsible Use of the Internet – Part III, Chapter 6, page 6

Amendment rights of students in the public schools are not the same as the rights of adults in other settings¹⁰ and must be "applied in light of the special characteristics of the school environment."¹¹ A school need not tolerate student speech that is inconsistent with its "basic educational mission."¹²

Supreme Court standards related to the importance of student access to information were eloquently set forth in the case of *Board of Education, Island Trees Union Free School District No. 26 v Pico*¹³:

"(T)he state may not, consistent with the spirit of the First Amendment, contract the spectrum of available knowledge. In keeping with this principle, we have held that in a variety of contexts the Constitution protects the right to receive information and ideas....

In our system, students may not be regarded as closed-circuit recipients of only that which the State chooses to communicate. ...[School] officials cannot suppress 'expressions of feeling with which they do not wish to contend.

(J)ust as access to ideas makes it possible for citizens generally to exercise their rights of free speech and press in a meaningful manner, such access prepares students for active participation in the pluralistic, often contentious society in which they will soon be adult members. ...

(S)tudents must always be free to inquire, to study and to evaluate, to gain new maturity and understanding. The school library is the principle locus of such freedom. ... In the school library, a student can literally explore the unknown, and discover areas of interest and thought not covered by the prescribed curriculum¹⁴.

Clearly, at this point in our society, the access to the Internet in school serves a similar, but more expansive, role to that of a school library in providing students with access to information that is vital to education and preparation for adulthood. As the court in *ALA* noted:

The architecture of the Internet, as it is right now, is perhaps the most important model of free speech since the founding. . . . Two hundred years after the framers ratified the Constitution, the Net has taught us what the First Amendment means. . . . The model for speech that the framers embraced was the model of the Internet - distributed, noncentralized, fully free and diverse¹⁵.

¹⁰ *Bethel School District No. 403 v. Fraser*, 478 U.S. 675, 682 (1986).

¹¹ *Tinker* at 506

¹² *Fraser*, *supra*, at 685

¹³ 457 US 853 (1982).

¹⁴ *Id.* at 866-896 (citations and quotations omitted).

¹⁵ *ALA* at IV.D.2. (quoting Lawrence Lessig, *Code* 183 (1999))

The lead case addressing determination of type of forum in public schools is *Hazelwood School District v. Kuhlmeier*¹⁶. This case involved a decision by a school principal to remove several articles from a student newspaper.

School facilities may be deemed to be public forums only if school authorities have 'by policy or practice' opened those facilities 'for indiscriminate use by the general public, or by some segment of the public, such as student organizations.' If the facilities have instead been reserved for other intended purposes, 'communication or otherwise,' then no public forum has been created, and school officials may impose reasonable restrictions of the speech of students, teachers, and other members of the school community.

...

(W)e hold that educators do not offend the First Amendment by exercising (control) of student speech in school-sponsored expressive activities so long as their actions are reasonably related to legitimate pedagogical concerns¹⁷.

Applying the above standard for the identification of the type of forum to the current question of the constitutionality of the use of proprietary-protected filtering software in schools requires an analysis of the manner in which schools have provided student access to the Internet.

The common practice in most public schools has been to limit student use of the Internet under terms of an Internet use policy. Generally, the terms of these policies specify that student use of the Internet should be for an educational purpose. The policies also generally include a list of types of web sites that students are not allowed to access.

However, some school districts also provide the ability of students to use the Internet for "open access" for personal or entertainment use purposes. When such non-educational use is allowed, there generally remains policy limitations on the types of sites students can access and activities students may engage in. However, this manner of use could be considered equivalent to use of the Internet in a public library. For many students, the Internet in school is their only avenue for access. Further complicating this analysis is the fact that in some regions, the school library also functions as the community's public library.

It is probable that when this issue is addressed by the courts, it will be determined that school districts have not opened use of the Internet for indiscriminate use and that issues related to student use should be considered use in the context of a non-public forum. The use of proprietary-protected filtering software would, therefore, be subject to review under the basis that the school may place reasonable restrictions related to legitimate pedagogical concerns as long as those restrictions do not result in viewpoint discrimination.

If this is the case, the ruling in *ALA* will not be directly applicable. However, many of the findings of facts and the analysis in *ALA* are certainly relevant in an analysis of the

¹⁶ 484 US 260 (1988)

¹⁷ *Id.* at 267 and 271 (citations omitted)

reasonableness of the decision of school officials to utilize proprietary-protected filtering software.

However, it is also possible to make an argument that since the terms of most Internet use policies only specify limitations related to subjects or content, that student use of the Internet in schools should be considered under the standards for a designated (or limited) public forum. This argument is particularly relevant in schools where students are allowed to engage in open access to the Internet much in the manner that they would have access in a public library and in those schools where the school library is the public library. If this is the case, then the ruling in *ALA* may be directly applicable.

Analysis of the Use of Proprietary-Protected Filtering Software in Schools Based on Designated Public Forum Standards

If student use of the Internet is determined to be use within a designated public forum, would the decision by school officials to use proprietary-protected filtering software be considered constitutional?

The recent ALA case provides guidance in the application of the strict scrutiny standards related to the use of proprietary-protected filtering software. As noted, this ruling may not be directly applicable to the situation in schools if the forum is determined to be a non-public forum. The court in *ALA* stated:

The application of strict scrutiny to a public library's use of filtering products thus requires three distinct inquiries. First, we must identify those compelling government interests that the use of filtering software promotes. It is then necessary to analyze whether the use of software filters is narrowly tailored to further those interests. Finally, we must determine whether less restrictive alternatives exist that would promote the state interest¹⁸.

The court also addressed the question of whether the ability of library officials to disable the filtering software to provide access to inappropriately blocked material would function as a cure for the limitations placed on access to constitutionally protected material by filtering software. This issue, which is relevant an analysis under either type of forum, will be addressed below.

Are there compelling interests that the use of filtering software in schools would promote?

The court in *ALA* acknowledged that the use of filtering software furthers the legitimate and compelling interests preventing adult patrons from accessing illegal material, preventing

¹⁸ *ALA* at V.

children from accessing material considered harmful to minors, and preventing patrons from being unwillingly exposed to offensive content.

It is probable that courts would find that the use of filtering software in schools furthers the legitimate and compelling interest of protecting students from the accidental and intentional access of inappropriate material on the Internet.

However, a recent study funded by the Kaiser Family Foundation, that assessed the effectiveness of proprietary-protected filtering software, presents data that calls into question reliance on such software as the means to prevent access to inappropriate material¹⁹. This study assessed the performance of the top six selling filtering products in public schools. The products were configured at a least restrictive level, an intermediate constrictive level, and a most restrictive level.

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.

Is the use of filtering software narrowly tailored to further the identified compelling interests?

The court in *ALA* determined that the use of filtering software was not narrowly tailored to further government interests. The court noted

(A)s discussed in our findings of fact, every technology protection measure used by the government's library witnesses or analyzed by the government's expert witnesses blocks access to a substantial amount of speech that is constitutionally protected with respect to both adults and minors.²⁰

While the National Research Council's report was not issued in time to be considered as evidence for the case, the court specifically noted the report in a footnote:

Although it was not proffered as evidence in this trial, (and hence we do not rely on it to inform our findings), we note *that Youth, Pornography, and the Internet*, a congressionally commissioned study by the National Research Council, a division of the National Academies of Science, see Pub. L. 105-314, Title X, Sec. 901, comes to a conclusion similar to the one that we reach regarding the effectiveness of Internet filters. The commission concludes that:

¹⁹ Rideout, V. et. al. (2002), *See No Evil: How Internet Filters Affect the Search for Online Health Information Executive Summary*. Kaiser Family Foundation URL: http://www.kff.org/content/2002/3294/Internet_Filtering_exec_summ.pdf.

²⁰ *ALA* at V.B.

All filters-those of today and for the foreseeable future-suffer (and will suffer) from some degree of overblocking (blocking content that should be allowed through) and some degree of underblocking (passing content that should not be allowed through). While the extent of overblocking and underblocking will vary with the product (and may improve over time), underblocking and overblocking result from numerous sources, including the variability in the perspectives that humans bring to the task of judging content²¹.

While not quoted in the ALA case, the NRC report also stated the following:

(F)ilters can be highly effective in reducing the exposure of minors to inappropriate content *if the inability to access large amounts of appropriate material is acceptable*²².

In various site visits conducted by the NRC committee students "often reported that information on blocked sites might have been useful for legitimate academic research purposes" and teachers reported that "educationally relevant sites were blocked regularly"²³.

The finding is also in accord with the findings of the Children's Online Protection Act Commission²⁴.

This technology (referring to server-side filtering) raises First Amendment concerns because of its potential to be over-inclusive in blocking content. Concerns are increased because the extent of blocking is often unclear and not disclosed, and may not be based on parental choices. ... There are significant concerns about First Amendment values when server-side filters are used in libraries and schools²⁵."

Subsequent to the issuance of the ALA ruling, 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 installed²⁶. As noted above, 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.

²¹ ALA at footnote 19.

²² NRC, supra at Section ES 8.

²³ NRC, supra at Section 12.1.3.

²⁴ The Children's Online Protection Act Commission was a commission established by Congress in the Children's Online Protection Act legislation. Their report is online at URL: <http://www.copacommission.org>.

²⁵ Final Report of the COPA Commission. Presented to Congress, October 20, 2000. II. B. 3.

²⁶ Rideout, supra.

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.

In sum, there is no question that the use of proprietary-protected filtering software results in the inability to access a wide range of perfectly appropriate, constitutionally-protected material, including material that is likely to be educationally-relevant but potentially controversial. Therefore, the use of filtering software cannot be considered to be a narrowly tailored restriction.

Are there less restrictive alternatives exist that would promote a school's interest in preventing student access to inappropriate material?

The court in *ALA* found there to be many less restrictive alternatives to address the concerns of adult access to illegal material, youth access to material considered harmful for minors, and the prevention of unwilling exposure to patrons:

(L)ess restrictive alternatives exist that further the government's legitimate interest in preventing the dissemination of obscenity, child pornography, and material harmful to minors, and in preventing patrons from being unwillingly exposed to patently offensive, sexually explicit content. To prevent patrons from accessing visual depictions that are obscene and child pornography, public libraries may enforce Internet use policies that make clear to patrons that the library's Internet terminals may not be used to access illegal speech. Libraries may then impose penalties on patrons who violate these policies, ranging from a warning to notification of law enforcement, in the appropriate case. Less restrictive alternatives to filtering that further libraries' interest in preventing minors from exposure to visual depictions that are harmful to minors include requiring parental consent to or presence during unfiltered access, or restricting minors' unfiltered access to terminals within view of library staff. Finally, optional filtering, privacy screens, recessed monitors, and placement of unfiltered Internet terminals outside of sight-lines provide less restrictive alternatives for libraries to prevent patrons from being unwillingly exposed to sexually explicit content on the Internet²⁷.

The NRC report goes beyond the ruling in the *ALA* case and concluded the following:

Much of the debate about "pornography on the Internet" focuses on the advantages and disadvantages of technical and public policy solutions. Technology solutions seem to offer quick and inexpensive fixes that allow adult caretakers to believe that the problem

²⁷ *ALA* at I.

has been addressed and it is tempting to believe that the use of technology can drastically reduce or even eliminate the need for human supervision. Public policy approaches promise to eliminate the sources of the problem.

In the committee's view, this focus is misguided: neither technology nor public policy alone can provide a complete--or nearly complete--solution. ... (Technology (is not) a substitute for education, responsible adult supervision, and ethical Internet use²⁸.

A reasonable reading of the NRC report leads to the conclusion that what the ALA court considered "less restrictive alternatives," are, in the eyes of the NRC, the foundation of an appropriate response to the concerns.

The NRC report contains an extensive discussion of various social and educational strategies. The NRC also published a separate report, *Nontechnical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet: Summary of a Workshop*²⁹ that specifically addresses effective nontechnical strategies.

Many of the less restrictive alternatives identified in the library setting are directly applicable in the school environment. Schools that have not installed filtering software generally report that they utilize a combination of similar approaches. Those schools also report that these less restrictive approaches are successful in addressing the issues of concern related to intentional or inadvertent access to inappropriate materials on the Internet. Further, schools that focus on the use of these educational and supervision-based alternatives are clearly preparing their students to more effectively and responsibly use the Internet, regardless of where access might occur³⁰.

These educational and supervision-based school strategies are outlined at the conclusion of this report.

Analysis of the Use of Proprietary-Protected Filtering Software in Schools Based on Non-public Forum Standards

Reasonable Restriction Related to Legitimate Pedagogical Concerns

The reasonableness standard for analysis of school restrictions placed upon speech as expressed in *Hazelwood* was:

²⁸ NRC, *supra* at Section 14.3, when the NRC refers to technology this includes more than filtering.

²⁹ National Research Council. 2001. *Nontechnical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet: Summary of a Workshop*. Board on Children, Youth, and Families and Computer Science and Telecommunications Board. Joah G. Iannota, ed. Washington D.C.: National Academy Press. The author of this document testified before the NRC Committee at this workshop. This testimony is available on the CATE and Responsible Netizen Institute sites.

³⁰ These are conclusions of the author of this report, based on extensive ongoing discussions with school officials and educators. **Safe and Responsible Use of the Internet – Part III, Chapter 6, page 13**

(W)e hold that educators do not offend the First Amendment by exercising (control) of student speech in school-sponsored expressive activities so long as their actions are reasonably related to legitimate pedagogical concerns³¹.

The question of reasonableness can be considered from a variety of perspectives.

Is the decision by school officials to use proprietary-protected filtering software reasonable in light of the fact that proprietary-protected filtering software has been found to prevent access to constitutionally-protected, educationally-relevant material and there are less restrictive, educationally-appropriate strategies that can address the legitimate concerns of student access to inappropriate material?

As the ruling in *ALA* was based on a strict scrutiny analysis, the ruling is not directly applicable to an analysis based on reasonableness standard. However, much of the discussion above is relevant to the consideration of whether the decision by school officials is reasonable.

Further, the NRC report stated:

In an educational setting, the restrictions on information flow associated with filters may lead to substantial problems with teachers and librarians who are trying to develop useful and relevant educational activities, assignments, projects, and so on. Indeed, some teachers reported to the committee during site visits that sometimes their lesson preparations were hampered by the fact that their Internet access was filtered at school. In other cases, when they prepared a lesson plan at home (with unfiltered access), they were unable to present it at school because a site they found at home was inaccessible using school computers³².

And

The use of blocking filters does not promote the development of responsible choice in children³³.

And

The committee has identified social and educational strategies to teach children and youth how to make good decisions about using the Internet as foundational to any approach to protection³⁴.

³¹ *Hazelwood*, supra at 271.

³² NRC, supra at Section 12.1.5.

³³ NRC, supra at Section 12.1.8.

³⁴ NRC, supra at Section 14.4.1.

Th sum, the NRC found that proprietary-protected filtering software is blocking access to educationally relevant material, is not promoting the development of responsible choice in students, and there are less restrictive, and more educationally appropriate, alternatives to address the concerns. These findings raise serious questions regarding whether the decision by school officials to use proprietary-protected filtering software can be considered "reasonable."

Is the decision by school officials to use proprietary-protected filtering software related to legitimate pedagogical concerns?

A finding made by the NRC may directly relate to the consideration of this issue.

In most of the schools and libraries that the committee visited, teachers, librarians, and administrators told the committee that filters played a very small role in protecting students and library patrons from inappropriate material ... Nevertheless, the school or library filter served a useful political purpose in forestalling complaints from the community about 'public facilities being used for shameful purposes.' In virtually every school the committee visited, avoiding controversy and/or liability for exposing children to inappropriate sexually explicit material was the primary reason offered for the installation of the filters.³⁵

If the primary reasons for installing filters are to avoid controversy and liability, this may be very relevant to the question of whether use of such filters is reasonably related to legitimate **pedagogical** concerns. Is preventing controversy or liability a pedagogical concern?

Is it reasonable for local school officials to delegate authority for making decisions regarding the appropriateness of information for students to proprietary-protected filtering software companies when blocking decisions are not being made by professional educators or librarians, the category definitions and categorization decisions of the companies are made without reference to local community and school standards, the lists of blocked sites, as well as the specific methods that filtering software companies use to compile and categorize lists are considered proprietary information, and when there is no vehicle to ensure public accountability on the part of the proprietary-protected filtering software companies?

The Supreme Court addressed the importance of local school control in *Pico* as follows.

The Court has long recognized that local school boards have broad discretion in the management of school affairs. ... (B)y and large, "public education in our Nation is committed to the control of state and local authorities," and that federal courts should not ordinarily "intervene in the resolution of conflicts which arise in the daily operation of school systems." ... (W)e have 'repeatedly emphasized . . . the comprehensive authority of the States and of school officials . . . to prescribe and control conduct in the schools.'³⁶

³⁵ NRC, supra at Section 12.1.1.

³⁶ *Pico*, supra.

The primary reason offered by the justices who dissented from the decision in *Pico* was deference to local school authorities. Chief Justice Burger, (with Justice Powell, Justice Rehnquist, and Justice O'Connor) stated:

We can all agree that as a matter of educational policy students should have wide access to information and ideas. But the people elect school boards, who in turn select administrators, who select the teachers, and these are the individuals best able to determine the substance of that policy. ... (L)ocal control of education involves democracy in a microcosm. In most public schools in the United States the parents have a large voice in running the school. Through participation in the election of school board members, the parents influence, if not control, the direction of their children's education. A school board is not a giant bureaucracy far removed from accountability for its actions; it is truly "of the people and by the people." A school board reflects its constituency in a very real sense and thus could not long exercise unchecked discretion in its choice to acquire or remove books. If the parents disagree with the educational decisions of the school board, they can take steps to remove the board members from office³⁷.

The election of local school board members, open meetings laws and freedom of information/access to public records laws all ensure that members of the public have full access to information regarding the decision making of local school officials and can hold these officials publicly accountable for their decisions. Private companies are not subject to any of these laws to ensure public accountability.

The following findings in *ALA* raise significant concerns related to the degree to which school officials have any knowledge whatsoever regarding what material the proprietary-protected filtering product is or is not blocking, the degree to which the blocking decisions might reflect local community standards, and the degree to which proprietary-protected filtering companies can be held publicly accountable to the local community.

The category lists maintained by the blocking programs are considered to be proprietary information, and hence are unavailable to customers or the general public for review, so that public libraries that select categories when implementing filtering software do not really know what they are blocking³⁸.

(C)ategory definitions and categorization decisions are made without reference to local community standards³⁹.

The actual URLs or IP addresses of the Web sites or pages contained in the vendors' category lists are considered to be proprietary information and are unavailable for review by customers or the general public...⁴⁰.

³⁷ *Pico*, supra.

³⁸ *ALA*, supra at I.

³⁹ *ALA*, supra at II.E.1.

⁴⁰ *ALA*, supra at II.E.1.

While the way in which filtering programs operate is conceptually straightforward ... accurately compiling and categorizing URLs to form the category lists is a more complex process that is impossible to conduct with any high degree of accuracy. The specific methods that filtering software companies use to compile and categorize lists are, like the lists themselves, proprietary information⁴¹.

The NRC report also addressed this issue:

An important consideration is the extent to which the blocking criteria are known to the user. While nearly all filter vendors provide a list of categories that are blocked, very few provide a list of all of the sites on their default "to be blocked" list, and to the committee's knowledge, no filter vendor provides a list of the objectionable words sought in keyword searches. Most companies that do not release the list of blocked sites regard such lists as intellectual proprietary and argue that the non-release protects the efforts that went into making them. However, if users of these products do not know the criteria explicitly, they will know that sites are blocked only when access to those sites is blocked and they have been told that they are blocked. Thus they cannot make an a priori determination of such filter's fitness for purpose⁴².

The issue of the inappropriate delegation of decision-making authority to filtering companies was addressed in the case of *Mainstream Loudoun v. Board of Trustees of the Loudoun County*⁴³. This case also found the use of filtering software in a public library to be unconstitutional.

The degree to which the (library's filtering) Policy is completely lacking in standards is demonstrated by the defendant's willingness to entrust all preliminary blocking decisions -- and, by default, the overwhelming majority of final decisions -- to a private vendor,... . Although the defendant argues that (the filtering product) is the best available filter, a defendant cannot avoid its constitutional obligation by contracting out its decision making to a private entity. Such abdication of its obligation is made even worse by the undisputed facts here. Specifically, defendant concedes that it does not know the criteria by which (filtering company) makes its blocking decisions. (See statement in deposition) stating that (the filtering company) has refused to provide defendant with the criteria it uses to block sites). It is also undisputed that (the filtering company) does not base its blocking decisions on any legal definition of obscenity or even on the parameters of (the library's) Policy.

The deference that courts generally demonstrate to local school officials is clearly based on the premise that school officials are exercising their own decision-making authority and can be held accountable for these decisions by the local community -- not when school officials are delegating authority to others based with no knowledge whatsoever regarding what decisions are being made, how, and on what basis.

⁴¹ ALA, supra at II.E.2.a.

⁴² NRC, supra at Section 12.1.4.

⁴³ 2 F. Supp. 2d 783 (ED Va. 1998).

No Viewpoint Discrimination

Does the use of proprietary-protected filtering software companies result in inappropriate viewpoint discrimination?

The Court in *Pico* stated:

In brief, we hold that local school boards may not remove books from school library shelves simply because they dislike the ideas contained in those books and seek by their removal to "prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion." Such purposes stand inescapably condemned by our precedents⁴⁴.

If it is not permissible for school officials to engage in viewpoint discrimination, then it is clearly impermissible for school officials to implement the use of proprietary-protected filtering software if the proprietary-protected filtering company is blocking student access based on viewpoint discrimination.

At an initial level of analysis, it must be pointed out that since the criteria, keywords used for searching, and list of blocked sites are maintained by the companies as proprietary protected information, it is simply not possible for school officials to ascertain whether or not the proprietary-protected filtering product is or is not blocking access based on viewpoint discrimination.

In considering the potential of a finding of viewpoint discrimination, the following should be considered:

The court in *ALA* noted:

Given the speed at which human reviewers must work to keep up with even a fraction of the approximately 1.5 million pages added to the publicly indexable Web each day, human error is inevitable. Errors are likely to result from boredom or lack of attentiveness, **overzealousness, or a desire to 'err on the side of caution' by screening out material that might be offensive to some customers**, even if it does not fit within any of the company's categories⁴⁵.

The NRC report noted:

While the extent of overblocking and underblocking will vary with the product (and may improve over time), underblocking and overblocking result from numerous sources, **including the variability in the perspectives that humans bring to the task of judging content**⁴⁶.

⁴⁴ *Id.* at 866-896 (citations and quotations omitted).

⁴⁵ *ALA*, supra at II.E.2.b.

⁴⁶ NRC, supra at Section 12.1.8.

And:

Filter vendors have many incentives to **err on the side of overblocking** and few to err on the side of underblocking⁴⁷.

The NRC report also referenced in a footnote, a report published by the author of this analysis. The NRC reference states the following:

Fn 28. One concern raised by analysts such as Nancy Willard is that filter vendors sometimes have strong connections to religious organizations, and that the social and cultural values espoused by these organizations may drive the vendor's characterization of inappropriate content. For example, Willard finds that most of the companies have filtering categories in which they are blocking web sites ... known to be of concern to people with conservative religious values--such as { Web sites involving] non-traditional religions and sexual orientation--in the same category as material that no responsible adult would consider appropriate for young people." She also notes that "because filtering software companies protect the actual lists of blocked sites, searching and blocking key words, blocking criteria, and blocking processes as confidential, proprietary trade secret information it is not possible to prove or disprove the hypothesis that companies may be blocking access based on religious bias." At the same time, Willard finds that while "information about the religious connections can be found through diligent search, such information is not clearly evident on the corporate web site or in materials that would provide the source of information for local school officials," and though she acknowledges openly that "it is entirely appropriate for conservative religious parents or schools to decide to use the services of an ISP that is blocking sites based on conservative religious values. It is equally appropriate for parents to want their children to use the Internet in school in a manner that is in accord with their personal family values." See Nancy Willard, 2002 *Filtering Software: The Religious Connection*, Center for Advanced Technology in Education, College of Education, University of Oregon, available online at: <<http://netizen.uoregon.edu/documents/religious2.html>>⁴⁸⁴⁹

The following are just a few examples related to concerns regarding viewpoint discrimination:

Bait and Switch

Bennett Hazelton, a young filtering opponent, conducted an enlightening study where anti-homosexual statements were directly excerpted from a variety of conservative religious sites and

⁴⁷ NRC, supra at Section 12.1.3.

⁴⁸ NRC, supra at Chapter 12, footnote 28.

⁴⁹ Unfortunately, what the NRC did not include was the author's additional point that while it is appropriate for conservative religious parents to what their children to use the Internet in a manner that is in accord with their religious values, it is entirely inappropriate for public schools to utilize a filtering product that is blocking access to material on the Internet in accord with the conservative religious values of some families. The report also addresses strategies that public schools can use to reinforce appropriate educational standards and also support those parents who want to ensure that their children are abiding by their individual family values. This can easily be accomplished by providing parents with access to their children's individual Internet usage records.

placed on new "bait" web sites. Several filtering software companies were contacted with a request to block this new site under their "hate literature" category. The companies blocked generally blocked the sites submitted to them. However, when requests were made to the companies to block the sites where the material had been originally found, such requests were denied. This demonstrates the variability of the blocking decision-making and the probability that categorization standards are not being uniformly applied. This research was reported to the COPA Commission. <http://www.copacommission.org/papers/peacefire.org/BaitAndSwitch/>

Religious Influences

Three of the proprietary-protected filtering software companies that are major providers in the school market also have or have had significant marketing relationships with conservative religious Internet Service Providers that are representing to their customers that the filtering systems are blocking access to material that is not in accord with their conservative religious values. Here are some examples:

"Your home. Your values. Your Internet.

Helping maintain LDS values when you use the Internet"

- MStar.Net logo. (<http://www.mstar.net/isp/default.htm>)

Statement made when using N2N2 filtering software, December 2001. Mstar.Net is the ISP for the Church of Latter Day Saints.

The American Family Filter is built on the Christian principal of holiness and living a pure life. ... American Family Filter stands apart from other blocking software, employing a uniquely Christian approach to our content filtering. We adhere to a higher standard, because American Family Filter is a ministry first and foremost, and therefore we are accountable to a Higher Authority for the product we produce." - Statement on American Family Filter web site (<http://www.afafilter.com/about.asp>)

Statement made when using 8e6 Technologies filtering software, December 2001. The American Family Association has now established a new division, BsafeOnline (<http://bsafeonline.com>) which is marketing filtering services to schools.

"Upholding Biblical standards. We use a sophisticated server-based filtering process to eliminate objectionable material. ... We filter out the standard offensive material - pornography, profanity, and violence.

In addition, we uphold our own set of standards...Biblical standards."

- Statement on 711.Net web site, December 2001.

(<http://www.711online.net/filterphilosophy.htm>)

Statement made when using Symantec filtering software.

Category Descriptions

The existence of viewpoint discrimination is also apparent in the category descriptions provided by the some of companies. The problem presented by these categories is that material that would likely be considered to be appropriate and constitutionally-protected is included in categories

with material that is not likely to be considered acceptable for students to access. Virtually all companies have similar categories, the categories that appear to be most likely to block material based on viewpoint discrimination include sex related categories--blocking information on safe sex and sexual orientation, occult--blocking information on non-traditional religions, hate literature--blocking political speech, and anarchy/violence--blocking political speech. The following are some examples:

Sex Education / Sexuality

Sites dealing with topics in human sexuality. Includes sexual technique, sexual orientation, cross-dressing, transvestites, transgenders, multiple-partner relationships, and other related issues."

(<http://service4.symantec.com/SUPPORT/igear.nsf/pfdocs/2000110911532640>)

Symantec's category description includes material on sexual orientation in the same category as sexual technique and swinging.

Anarchy

Sites contain information regarding militias, weapons, anti-government groups, terrorism, overthrowing of the government, killing methods, etc."

(<http://www.8e6technologies.com/solutions/categories.html>)

8e6 Technologies blocking category. If this description were used to block access to information in the late 1700's, the Declaration of Independence and all other writings of the Founding Fathers would be blocked. IS this company also blocking access to President Bush's arguments supporting a regime change in Iraq?

21. Religion

21.1 Non-Traditional Religions. Sites that provide information on or promote religions not listed in 21.2 and on other unconventional religious or quasi-religious subjects, including cults.

21.2 Traditional Religions. Sites that provide information on or promote Buddhism, Baha'i, Christianity, Christian Science, Hinduism, Islam, Judaism, Mormonism, Shinto, and Sikhism; also atheism.

<http://www.websense.com/products/about/database/categories.cfm>

Websense's category for non-traditional religions includes protected religious subjects in the same category as cults. Virtually all of the filtering products have some form of a cult/occult/new age category that appears to be blocking non-traditional, and clearly constitutionally protected religious sites along with cults and Satanism.

Sex (sx).

This category contains URLs that reference, discuss, or show pornography, including pictures, videos, or text of sex acts, or sexually oriented material. This includes soft- and hard-core pornography, sado-masochism, bestiality, and so on. ...

Note: In the broader context of cultural norms and individual taste, it may be debatable what is considered sex or pornography or simply a form of entertainment, but in a standard business setting, URLs of this nature are non-business related and are considered unproductive for most employees to view during working hours.
<http://www.securecomputing.com/index.cfm?sKey=86>

Secure Computing's category description provides clear evidence of the lack of attention to educational standards. If the company is using work-place standards, then it is highly probable that sexual education material that would be appropriate for students is also being blocked.

Intolerance.

Pictures or text advocating prejudice or discrimination against any race, religion, gender, disability, or sexual orientation including intolerant jokes or slurs.
<http://www.surfcontrol.com/education/support/cybernot.asp>

This is SurfControl/Cyberpatrol's blocking category. Reportedly, the company is blocking access to the American Family Association web site under this category based on the presence of anti-homosexuality materials. http://www.afa.net/homosexual_agenda/principles.asp.

Kaiser Study

A close analysis of the data reveals blocking patterns that present significant concerns of viewpoint discrimination. While at the least restrictive level only 1.4% of all health sites were blocked, 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.

At the intermediate restriction level, typical of most school settings, the filters blocked potentially controversial health information sites at the following levels: ecstasy (drug education sites)—24.9%, safe sex—20.5%, condoms—27.7%, gay—24.6% and lesbian-17.1%.

At the most restrictive level, includes categories that some districts are blocking, the filters blocked potentially controversial health information sites at the following level: ecstasy (drug education sites)—36.2%, safe sex—50.0%, condoms—55.4%, pregnancy—31.6%, birth control—34.7%, abortion—44.6%, gay—59.9% and lesbian-59.0%. (Reporting only those categories with blocking rates over 30%.)

Clearly there is a significant base of evidence to demonstrate concerns that the use of filters is resulting in unacceptable viewpoint discrimination by preventing access to sites containing material that is controversial.

Overriding the Filter

Does the ability to override the filtering software to provide access to inappropriately blocked material cure the constitutional deficiencies in the technology?

The court in *ALA* noted the following:

The Supreme Court has made clear that content-based restrictions that require recipients to identify themselves before being granted access to disfavored speech are subject to no less scrutiny than outright bans on access to such speech.

...

By requiring library patrons affirmatively to request permission to access certain speech singled out on the basis of its content, CIPA will deter patrons from requesting that a library disable filters to allow the patron to access speech that is constitutionally protected, yet sensitive in nature.

...

(T)he requirement that a patron take the time to affirmatively request access to a blocked Web site and then wait several days until the site is unblocked will, as a practical matter, impose a significant burden on library patrons' use of the Internet.

...

Even if CIPA's disabling provisions could be perfectly implemented by library staff every time patrons request access to an erroneously blocked Web site, we hold that the content-based burden that the library's use of software filters places on patrons' access to speech suffers from the same constitutional deficiencies as a complete ban on patrons' access to speech that was erroneously blocked by filters, since patrons will often be deterred from asking the library to unblock a site and patron requests cannot be immediately reviewed⁵⁰.

This portion of the *ALA* decision is directly applicable to the situation in schools. School officials may want to take the position that they have retained local control because if a student wants to access material that has been inappropriately blocked, the student may request an override of the system. This position is not likely to withstand legal review.

If constitutionally protected material is being blocked based on inappropriate viewpoint discrimination of the filtering company, such material may be sensitive or controversial in nature. It would likely be considered unacceptable to place a burden on students who desire access to information that may be sensitive or controversial in nature to come forward to request access to such material.

In many cases, students are disinclined to request an override because of lack of access to information regarding why a particular site has been blocked. When a student is blocked from accessing a site, the student has no ability to ascertain whether or not the site contains material

⁵⁰ *ALA*, *supra* at V.D.

that should be blocked. Absent such insight, it is improbable that a student will request the filter to be overridden for fear of requesting access to an entirely inappropriate site.

Additionally, in most schools, the process of requesting access is overly burdensome and the time delay between when the information is sought and when an override can be accomplished significantly interferes with the effective use of such material for educational purposes.

Constitutionality of The Technology Protection Requirements of the Children's Internet Protection Act

The issue of the constitutionality of the technology protection measures requirements of CIPA in public schools is not clear. The discussion above addresses the question of the constitutionality of the use of proprietary-protected filtering software, which is how the vast majority of public school districts have responded to the requirements of CIPA.

The issue of the constitutionality of the public schools provisions of CIPA will be resolved by a determination of whether or not CIPA actually requires the use of proprietary-protected filtering software. In *ALA*, the expert testimony from both sides focused solely on the operations of four of the top-selling proprietary-protected filtering software products. The court discussed the issue of whether other technologies could be used that would meet the statutory requirement but would be more narrowly tailored to avoid restricting access to constitutionally protected material. The court noted:

As detailed in our findings of fact, any filter that blocks enough speech to protect against access to visual depictions that are obscene, child pornography, and harmful to minors, will necessarily overblock substantial amounts of speech that does not fall within these categories.

This finding is supported by the government's failure to produce evidence of any filtering technology that avoids overblocking a substantial amount of protected speech. ...

Thus, it is the government's burden, in this case, to show the existence of a filtering technology that both blocks enough speech to qualify as a technology protection measure, for purposes of CIPA, and avoids overblocking a substantial amount of constitutionally protected speech.

Here, the government has failed to meet its burden....

(W)e conclude that any technology protection measure that blocks a sufficient amount of speech to comply with CIPA's requirement that it "protect[] against access through such computers to visual depictions that are - (I) obscene; (II) child pornography; or (III) harmful to minors" will necessarily block substantial amounts of speech that does not fall within these categories.

Not wishing to undermine the very excellent analysis presented by the court in the ALA ruling, an argument can be made that from the perspective of schools, for which the restrictions on speech would likely be addressed under the non-public forum standard, there are alternative technologies that could be used to comply with the CIPA technology protection requirements that would not result in overblocking. The use of these technologies would not be appropriate in a public library because of the need to provide more open access to the Internet than is necessary in a public school and because of concerns regarding privacy of the library patrons—the privacy standards for students are very different than the privacy standards for library patrons.

The argument for the ability for schools to use alternative technologies to comply with the CIPA technology protection measures requirements is as follows:

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; ...⁵¹

TECHNOLOGY PROTECTION MEASURE.--the term 'Technology Protection Measure' means a specific technology that *blocks or filters* Internet access to (the prohibited material)⁵².

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. But the generic use of this term may not be what Congress had in mind. The specific terms of the statute are "blocks or filters." Filtering software functions by blocking. If schools are required to use products that block, then there is no reason for the use of both terms within the statute. The term "filter" could also be construed to mean "sort" or "analyze."

The statute also uses the terms "protect against access" not "prevent access." Presumably, therefore, any technology that either analyzes traffic or blocks traffic and is used for the purpose of protecting against access to inappropriate material could 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--

⁵¹ 47 U.S.C. 254 (h)(5)(B)

⁵² 47 U.S.C. 254 (h)(7)(I)

- (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, school board, local educational agency, library, or other authority in the administration of subsection (h)(1)(b)⁵³.

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 proprietary-protected filtering software, which does not allow for local determination of content, would meet the requirements of the law.

Senator John McCain, sponsor of the CIPA legislation has suggested the following:

Tuesday, March 20, 2001

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:

... 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 access⁵⁴.

The FCC also address 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

⁵³ 47 U.S.C. 254 (1)(2)

⁵⁴ URL: <http://mccain.senate.gov/intfilt01.htm> (emphasis added)

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.⁵⁵

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.

The NRC committee was charged under its implementing legislation with the task of conducting a study of "computer-based control technologies" and other approaches to address the concerns of pornography on the Internet⁵⁶. The NRC committee conducted a full study of various technologies that, in their words, "can be used to *protect* or limit children's exposure to inappropriate sexually explicit material on the Internet⁵⁷." Note the use of the term "protect," which is the same term used in the CIPA legislation.

Alternative Technology Protection Measures

Chapter 12 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 CIPA⁵⁸.

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	Can be configured to deny access to substantial amounts of adult-oriented sexually-explicit	In typical (default) configuration, generally denies access to substantial amounts of Web	Protects against both deliberate and inadvertent exposure for sites that are explicitly blocked; can be circumvented

⁵⁵ FCC, *supra*.

⁵⁶ P.L. 105-314, the *Protection of Children from Sexual Predators Act of 1998*, Title IX, Section 901.

⁵⁷ NRC Report, *supra* at Section 11.3.

⁵⁸ With the exception of Instant Help, which the NRC indicated was an after-the-fact solution.

	also block generic access to instant messages, e-mail, and chat rooms	material from commercial web sites	material that is not adult-oriented and sexually explicit.	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 content raters can be used	Effectiveness depends of broad acceptance of a common labeling framework	Likelihood of exposure depends on accuracy of labels given by labeling party
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

The following are the kinds of technology protection measures that could presumably be used by public schools to comply with CIPA which could be integrated into a more comprehensive education and supervision approach to address the concerns. The additional necessary components of a comprehensive approach are discussed below.

As discussed above, the primary reason for concerns about the constitutionality of the use of proprietary-protected filtering software is the lack of local control and public accountability due to the information about blocking decision-making that is kept confidential.

Technology Protection Measure Options

There are technology protection measures that function in a manner provide for local control and public accountability that should not result in excessive overblocking. The technological options appear to include:

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 sites⁵⁹. Here is what NRC had to say about ICRA:

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 providers⁶⁰.

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.

These products may not be as robust as the proprietary-protected products, they are 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

⁵⁹ <http://www.icra.org>.

⁶⁰ NRC Report, *supra* at Section 12.1.5.

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:

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 assistance⁶¹

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 an 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,⁶²)

⁶¹ NRC Report, supra at Section 12.1.6.

⁶² NRC Report, supra at Section 12.1.1.

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.
- Proxy 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 a non-profit education service or 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 Internet⁶³.

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 material⁶⁴. Clearly monitoring should be considered a technology that meets the CIPA requirements for a technology protection measure. Further, the NRC section that addresses monitoring includes a footnote⁶⁵ 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 met⁶⁶."

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 action⁶⁷.

Clearly, to fulfill its role as a motivation for deterrence, clear notice of the existence of monitoring is critically important. If appropriately, the use of monitoring technologies can fit into existing legal principles of school privacy and search and seizure. However, there are significant concerns about inappropriate invasion of privacy or inappropriate discipline of students for accessing controversial, yet educationally relevant material.

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

⁶³ NRC Report, *supra* at Section 12.2.1.

⁶⁴ 47 U.S.C. 254 (h)(5)(B).

⁶⁵ NRC Report, *supra* at Section 12.2 (footnote 38).

⁶⁶ 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.

⁶⁷ NRC Report, *supra* at Section 12.2.2.

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.

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.

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. This technology would not meet the requirements of CIPA because it neither analyzes nor limits access. In schools, "instant help" should be in the form of a "real world" caring, knowledgeable teacher.

*Comprehensive Strategy to Support the Safe and Responsible Use of the Internet by Students*⁶⁸

The NRC committee found:

Virtually all of the high school students to whom the committee spoke said that their 'Internet savvy' came from experience, and they simply learned to cope with certain unpleasant Internet experiences. They also spoke of passing their newfound expertise down to younger siblings, hence becoming the new de facto educators for younger kids in the 'second wave of digital children'⁶⁹.

⁶⁸ The strategies presented in this document are more fully addressed on the author's web site: URL: <http://responsiblenetizen.org>.

⁶⁹ NRC Report, supra at Section 14.3.

The misplaced reliance on filtering technologies by educators, parents, and decision-makers and the resulting failure to teach important safety skills is resulting in a need for our children to learn about Internet safety and the avoidance of inappropriate material through "trial and error." This is an unacceptable state of affairs.

Regardless of what ultimately happens in the courts with respect to CIPA or the assessment of the constitutionality of the use of proprietary-protected filtering in schools, the best advice for school districts is to shift their reliance from proprietary-protected filtering technologies to a more comprehensive approach that focuses on education and supervision.

The development of strategies to address issues of concern regarding the use of the Internet by young people must be grounded in knowledge of effective parenting and educational strategies. Parents and educators already know a great deal about helping young people learn to engage in safe and responsible behavior.

When children are too young to comprehend the dangers, to understand the expectations for their behavior, and to independently engage in safe and responsible decision-making, we keep them in safe places and supervise their activities. We keep them in fenced play yards. When we take our children to places that may be less safe, such as a public park, we even more closely supervise their activities. We also use these public excursions as opportunities to teach our children. We teach them about potential dangers, how to recognize dangerous situations, and what actions to take to keep themselves safe. We introduce these lessons with an understanding of the cognitive development and sensitivities of their age.

We also teach children about our positive expectations for their behavior. We teach them about respect for others and actions that are necessary to support the good of the community. And if they engage in unsafe or irresponsible behavior, we intervene with appropriate discipline. We use transgressions as "teachable moments" to review and reinforce the lessons of safe and responsible behavior.

As children grow, we allow them increasing freedom. We do not expect that teenagers will be satisfied remaining in fenced play yards. But we remain engaged. We know that young people who have parents and other influential adults who remain "hands-on," through active involvement, ongoing communication, and supervision, are much less likely to engage in unsafe or irresponsible behavior.

New issues related to potential dangers and expectations for behavior emerge. Issues that would not have been appropriate to address when a child was younger, such as date rape, become important issues to address at this age. We use the same pattern of instruction -- providing information about the issue of concern, how to recognize a situation presenting the concern, and how to effectively respond to the situation.

In sum, helping children and teenagers learn to engage in safe and responsible behavior involves imparting:

- Knowledge about potential dangers or concerns and expectations or standards for responsible behavior.
- Effective decision-making skills that include being able to recognize situations presenting concerns and knowing appropriate or effective responses to such situations.
- Motivation to behave in a safe and responsible manner.

How do these basic lessons in raising safe and responsible children translate to the Internet? First and foremost, we have to recognize that even though we may be accessing the Internet from the safety of a classroom or family room, the Internet is very much a public place. Allowing young children to have supervised, open access to the Internet (filtered or not) without close supervision would be the equivalent of leaving a child to play unsupervised in New York City's Central Park. Older children need to have the knowledge and skills to make safe and responsible choices in these public places.

Children who are in elementary school are too young to be fully informed about Internet dangers and should not be expected to be able to engage in safe behavior in unsupervised environments. Children's use of the Internet should be almost exclusively in "safe Internet spaces"-- environments that provide access to only pre-reviewed appropriate sites. Their use of electronic communications should likewise be in safe communication environments.

If it is necessary for elementary age children to use the open Internet, they should do so only in highly structured environments with close over-the-shoulder supervision. These experiences provide the opportunity to introduce important safety skills.

There is one vitally important safety skill that all children should be taught prior to using the Internet, even in safe environments. All children should know that there is "yucky" stuff on the Internet that, through no fault of their own, may appear on the computer screen. Children should know that if "yucky" material ever appears on their screen, they should immediately turn off the screen (the process to do this may vary depending on the computer system) and tell a teacher or their parent.

When students are in middle school and high school, access should be more open and the focus should shift to instruction on basic safety skills, supervision, monitoring, and responsive discipline. The primary *protection* at this point should be the student's own skills and motivation. It is also important for adults to remain "hands-on"—keeping an eye on where the teen is going online, who the teen's online friends are, and what the teen is doing in the online environment, intervening if necessary, and, most importantly, being available for discussion, without overreacting, if the teen experiences difficulties. In the teen years, the focus must shift to the importance of making choices on the Internet that are in accord with the teenager's emerging sense of personal identity and moral values.

Components of a Comprehensive Strategy

A comprehensive education and supervision strategy is developed in accord with these basic principles. This strategy includes the following components:

- Place a strong focus on the effective educational use of the Internet. When students are actively engaged in exciting Internet learning, the opportunities and inclinations for misuse are significantly reduced. The foundation for this strong educational focus is professional development and curriculum development.
- **Enact a comprehensive Internet use policy that addresses issues related to the use of the Internet and provides the foundation for educational program addressing the safe and responsible use of the Internet. Additional information on the components of this policy is below.**
- Follow a strategy that reflects an understanding of the age and understandings of the students. The focus for elementary students should be on limiting access to safe Internet places for accessing information and communicating. Elementary students do not have the knowledge or skills to adequately protect themselves on the open Internet. By middle school, the strategy should shift. Students of this age are freely using the Internet from a variety of locations. The focus should be on comprehensive education and effective supervision and monitoring that is sufficient to detect and respond to instances of misuse.
- Provide comprehensive education to staff, students, and parents regarding safe and responsible Internet use issues and skills, as appropriate to their age and understanding. This education should prepare students to independently protect their personal safety when using the Internet, respond effectively to Internet concerns, and abide by their responsibilities as "Cybercitizens." Incorporate Internet safety issues into other curriculum areas, such as addressing online predation in sex education classes.
- Develop or utilize an educational web site that channels student use to sites that have been reviewed by educators, librarians, and other professionals and have been determined to present accurate, educationally relevant information in an appropriate manner. Limit elementary students access to these pre-reviewed educationally appropriate sites unless they are being closely supervised by the teacher. Direct or channel secondary students to such sites, while allowing for open access when necessary and appropriate.
- Established a safe electronic communication system that promotes communication for educational purposes only.
- Establish supervision and monitoring systems that ensure accountability. Students and staff should know that they have limited privacy in their Internet use through the school system. Offer parents the ability to have access to the Internet records of their children so that they can assure themselves that their children are using the Internet at school in accord with their family values.

- Respond with appropriate discipline in the event of misuse, using such instances as "teachable moments." Additionally, review instances of misuse to reevaluate the district's approach.
- Use a variety of technologies to support this comprehensive approach, including technologies that block access to sites that have rated themselves as sexually explicit or inappropriate for minors, technologies that limit or guide students to educationally appropriate sites, technologies that protect against unwanted commercial or pornographic electronic communication, and technologies that facilitate effective monitoring of student use.

Components of an Internet Use Policy

The requirements set forth in NCIPA for the development of an Internet Safety Plan provide an excellent outline for the key issues that should be addressed in a district Internet use policy⁷⁰. As noted above, the district policy should provide the foundation for the district's educational efforts.

- **Inappropriate Material**

The district Internet use policy should clearly define what kinds of material are considered to be inappropriate in school. It is recommended that three categories of material be identified:

Prohibited Material should not be accessed by the students or staff at any time, for any purpose. This material includes material prohibited under CIPA, as well as other material considered to be inappropriate by the district.

Restricted Material may be accessed by high school students only in the context of specific learning activities that have been approved by teachers or by staff for legitimate research or professional development purposes. (E.g., access to hate literature in the context of study of discrimination.)

Limited Access Material is generally considered to be non-educational or entertainment, but may be accessed in the context of specific learning activities or during "open access" times.

- **Safe and Security of Students When Using Electronic Communication**

The district should address this by establishing or using safe electronic communication environments, limiting the use of electronic communications to educational purposes, and providing instruction in privacy and communication safety standards.

- **Unauthorized Access and Other Unlawful Online Activities**

⁷⁰ 47 U.S.C. 254(l)(1)(A))

The district Internet use policy should address issues of illegal and unethical Internet use, including computer security, copyright infringement, plagiarism, and harmful speech.

- Unauthorized Disclosure, Use, and Dissemination of Personal Information Regarding Students

District should have policies addressing staff and student requirements related to personal information which address the protection of student privacy under any relationships with third parties on the Internet, staff disclosure of student confidential information, and student disclosure of personal information of others or self.

District Checklist for the Development of a Comprehensive Safe and Responsible Internet Use Plan

The following checklist provides a vehicle for educators to evaluate their current district status and a guide for the development of policies and procedures to more effectively address the safe and responsible use of the Internet by students. The intention in the development of this list was to create a guide for planning and assessment. This is a comprehensive list. Districts may decide that it is not necessary, or not possible to accomplish everything on the list. Some of the items are repeated because they relate to general issues as well as to issues within a particular category.

This document is provided online at: <http://responsiblenetizen.org>. It can be downloaded to facilitate reformatting for use in planning.

It is recommended that districts address the items on this checklist with the following questions:

- What are we doing to address this issue?
- Do we need to be doing something more to address this issue?
- If we need to be doing more,
 - What should we do,
 - Who should be responsible,
 - What resources should be provided, and
 - How will we assess the effectiveness?

Education Purpose

Activities that provide the foundation for the effective educational use of the Internet for educational purposes.

- Policy provisions that specify appropriate educational activities.
- Clearly define circumstances when it is permissible for students to use the Internet for entertainment or non-educational purposes (may be on a school basis).
- District provides technical skills training for staff. Staff are becoming technically proficient.

- District provides professional development for teachers and administrators on use of the Internet to assist students in achieving curriculum objectives. Teachers and administrators are increasing their understanding and skills in the effective use of the Internet to support curriculum objectives.
- District has created or is facilitating access to Internet-based lesson plans that support use of the Internet to assist students in achieving curriculum objectives.
- District web site provides links to pre-reviewed educational resources
- Teachers have the knowledge and skills to create classroom/lesson web sites with links to Internet resources (if teachers do not have knowledge/skills, technical support is provided to facilitate the timely creation of such sites).
- Technical support is provided at an adequate level.
- Instructional support systems, such as mentoring and electronic communication environments to support instructional/educational activities, have been established.
- District periodically evaluates web usage logs to determine degree to which Internet is being used for high quality educational activities.
- District distance education programs meet standards for disability access.

Education about Safe and Responsible Use of the Internet

Activities that prepare students, teachers, and administrators to use the Internet in a safe and responsible manner.

- Students have been educated about requirements of District Internet Use Policy. Secondary students demonstrate understanding of the Policy prior to receiving individual account on the system.
- Parents have received information about District Internet Use Policy and strategies to address concerns at home.
- Parent Internet use classes are offered.
- Students receive instruction related to safe and responsible use of the Internet in a manner appropriate to grade level and Internet usage.
- Teachers and administrators receive instruction related to safe and responsible use of the Internet.
- Internet safety and responsible use instruction for students and staff includes:
 - Avoiding unintentional access (effective search skills, URL porn-napping).
 - **Dealing with accidental access (getting out of mouse-traps reporting).**
 - Recognizing and dealing with unwanted SPAM.
 - Communication safety skills (protection of privacy, recognizing predators, reporting predators, protecting friends).
 - Protection of privacy (personal privacy, privacy of others, privacy on commercial sites).
 - Harmful speech (defamation, harassment, violation of privacy, abusive language, flame wars, etiquette, recognizing harmful speech/hate sites, consequences for offenders, effective victim responses).
 - Responsible speech -- free speech rights, effective online advocacy, disability IT access.
 - Copyright (rights and responsibilities).
 - Plagiarism.

- Computer security (unlawful computer activities).
- Network security and resource limits (passwords, viruses, quotas, downloads, group lists, etc.)
- Online addiction (sexual, violent games, gambling).
- District is addressing issues that are underlying Internet concerns in appropriate classes. Curriculum objectives for courses include:
 - Sex education classes: Internet pornography, predation, online addiction.
 - History and social science: online hate/harmful speech, free speech/responsible speech.
 - Information literacy and copyright throughout curriculum.
 - Writing instruction: copyright and plagiarism.
 - Technology classes: technology ethics, computer security.

Supervision and Monitoring

Establishment of an environment where student misuse of the Internet will be detected and addressed.

- Secondary students log onto Internet system with a unique student identifier that allows for determination of identity of student.
- Internet usage logs retained in manner that facilitate monitoring and provision of student usage logs to parents.
- Expectation has been communicated to staff that student use of the Internet will be supervised in a manner appropriate to age and circumstances of use.
- Elementary staff understand that no student should have access to open Internet unless there is close, over-the-shoulder supervision by the teacher.
- Building administrators, or designee conduct annual review of placement of all computers to facilitate effective supervision.
- District/schools have established a technical monitoring system that is appropriate in accord with the circumstances of the school (relates to size of school, number of computers, etc.).
- Parents have been informed of their right to receive their child's Internet use records.
- E-mail traffic and web usage volume is tracked to detect excessive use that may be the result of misuse.
- District has established record retention process in compliance with state public records laws.
- Staff have been informed of impact of state public access laws.
- Students have been fully informed of all district monitoring and parents right to access all Internet usage records.

Discipline

The district's disciplinary approach reinforces the importance of using the Internet in a safe and responsible manner.

- Administrators have received professional development in issues related to administrative concerns when addressing student online behavior, including issues of district liability, due process, and addressing harmful online speech on and off campus.

- Incidents of misuse result in a "teachable moments" for offending students.
- Incidents of misuse are evaluated by Technology Committee to guide policies and procedures.
- Issues related to incidents of misuse are addressed in educational efforts.

Access to Inappropriate Material

Concerns related to the potential of student access to inappropriate material.

General

- District has developed a Policy that addresses in clear and unambiguous language what material is considered inappropriate for students to access.
- Determination of what material is and is not considered appropriate has been developed in accord with constitutional standards related to students' rights of access to information.
- District has Policy that allows for access to certain restricted material in the context of appropriate educational activities (access hate literature to study hate literature)
- District (or school) has Policy that specifies when students may use the Internet for entertainment purposes.
- District encourages students to use the Internet in accord with family values and provides parents with access to their child's records.

Elementary Students

- District has established a safe Internet space (district web site with pre-reviewed sites) for elementary students.
- Elementary teachers understand that any access to the open Internet must be closely supervised.
- Elementary teachers know how to create a class/lesson web site and add links to the district site (if teachers do not have these skills, support is provided).
- Classroom e-mail accounts or other form of protected electronic communication facilities have been established for student electronic communication.

Secondary Students

- District is providing instruction in:
 - Prohibitions and standards related to inappropriate material set forth in Policy.
 - Strategies to avoid access to inappropriate material (search methods, problems with porn-napping)
 - Appropriate responses in the event of mistaken access inappropriate material (responding to mouse-trapping, need to report).
 - The manner in which the district is monitoring student use and activities that will provide the foundation for a "reasonable suspicion" that will justify an individualized search of student's usage records.
 - Parent's rights to receive access to student usage logs and e-mail files.

Technology Protection Measure

The following are technology approaches that do not require use of proprietary-protected filtering software. These approaches will result in under-blocking and thus the ability of students to inadvertently or intentionally access inappropriate material. Therefore, the following approaches should only be used in context of a comprehensive strategy that includes safe space for elementary students and education/monitoring of secondary students, such as outlined in this document.)

Options:

- Install blocking system that provides complete information regarding criteria, processes and an actual list of all blocked sites.
- Use the Internet Content Rating Association technology, which blocks access to sites that have rated themselves as inappropriate for youth.
- Use a filtered monitoring program that will filter all Internet traffic and report instances of potential misuse.
- Use a spam filter, if spam is a concern in electronic communication facilities.

Safety and Security when Using Electronic Communication

Addressing the safety and security of students when they are using electronic communications.

- Policy includes provisions addressing personal privacy, respecting privacy of others, required disclosure of inappropriate messages, warning that excessive e-mail use can constitute grounds for reasonable suspicion that the student may be misusing the Internet service, and warning that the students' parents can have access to e-mail files.
- Students receive instruction in all of the above as appropriate for grade level and level of access.
- District has established an electronic communication environment that is protected and facilitates access for appropriate monitoring (i.e. not Hotmail or Yahoo).
- Elementary students use electronic communications in safe environments with total teacher access -- class account, monitored account, or the like.
- Secondary students receive individual accounts only after participating in training regarding communication safety and requirements of district Policy.
- Individual student accounts are established with unique student identifier that disguises students' real names.
- District has established a Policy to review e-mail use to detect excessive use that may indicate inappropriate use. (Or district uses filtered monitoring to detect instances of possible misuse.)

Responsible and Legal Use Issues

Promoting the responsible and legal use of the Internet.

- Policy includes provisions that address: computer security, use of district system to commit unlawful acts, harmful speech, copyright, plagiarism, network security and resource limits (passwords, viruses, quotas, downloads, group lists, etc.)

- Students and staff receive instruction in all of the above, as appropriate for grade level/position.
- District has established network protection processes and provided information to staff and students about responsibilities.
- District conducts network review to detect excessive or inappropriate use that may indicate inappropriate use.
- The district has established a program to reduce plagiarism:
 - District's curriculum objectives and writing instruction program has been designed to assist students in learning how to write effectively without engaging in plagiarism.
 - Teachers assign writing projects in a manner that reduces the incentive or likelihood that students will engage in plagiarism.
 - Teachers seek to detect and effectively address incidents of plagiarism. (Punishing students for engaging in plagiarism is not acceptable unless the district has provided the necessary education in effective writing to avoid plagiarism.)

Unauthorized Use, Disclosure, or Dissemination of Personal Information of Students

Addressing the protection of student personal information.

- All contracts and agreements with third party companies accessed through the web are reviewed to assess compliance with federal and state laws and district policies related to the protection of student personal information.
- The district has established an effective process to manage the disclosure of student information/work or photographs of students on the district web site. Parental permission is obtained prior to any disclosure.
- District has established a process to manage the transmission of confidential student information via staff e-mail and has communicated to staff the requirements for such transmission.
- Policy prohibits students from distributing personal information of other students in an e-mail or elsewhere on the Internet.
- Policy prohibits students from disclosing personal information regarding self in e-mail or elsewhere except for specifically approved situations (e.g. disclosure by high school students for continuing education, job search, etc.)
- District prohibition against the establishment of student accounts on third party systems unless there is a clear educational purpose, no collection of student information for consumer market research purposes, and parents have been informed and approve.