

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

1. District Liability Related to Access to Inappropriate Material or People

Avoiding Liability and Controversy

Far too many school districts have installed filtering software thinking that such measures are necessary to protect the district against liability. Many filtering software companies use fear of litigation as a marketing tool. An example from the marketing literature for one such product reads:

Protect your school from legal liability

Letting students or staff surf anywhere on the internet may lead them to stray to inappropriate sites. This kind of activity can lead to lawsuits, harassment charges, and even criminal prosecution. Protect your students and your school by promoting intelligent Internet use¹.

The *NRC Report* noted the degree to which avoidance of liability and controversy was the motivating factor for the use of filtering.

While filters are designed to reduce children's access to inappropriate material on the Internet, there are some interesting psychological and social phenomena related to their use. 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 users from inappropriate material, large because most of these students and library users had unfiltered Internet access somewhere else (usually at home). ... 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 filters².

Statutory Immunity

Although there are no cases directly on point it is probable that schools will enjoy statutory immunity for harm if a student accesses material placed by a third party on the Internet. This immunity was established through a section of the Computer Decency Act of 1996³. Other sections of the Computer Decency Act were ruled unconstitutional, however, this section remains in force and has been upheld in a number of court cases. §230(c)(1) provides:

- (1) TREATMENT OF PUBLISHER OR SPEAKER- No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

As to whether an education institution offering Internet access to its students is an "interactive computer service", the question is directly addressed by §230(e)(2):

The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by *libraries or educational institutions*⁴.

¹ From the SurfControl brochure for CyberPatrol. When the I received a copy of this brochure at the 2001 NECC Conference, I questioned the SurfControl staff about these assertions. The staff indicated that they were not aware of any district that had been found liable for misuse of the Internet. To include such statements in the brochure absent any evidence of potential liability raises concerns of false or misleading advertising.

² *Id.* at 12.1.2 (footnotes omitted).

³ 47 U.S.C.A. §230(c)

⁴ Emphasis added.

§230(d)(3) provides:

- (3) STATE LAW- Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

In sum, §230(c)(1) provides that an "interactive computer service" is not to be treated the same as a content provider; §230(e)(2) provides that an education institution offering Internet access is an interactive computer service; and §230(d)(3) provides that inconsistent state laws may not be used as a basis of liability.

The word "immunity" is not in the statute itself. But in *Zeran v. America Online, Inc.*,⁵ the Fourth Circuit Court of Appeals expressly held that "[b]y its plain language, §230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service⁶."

In a more applicable case, *Kathleen R. v City of Livermore*⁷, a mother of a teenage boy sued the library because her son had accessed sexually explicit pictures through the library's Internet service. The City made two arguments based on §230. The first argument was that §230 provides federal immunity from liability to service providers for the speech of third-party content providers. The second argument was that in enacting §230, Congress preempted any state law which may be to the contrary. The action was dismissed. The dismissal was upheld on appeal⁸.

The appellate court found that under CDA, the library was an interactive service provider and was entitled to immunity under §230(c)(1). The court noted that although the purpose of CDA was to prevent minors from getting access to pornography, Congress made a deliberate policy choice not to subject those providing Internet access to tort liability.

Impact of CIPA

On its face, there is no language in CIPA that would establish liability of a school district. The liability issue was raised during the FCC proceedings in the development of CIPA regulations. Here is the pertinent section of the FCC Order discussing this issue:

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

⁵ 129 F.3d 327 (4th Cir. 1997)

⁶ *Id.* at 330.

⁷ Cal. Ct. App., 1st App. Dist., A086349, 3/6/01)

⁸ URL: <http://www.techlawjournal.com/courts/kathleenr/Default.htm>

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 effective⁹.

Based on the language of the law and the comments of the FCC, it appears unlikely that CIPA has raised a potential basis for liability.

Informed Consent

Unfortunately, CIPA could have raised expectations in the minds of parents that a school district's use of filtering would totally protect their child. The plain facts are that *no* approach will ever be successful in totally preventing children using the Internet from accidentally or intentionally accessing inappropriate material or coming into contact with a dangerous individual. Such risks are inherent with the use of the technology. The risks must be addressed through effective education and supervision and balanced against the benefits of using the Internet for educational purposes.

Districts should not amplify the potential risk of liability (or controversy) by promising that the District Safe and Responsible Use Plan will prevent such access or contact. Honest disclosure of the potential risks and the strategies that have been adopted to address the risks is the most appropriate approach to address these concerns.

- Always make it clear to parents and to the community that the district is engaging in a good faith effort to address the concerns, but that given the nature of the Internet, no strategy can ever be assumed to be totally effective.
- Include a disclaimer of liability in the policy and the agreement that parent/guardians sign granting permission for their children to use the Internet.

The following statement is example statements that can address the concerns:

"Information for Parents about Student Use of the Internet

The Internet is a global information and communication network that provides a tremendous opportunity to bring previously unimaginable education and information opportunities to our students. Through the Internet, students can access up-to-date, highly relevant information that will enhance their learning. Students also have the opportunity to communicate with other people from throughout the world. Use of the Internet for

⁹ Federal Communications Commission, *In the Matter of Federal-State Joint Board on Universal Service Children's Internet Protection Act. Report and Order*. April 5, 2001.

URL: http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc.

enriching educational activities will assist in preparing students for success in life and work in the 21st Century.

The Internet is, however, a public space. As is true with all public spaces, there is a potential that students may come into contact with potentially harmful or inappropriate material or people. Therefore use of the Internet by young people necessarily raises concerns about safety and security. Young people may also use the Internet to engage in actions that are ethical, legal and responsible. Schools that provide Internet access to students have an obligation to help students learn to use the Internet in a safe and responsible manner.

The following Safe and Responsible Internet Use Plan addresses the strategies the District will utilize to create an environment that will support the safe and responsible use of the Internet by students. The District's Internet Safe and Responsible Use Policy and Regulations contain the specific guidelines necessary to implement this Plan. The Student Internet Use Policy addresses student responsibilities related to this Plan. Through this Plan the district seeks to:

- Establish an appropriate environment that will support the safe and responsible use of the Internet by students in school
- Impart to students the knowledge, skills, and motivation to use the Internet in a safe and responsible manner regardless of where or how they have access to the Internet.

Limitation of Liability

Due to the nature of the Internet, there can be no absolute guarantee that the implementation of the safe and responsible use measures contained in this Plan, including the Technology Protection Measure, will fully protected against access to material or people that may be considered inappropriate or potentially harmful. The district will not be responsible for any damage students may suffer if they accidentally or intentionally are exposed to such materials or people. Use of the system by students will be limited to those students whose parents have signed a disclaimer of claims for damages against the district."

2. District Liability for Material Placed on Web Site or Transmitted Through System

Dissemination of Harmful Speech

Legal Standards

When district staff or students use the district's Internet system for the publication or dissemination of material, such publication or dissemination may pose concerns regarding potential liability. Civil liability for harmful speech may arise in cases of libel (defamation) and invasion of privacy.

Libel (Defamation)

There are four elements for a successful claim of libel:

- The statement must be published.
- The person claiming libel must be able to prove he or she was identified by the statement.
- The libel victim must prove that the statement harmed his or her reputation in the community.
- The libel victim must prove fault -- that the person committing the libel did something they should not have done or failed to do something that they should have done.

If the libel victim is a public official or public figure, the victim must prove that the person committing the libel did so with actual malice. Actual malice means that the person either knew the statement was false or was reckless in verifying its accuracy.

Material that Constitutes an Invasion of Privacy

There are actually four related legal claims that fall under the "invasion of privacy" concept. Two legal claims are most relevant to the issues that could arise related to dissemination of materials through or publication of materials on the Internet. These are:

- **Public Disclosure of Private Facts.** Public disclosure of private facts occurs when a person publicly discloses a non-public detail of another person's private life when the effect would be highly offensive to a reasonable person.
- **False Light in the Public Eye.** False light in the public eye occurs when a person is placed before the public in a false light and this false light would be highly offensive to a reasonable person.

Defenses to actions based on invasion of privacy are that the facts are "newsworthy" (First Amendment) or that the victim gave consent. However, consent must be provided by someone capable of giving it. Minors are generally not considered capable of giving legal consent.

The Question of Statutory Immunity

There are two U.S. laws that relate to issues of statutory immunity of Internet service providers and Internet information providers. School districts may in certain aspects of its operations be considered an Internet service provider, but in other aspects of its operations be considered an Internet information provider. As will become apparent, this is an important distinction.

As discussed in the chapter on "District Liability Related to Access to Inappropriate Material or People" 47 U.S.C. § 230 of the Computer Decency Act provides:

- (1) Treatment of publisher or speaker.-- No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

The following definitions are relevant to an analysis of this provision:

- (2) Interactive computer service.-- The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provide access to the Internet and such systems operated or services offered by libraries or educational institutions.
- (3) Information content provider.-- The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

It is important to note, the statutory immunity provided by (1) to "interactive service providers" is not provided to "information content providers." Here are the provisions of the statute addressing

- (c) Information Residing on Systems or Networks At Direction of Users. -
 - (1) In general. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider -
 - (A)
 - (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
 - (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

...

k) Definitions. - (1) Service provider. - (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

It is important to recognize that the CDA provides immunity for “interactive service providers” for material that is transmitted *through* their system, but not for “information content providers” that are posting information *on* a web site.

Education institutions are included in the definition of interactive service provider, but this designation only addresses situations where the district has no control or supervisory responsibilities related to the material transmitted through the system. If the district establishes a district web site, the district is also an "information content provider" and can be held to publisher standards for any defamatory or other harmful material posted on the site.

It is possible that districts could be held liable for harm caused by material transmitted through the system by students due to the failure to adequately supervise. But it is also arguable that the immunity provided by 47 U.S.C.A. § 230 would apply in such a case. The district can be held liable for harm caused by material transmitted by staff.

Copyright Infringement

The district may be held liable for the presence of any material that is posted on the district web site in violation of copyright laws. Under copyright law, there are limitations of financial liability for Internet service providers who host material placed by others on their web site.

(c) Information Residing on Systems or Networks at Direction of Users.-

(1) In General.-- A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider,

(A)

(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;(ii) in the absence of such

actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent ...¹.

There are also limitations of liability granted to institutions of higher education.

- e) Limitation on Liability of Nonprofit Educational Institutions.-
 - (1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research ...².

These provision *do not* provide immunity for school districts for material placed on district, school, or class web sites because school personnel can and should maintain the ultimate responsibility for the material placed on such sites. No school district should operate a district, school, or class web site to operate without district staff having actual knowledge of what material is being placed on the site. School districts are not Internet "service providers" when they are presenting information on a district web site³.

The statute providing immunity for institutions of higher education does not refer to other institutions of education. Unfortunately, advocacy groups that support K-12 educational legislation were not paying enough attention to this copyright law, because clearly there are strong arguments for the enactment of provisions providing limitations of liability for k-12 institutions similar to those provided for institutional of higher education

Strategies to Address the Concerns

One of the requirements for Internet service providers under 17 U.S.C § 512 is that the service provider has designated an agent to receive complaints of copyright infringement and provides contact information on its web site for those concerned about material placed on the site. While such a designation and notice would not provide statutory limitation of liability for a school district under copyright law, this approach presents is an excellent preventative strategy to seek to limit the potential of liability for unintentional copyright infringement and other web site publication concerns.

To limit the potential of district liability for defamation, invasion of privacy, and copyright infringement, the following actions are recommended:

- Have provisions in the District Internet Use Policy that address these issues.

¹ 17 U.S.C § 512 (c).

² 17 U.S.C. § 512 (e). This statute unfortunately applies only to institutions of higher education.

³ I have had some disagreement on this interpretation with other school attorneys, who believe that schools fall under the provisions of §512. But it is clear from the legislative history of these provisions, that Congress intended to provide immunity for Internet service providers who were not in a position to know what material was being placed on their site, not Internet content providers. School officials must be in a position of knowing what is being put on their site. Schools should not be in a position of offering "free student web pages." If a school district does not maintain such control, the district will lose the right to limit student speech for educational reasons.

- Place on the district web site and each school web site a "Web Site Concerns" link. This link will take the reader to a page where the district states:

"XYZ District seeks to ensure that all materials placed on the district or school web sites are placed in accord with copyright law and do not infringe on the rights of or harm others in any way. To accomplish this we are taking three steps:

- We have provisions in our Internet Use Policy that address copyright, defamation, invasion of privacy, and other harmful speech. <link to policy>
 - We have established web site management procedures to review materials prior to their placement on the web site. <link to procedures>
 - We will promptly respond to any issues of concern. If you have a concern about material placed on our web site, please contact us. <link to e-mail to an administrator who has the responsibility of promptly responding to any complaint>"
- Establish web site management procedures that require review by a knowledgeable staff person prior to the posting of material.

It is important that this web site management process not become a bottleneck that unnecessarily restricts the effective educational use of the Internet with students. The best way to address this concern is through staff professional development related to web site liability concerns and the granting of authority to those staff members who have completed such professional development to approve the posting of material on a district, school, or class web site. (More information on a copyright management plan is included in "Copyright.")

3. District Liability to Students and Other Liability Concerns

Liability to Students

Violation of Student Rights

One area of potential liability is the district's failure to recognize a student's constitutional rights. If a student's rights, as addressed elsewhere in this guide, are not recognized by the district and the student suffers harm as a consequence, the district could be held liable. Potential areas of concern are related to due process, search and seizure, and free speech.

Recently, a number of districts have been held liable for damages to students as a result of the inappropriate imposition of discipline for offensive material that the students have posted on their personal web sites. These cases are discussed more fully in "Student Speech."

Another incident regarding student rights occurred at the Winter School District, Winter Wisconsin¹. A high school student was told that she could not look at sites about the Wiccan religion during after-school open access Internet. The student filed a complaint with the State Department of Public Instruction claiming, among other things, that the student's right to practice freedom of religion was violated. The district was facing litigation, but the matter was resolved when the Superintendent sent a letter to the student admitting that the policy was in error.

A districts that unfairly disciplines students for accessing controversial material may find itself in a position of potential liability on the basis of discrimination or violation of student's free speech right to access information. The same may be true for a district that selects, configures, and/or implements a Technology Protection Measure in a manner that appears to be indicating disapproval of certain information or ideas and thereby indicating disapproval of certain students based on their beliefs or status.

It is exceptionally important for all school administrators to have a full understanding of the constitutional rights of students that may be implicated in the use of the Internet. If in doubt, placing a call to the school attorney prior to imposing discipline or restricting student access to potentially controversial, but not inappropriate, material would be prudent.

Failure to Address Online Harassment

School-based harassment is a violation of Title VI and Title VII of the Civil Rights Act of 1964 and of Title IX of the Education Amendments of 1972. Schools are responsible for illegal actions they know about or should have known about. Schools are also obligated to prevent harassment in the school by anyone. Districts must react to harassment of students and staff at the hands of staff, students, and others.

¹ URL: <http://www.nytimes.com/library/tech/98/06/cyber/education/03education.html>.
Safe and Responsible Use of the Internet – Part III, Chapter 3, page 1

Federal law requires schools to have a policy against race and sex discrimination and to notify staff, students and parents of the policy. Compliance includes monitoring and implementing proactive efforts to foster prevention. Under Title IX, schools also are required to adopt and publish grievance procedures for resolving discrimination complaints, including harassment. In addition, schools are required to have at least one staff member responsible for coordinating efforts to comply with Title IX.

If a school finds there has been harassment, the obligation is to stop it and ensure it doesn't happen again. This means ending any quid pro quo, eliminating a hostile environment, preventing harassment from occurring again, and, when appropriate, correcting the effects on the student who has been harassed.

As discussed in "Preparing Young People to Make Safe and Responsible Choices," the lack of tangible feedback when communicating online can lead to rude and offensive speech. Such online speech may rise to the level of harassment. It is critically important that staff, students, and parents know that the district policies addressing harassment include online harassment. The staff member responsible for coordinating the grievance procedures for the district must have good insight into issues related to online bullying and harassment.

Conveniently, establishing evidence of online harassment is easy to accomplish due to the availability of the electronic records.

Other Liability Concerns

Other liability concerns include the following.

Computer Security Violations

There are a range of activities that constitute computer security violations, including attempts to invade computer systems, the deliberate transmission of a virus or worm, and the like.

Technically sophisticated students may be engaged in such activities using district technology resources. School districts could face potential liability if staff know, or have sufficient reason to suspect, that students have been engaged in such activities using district resources.

Recommendations to address this concern include:

- Include an immunity provision in the Student Internet Use Policy.
- Take *prompt* action if there is any suspicion of inappropriate behavior.
- Provide instruction about computer crime and its consequences in computer science classes.
- Monitor Internet traffic to detect excessive usage that could be an indicator of potentially inappropriate behavior.

Losses Caused by System Failure

There is a potential that a district could be held responsible for losses sustained by users as a result of a system failure. These losses could involve loss of data, an interruption of services, or reliance on the accuracy of information maintained on the district system or accessed through the system. The use of a disclaimer that provides notice of the potential for such loss and disclaims district responsibility should protect the district from liability. Users should also be advised to make a personal back-up of material contained on the district system.

Unauthorized Purchases

Districts should be concerned about the potential that a student will violate the district restriction against purchasing products or services through the system. The district will want to make it clear to parents that there is a potential for students to use the system in such a manner. The district will also want to include in its policy a disclaimer for any financial obligations arising from unauthorized use of the system for the purchase of products or services.

Damage to District System

Another area of concern is damage to the district system by misuse of the system that causes damage to the system. An example would be a student intentionally placing a virus on the system. This is no different than any other damage caused by a student or staff member and is likely covered in other district policies.

Copyright Infringement

Districts can be held liable for materials placed on the district web site in violation of copyright. This issue was discussed "District Liability for Material Placed on Web Site or Transmitted Through System." Districts can also be held liable for violation of copyright or licensing agreements in the use of computer software or for material downloaded from the Internet. These issues are discussed in "Copyright."

4. *Student and Staff Privacy Issues*

Legal standards

Monitoring student and staff use of the Internet in schools necessarily raises the issue of legal standards related to student and staff privacy. Most of the case law related to privacy issues has emerged in the context of criminal cases and have related to an interpretation of the Fourth Amendment restrictions on search and seizure. This case law has also be interpreted in the context of searches of student or staff personal belongings in school.

The initial analysis in such cases relates to the expectation of privacy. The United States Supreme Court in *Katz v. United States* first enunciated the constitutional standards related to expectations of privacy and established a two-part test¹. The first part of the test requires "[t]he person must have had an actual or subjective expectation of privacy."² The second part requires that this subjective "expectation be one that society is prepared to recognize as 'reasonable.'³" If these two tests are satisfied, then there is said to be a "reasonable expectation of privacy."

There are two additional doctrines that have emerged in this area that appear to be relevant. The first is the plain view doctrine. Under the plain view doctrine, if a public official who is legitimately where he or she is able to be, sees something in plain view, there are no privacy protections. The second doctrine is that of consent. In *United States v. Simons*, government agency network services administrator found patterns of use that indicated that an employee was accessing Internet pornographic material. Further search was made of the employee's computer and a significant number of pornographic files were found. The employee objected to the search on Fourth Amendment grounds. The court upheld the search, indicating that the government agency's policy on computer use indicated the potential of audits of web usage to identify instances of inappropriate activity.

The standards for school officials in conducting a search and seizure of a student in the school setting where there is a legitimate expectation of privacy were enunciated by the Supreme Court in the case of *New Jersey v. T.L.O.*⁴. These standards are:

- Was the search "justified in its inception"⁵? A search is justified when there are "reasonable grounds for suspecting that the search would turn up evidence that the students has violated or is violating either the law or rules of the school"⁶.
- Was the search "reasonably related in scope to the circumstances which justified the interference in the first place"⁷? A search is reasonable when "the measures adopted are

¹ *Katz v. United States*, 389 U.S. 347 (1967) The two-part test was first enunciated in Justice Harlan's concurring opinion and subsequently applied in other Fourth Amendment cases. e.g., *Smith v. Maryland*, 442 U.S. 735, 740-41 (1979)

² *Id.* at 350-52, 360.

³ *Id.* at 361 (Harlan, J., concurring).

⁴ 469 U.S. 325 (1985).

⁵ *Id.* at 341.

⁶ *Id.* at 342 (citations omitted).

reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction⁸."

The extent of a district's ability to investigate the personal files of staff is less clear. In *O'Connor v. Ortega*⁹, the Supreme Court held that employees did have constitutionally protected privacy interests in the work environment but that the reasonableness of the employee's expectation of privacy must be determined on a case-by-case basis. The Court then applied the *T.L.O.* standards of reasonableness to employer intrusions of employee privacy for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct.

Application of Legal Standards to Internet Use in Schools

Expectations of Privacy

Based on the above standards, let's now consider the situation related to Internet use in schools. Many school districts have a policy that reads something like. "There are no expectations of privacy in the use of the Internet."

What does this mean?

- Does this mean that any teacher can, at any time, review the web usage records and e-mail files of any other staff member or student?
- Does this mean the superintendent can regularly review the e-mail messages of staff union leaders?
- If a group of students are working to establish a chapter of the Gay, Lesbian, Straight Education Network at school, can the building principal who objects to the establishing of this organization request access to the web usage logs and e-mail files of these students?

Regardless of the statement in the district policy, it is likely that the vast majority of people would not be comfortable with the above intrusions into Internet records.

On the other hand, when students are using the Internet in a computer lab, there is very little privacy because much of what they are doing is in plain view.

On the other hand, if there is no expectation of privacy, then how is it that users are asked to establish a password for access to their personal files and warned to keep that password private?

On the other hand, there appears to be a higher expectation of privacy in a person's e-mail files as compared to records of web searches. This may be because just about everyone knows that web usage is being tracked by different entities for different purposes, whereas the contents of e-mail messages are not so publicly available. This may be because of the nature of personal

⁷ *Id.* at 342.

⁸ *Id.* at 342 (citations omitted).

⁹ 480 U.S. 709 (1987).

communication, rather than information searching. Essentially, the rationale for this perception is unknown.

On the other hand, electronic communications of public employees are generally considered to be discoverable under state public records laws, therefore it could be argued that employees have no expectation of privacy.

On the other hand, the common practice is to treat staff e-mail as private.

In other words, there are a lot of "*on the other hands*" in this situation -- meaning that despite a clear statement in a policy, there remains an expectation on the part of many users of a district system that there is, at least, some level of privacy in their use of the Internet at school.

Locker Search Standard

Looking at the situation from a different angle, it would be recognized that most school districts have students search and seizure policies related to student lockers and desks that are in accord with the *T.L.O.* legal standards. The policies provide that a general inspection may occur on a regular basis, with advance notice to the students. Special inspections of individual lockers or desks may be conducted when there is reasonable suspicion to believe that illegal or dangerous items or items that are evidence of a violation of the law or school rules are contained in the locker or desk. These same standards can be applied in the context of analysis of Internet usage records and e-mail files.

To further explore this issue, the author raised this topic for discussion on an e-mail discussion list. Several respondents indicated that their district policy was that there was no privacy. Then the author presented scenarios such as those above and pressed the respondents to further explore the issue. In every case, the basic desired standard that emerged through the discussion was a version of the locker and desk standard.

Essentially, there appears to be a basic underlying perception of a limited expectation of privacy in schools. The underlying expectations appear to be different for web usage logs, as compared to e-mail files. It is acknowledged that the district must regularly review web usage logs. It is not generally anticipated that the district will regularly investigate personal e-mail files. An exception to this is in elementary school, where students using a classroom account have no expectation of privacy.

Further, it appears that it is considered to be appropriate for the school district to investigate personal files -- including an analysis of an individual user's web usage logs or their personal e-mail files, if, and only if, there is a reason to believe that the user has engaged or is engaging in inappropriate activity. Essentially, this is the "reasonable suspicion" standard.

The following is the outline of the manner in which the standard school locker and desk search standards can be applied in the context of Internet usage.

Routine Monitoring

Users should be provided with a notice that all use of the Internet will be monitored on a regular basis.

Some districts may opt for staff monitoring of web logs and other usage data. This approach is feasible with a smaller district with low amounts of Internet usage. For larger districts, the staff monitoring activity may become unnecessarily time consuming and/or ineffective.

Routine monitoring may be facilitated with the use of technical monitoring tools. These tools may operate in "real time," such as monitoring systems that allow an administrator to directly remotely view what is on the screen of another computer. Filtered monitoring technologies utilize an intelligent analysis of Internet use traffic that seeks to detect communication patterns that may reveal instances of inappropriate activity.

Individualized Searches

Special inspection of the online activities of an individual user would occur when there are indicators that raise a reasonable suspicion that inappropriate activity has or is occurring.

The district should establish a process by which individualized searches are considered appropriate. Any individualized search of student e-mail files should be conducted only by authorized staff. Generally, the staff that are authorized to conduct an individualized searches will be the district's technology director, his/her designee, and administrators in the students' school.

Filtered monitoring technologies that analyze Internet usage and report on activity that is suspected to be in violation of the policy work in a manner that would meet the reasonable suspicion standard. They report on activity that is suspected to be in violation of the district's policy or the law, based on parameters established by the district. An individualized search can verify whether or not the reported suspected misuse is actual misuse or not. Internet usage traffic that does not raise concerns of possible misuse remains private.

Instances Where There are No Expectations of Privacy

There also may be situations where there are no expectations of privacy. These situations may include the following:

- Elementary students using electronic communications should likely have no expectations of privacy. They should use group or classroom e-mail accounts. If individual e-mail accounts are established, teachers should have full and complete access to these accounts at any time for any reason.
- The elimination of any expectation of privacy may be an appropriate disciplinary response when a student has been misusing electronic communications. As a disciplinary consequence, a student can be informed that for a period of time an administrator can and will regularly review his/her personal e-mail files or the e-mail system can be configured to have an automatic copy of any communication by the student sent to the teacher.

- If there are significant problems emerging within a particular school related to electronic communications, the school administrator may decide that for a period of time there will be absolutely no expectation of privacy and any and all student personal e-mail files may be reviewed at any time.
- There is no expectation of privacy for students in the event their parent requests access to their Internet usage files.
- There is no expectation of privacy, in the event of a public records request, except as provided under the state's public records laws.

Staff Privacy

The district policies related to staff privacy should likely also be addressed in collective bargaining agreements. In many cases, the standards for special inspections of staff classrooms or desks are similar to those set forth in student policies, that is, desks and classrooms may be searched if there is reasonable suspicion that the staff member is violating a law or school policy. Collective bargaining agreements also generally contain provisions regarding documentation of any individualized searches. These policies and agreements should be reviewed to determine their applicability to Internet searches.

NOTICE!

The most important step a district must take is fully and completely informing all students and staff what they can expect in terms of privacy.

All users of the system should be provided with absolutely clear notice about how the district will monitor Internet use. If any technology monitoring tools are used, secondary students and staff should be provided with records of how the system works and what evidence it can detect. Districts may want to remind students of the monitoring with a notices and examples of usage records placed in computer labs. Some districts provide information about the limitations of privacy directly on the log-on screen so users are reminded of monitoring every time they log onto the computer.

The most important reason to provide effective notice is the preventive effect of such notice. Providing students with demonstrations of how the district's monitoring strategy or system identified misuse can act as an effective deterrent to future misuse. When students are fully aware of how their actions are being monitored, only the most foolish will risk engaging in misuse.

The following is an example of policy language that can be used to specifically address student and staff privacy in the use of the Internet that will provide adequate notice:

"Users have a limited expectation of privacy in the contents of their personal files, communication files, and record of web research activities on the district's Internet system. Routine maintenance and monitoring, utilizing both technical monitoring systems and staff

monitoring, may lead to discovery that a user has violated district policy or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated district policy or the law. Students' parents have the right to request to see the contents of their children's files and records. Staff are reminded that their communications are subject to Freedom of Information laws."

Districts can provide ongoing notice of by providing a notice as part of the computer log-on screen in a manner such as follows:

"The district's computer and Internet system is to be used for educational purposes. Users are reminded that all Internet use is monitored by the district."

Addressing Expectations of Privacy

People are still struggling to hold onto the right of privacy at the same time that technology seems to be removing many vestiges of this important interest. It is reasonable for districts to expect concerns to be raised regarding intrusions into privacy and to provide a rationale for the manner in which the district intends to monitor student use of the Internet.

The basis of this rationale is learning to distinguish when and where we can and should expect privacy and when and where we should not expect privacy -- and then to govern our behavior and communications based on that expectation. For example, students who discuss private matters in the middle of a crowded lunch room are in no position to complain about the violation of their personal privacy on the part of those who might overhear their conversation.

School districts have an obligation to protect the safety of students when they are using the Internet and to ensure that the district's Internet resources are being used responsibly. The district cannot meet this obligation without engaging in supervision and monitoring. Therefore expectations of privacy must be guided by an understanding of the limitations of privacy when using the district's Internet system.

Further, districts must prepare students to be successful in their future work environments. The vast majority of employers, both corporate and government, are regularly monitoring employee use of the Internet, including web logs and e-mail. Therefore, it is appropriate for students to learn how to manage their behavior on monitored Internet systems.

5. *Public Records*

Instructional Stories

District Internet records and employee e-mail and other personal files are public records, subject to retention and disclosure of the state public records laws, the issue should be addressed within the context of the district Policy and Regulations. The following are the tales of one state education network and three districts.

One state education network was featured in some news articles about its filtering program and the level of denial hits it was reporting. Some anti-filtering advocates seeking to analyze the kinds of denial hits made a public records request for the actual data. The education network denied the request. The denial was appealed to the appropriate state agency. The state agency ordered the network to provide the records, but then it was found that the network had destroyed the records. The state agency recommended criminal prosecution but the case was not pursued by the local district attorney. The public advocacy group eventually received new data¹.

A school district employee was fixing the computer of the district superintendent and stumbled onto some sexually explicit materials. The school board convened an emergency meeting. The superintendent did not attend but did submit his resignation. Two local newspapers sought access to the computer files. The board denied the request, but did turn the computer over to legal authorities. No criminal charges were filed. The public records question was addressed in an appeal to the state agency. The board argued that the files were confidential personal notes and therefore exempt. The state's public access agency held that a "public record" is any material created, maintained, received or used by a public agency, and generated in any form or medium, including electronically stored data. The electronic record of Internet use stored on the school district's computer hard drive was clearly a public record².

The father of a public school student made a public records request for the Internet usage records of all of the students in the school district. It was apparent that the father was seeking data to support objections to the district's policy of not installing filtering/blocking software. The district refused to provide the records. The father took the matter to court. Two key district's arguments were that the provision of records may result in the disclosure of student confidential information and that provision of the records would violate student privacy. The court ruled that since a program could be used to redact student information, confidentiality was not an issue. Further, since students signed an AUP that indicated their use would be monitored, they had no expectation of privacy. The district also noted the excessive amount of data and the costs involved. The court indicated that this was not a matter of concern if the father was willing to pay for the costs. However, the district did have to pay for the father's attorney fees since the

¹ URL: <http://censorware.net/reports/utah/main.html>.

² URL: <http://www.gannett.com/go/newswatch/2000/november/nw1122-4.htm>.

district knew or should have known that under state public records laws it should have provided the records³.

A TV station made a public records request of the Internet usage records of one of the largest public school districts in the state. The district chose not to fight the public records request. It set up a FTP site to allow the station to download all available records related to the station's request. Internally, the district prepared an information strategy to positively address any potential negative findings. The district also kept track of all of the costs involved in the provision of the public records, and submitted this bill to the TV station, as was allowed under state law. The TV station was not able to find any instances of inappropriate use of the district's Internet system⁴.

Moral of Stories

Do not waste district resources fighting public records requests. Manage your Internet records with an understanding that such request may come at any time. Let your district's efforts in addressing legitimate concerns speak for themselves.

Issues of Concern

State laws of public records vary from state to state. Therefore this Guide can only address the issue from a general perspective. The two issues that districts should be concerned about related to the retention and disclosure of public records are:

- The massive amount of data that must be stored and the limited capacity of the district to store such data.
- The potential that the disclosure of data will violate the confidentiality/privacy interests of staff or students. State laws would protect such confidentiality/privacy -- but removing such information from the stored public records could present significant problems.

The one issue that districts should not be concerned about is whether or not public disclosure of usage of the district's Internet system will reflect well or badly on the district or individuals within the district. Public accountability is important. Districts must be prepared to provide accurate and helpful information to the public about its strategies to address the legitimate concerns about potential dangers in student use of the Internet, as well as the legitimate concerns that current technology protection measures are unnecessarily blocking student access to appropriate information. Proactive strategies to educate the community and the press are more effective in this regard than reactive strategies.

³ URL: <http://www.newsbytes.com/news/00/157754.html>.

⁴ Personal communication with John Adsit, Director of Technology for Jefferson County School District, Colorado. August 2001.
Safe and Responsible Use of the Internet – Part III, Chapter 5, page 2

Public Records Management

Retention and Destruction

Districts should identify what records are required to be retained under state laws and ensure that Internet usage records are retained and destroyed in accord with the provisions of state law. It is probable that districts will find that all staff e-mail files must be retained for a period of time. In many cases, this period of time is one year. But some records may be more important and thus may need to be retained for a longer period of time. Student e-mail files are not considered to be public records. Therefore, the district must organize its files in a way that will allow for the systematic and frequent destruction of student e-mail files, and the retention of staff e-mail files.

Some state public records laws have provisions that allow for the immediate destruction of non-essential records. Districts should request clarification from the state agency responsible for public disclosure regarding whether or not this provision will allow for the destruction of web usage logs. While issues of confidentiality and privacy can generally be handled with technical means, the sheer mass of data involved in the retention of web usage logs will overwhelm most districts.

If the district is not required under state law to retain web usage records, these records should be destroyed on a regular and routine basis. *But* a district should never, ever destroy records after the receipt of a public records request, even if such records are scheduled for routine destruction. Wait until after the public records request matter has been completed to resume the normal destruction schedule. Districts should analyze the manner in which records are retained so that they can easily and inexpensively redact any personal information.

Retention of Web Records for Quality of Use Analysis

Web usage logs are also important sources of data to enable the district to analyze the quality of student use of the Internet. Therefore, it is very important that representative samples of student usage data be analyzed to ascertain the quality of use. Districts should clarify the public records status of any analysis or reports that are completed regarding web usage. It is probable that reports and the data analyzed in regards to the reports will need to be retained for longer periods of time. Ideally, districts will think that it is important to retain small samples of web usage data over the years to allow for research into patterns of student usage of the Internet in schools.

Staff Awareness

Staff should be regularly reminded that the entire contents of their personal files on their computer, as well as their e-mail, would likely be considered to be public records, and thus subject to disclosure. A requirement that all staff use an e-mail signature that includes their name, title, and the district address is a helpful everyday reminder of the public records status of their electronic communications.

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 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.

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.

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 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

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/.

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.

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.

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 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:

⁸ *ALA* at I.

⁹ *Tinker v. Des Moines Independent Community School Dist.*, 393 U.S. 503, 506 (1969).

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).

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.

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

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

¹⁶ 484 US 260 (1988)

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

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 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.

¹⁸ *ALA* at V.

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 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

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.

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:

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.

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.

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

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

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

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:

²⁷ *ALA* at I.

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 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

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.

Reasonable Restriction Related to Legitimate Pedagogical Concerns

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

(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

³¹ *Hazelwood*, supra at 271.

³² NRC, supra at Section 12.1.5.

³³ NRC, supra at Section 12.1.8.

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.

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

³⁴ NRC, supra at Section 14.4.1.

³⁵ NRC, supra at Section 12.1.1.

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 "

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 .

³⁶ *Pico*, supra.

³⁷ *Pico*, supra.

³⁸ *ALA*, supra at I.

³⁹ *ALA*, supra at II.E.1.

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.

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.

⁴⁰ ALA, supra at II.E.1.

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).

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.

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:

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

⁴⁵ *ALA*, *supra* at II.E.2.b.

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.

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

⁴⁶ NRC, supra at Section 12.1.8.

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.

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 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

⁵⁰ *ALA*, supra at V.D.

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 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.

⁵¹ 47 U.S.C. 254 (h)(5)(B)

⁵² 47 U.S.C. 254 (h)(7)(I)

The NCIPA statute also contains the following provision:

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

- (A) establish criteria for making such determination;
- (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

⁵³ 47 U.S.C. 254 (1)(2)

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

burden we place on schools and libraries. Therefore, we will not adopt an effectiveness certification requirement.

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

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

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.

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

7. Student Speech

It must be recognized that students do not shed their constitutional rights on the school district's onramp to the Information Superhighway¹.

Overview of Issues

The issue of students' rights to free speech in the material transmitted through the Internet will arise in a number of ways:

- Student speech in public, discussion group messages.
- Student speech in private e-mail messages.
- Student speech posted on a district web site, including material posted in classroom sections, the school newspaper, and, if allowed by the district, material posted on an individual student web page or on an extracurricular organization web page.
- Student speech posted on another web site that has been accessed through the district system.
- Student speech that pertains to the school, teachers, or other students and that appears on a personal web site or is transmitted through personal e-mail account.

Pre-Internet Legal Decisions

There have been a number of Supreme Court cases addressing student's First Amendment speech rights. Three of these cases provide the greatest guidance for educators in addressing issues of student speech on the Internet. The cases are: *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*², *Bethel Sch. Dist. v. Fraser*³, and *Hazelwood School District v. Kuhlmeier*⁴.

In *Tinker*, school officials had disciplined students for wearing black arm bands to protest the war in Vietnam. The standard established in *Tinker* was:

In order for the State in the person of school officials to justify prohibition of a particular expression of opinion, it must be able to show that its action was caused by something more than a desire to avoid the discomfort and unpleasantness that always accompany an unpopular viewpoint. Certainly where there is no finding and no showing that engaging in the forbidden conduct would 'materially and substantially interfere with the requirements of appropriate discipline in the operation of the school,' the prohibition can not be sustained⁵.

¹ *Tinker v. Des Moines*, 393 U.S. 503 (1969) (Slightly restated)

² 393 U.S. 503 (1969)

³ 478 U.S. 675 (1986)

⁴ 484 U.S. 260 (1988)

⁵ *Id.* at 509

Subsequent court cases that addressed student underground publications, for example, *Thomas v. Board of Education*⁶, have applied the *Tinker* standard to such publications. In *Thomas*, students created a newspaper that contained sexually related articles and parodied several school officials. The newspaper was sold off-campus. The students were punished. The court ruled that such punishment was inappropriate. The court's ruling was based on the "supposition that the arm of authority does not reach beyond the schoolhouse gate."⁷ The court indicated that it was not appropriate for school officials to attempt to restrict free speech in the general community "where freedom accorded expression is at its zenith."⁸ The court did indicate that school officials were entitled discipline students if the off-campus speech "incites substantial disruption within the school from some remote locale."⁹

In *Frazer*, the Supreme Court found in favor of school officials who disciplined a student whose speech before a school assembly included sexual references. The Court distinguished between the purely political speech in *Tinker* with the student's vulgarity, and held that it was within the ambit of school officials' authority "to prohibit the use of vulgar and offensive terms in public discourse."¹⁰ Justice Brennan's statement in his concurrence in *Fraser* is particularly relevant to the present discussion. Brennan noted, "(I)f respondent had given the same speech outside of the school environment, he could not have been penalized simply because government officials considered his language to be inappropriate."¹¹

The issue involved in *Hazelwood* was a principal's decision to remove several articles from publication in the school newspaper. Here, the Court stated:

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 community¹².

Since the district's Internet system has been established for an educational purpose, it should be considered a limited forum, similar to a school publication where the school has maintained editorial control. This conclusion is strengthened by the fact that every user of the district system will be identified by the district domain name that appears in their address and, therefore, all speech that originates from the district system, even private messages, will bear the imprimatur of the district.

⁶ 607 F.2d 1043 (2nd Cir. 1979)

⁷ *Id.* at 1044.

⁸ *Id.* at 1050.

⁹ *Id.* at 1052. n. 17.

¹⁰ *Id.* at 683.

¹¹ *Id.* at 688.

¹² *Id.* at 267 (citations omitted)

Thus speech that occurs on or through the district's Internet system would be governed by the standards set forth in *Hazelwood*. However, districts that provide a significant amount of open access -- allowing their students to indiscriminately use the system in a manner similar to general public Internet access -- may find that they have established a public forum for their students. In such cases the ability of the district to govern student speech may be more limited. Such districts may need to establish requirements that relate specifically to school-use of the Internet, and other requirements that govern when the internet system is used for open access.

Student speech that occurs on personal web sites clearly would be considered speech that occurs in a public forum, thus the ability of the district to intervene or discipline a student appearing on a persona web site or transmitted through a personal e-mail account is extremely limited. The standards set forth in *Tinker* are the standards that would apply to such speech.

Student Speech involving the District System

Legal Standards

In *Hazelwood*, Court ought to craft a standard for the application of the First Amendment in "school-sponsored publications, theatrical productions, and other expressive activities that students, parents, and members of the public might reasonable perceive to bear the imprimatur of the school."¹³ The standard expressed by the Court was:

Educators are entitled to exercise greater control over [activities that may be characterized as part of the school curriculum] to assure that the participants learn whatever lessons the activity is designed to teach, that readers or listeners are not exposed to material that may be inappropriate for their level of maturity, and that the views of the individual speakers are not erroneously attributed to the school. Hence a school may ... 'disassociate itself' ... not only from speech that 'would substantially interfere with its work ... or impinge upon the rights of other students but also from speech that is, for example, ungrammatical, poorly written, inadequately researched, biased or prejudiced, vulgar or profane, or unsuitable for immature audiences. A school must be able to set high standards for student speech that is disseminated under its auspices¹⁴.

Reasonable Education-based Restrictions

The educational-based restrictions that would appear to be appropriate for a district to impose related to the use of the Internet by students could include:

- Criminal speech and speech in the course of committing a crime. Threats to the president; instructions on breaking into computer systems; child pornography; drug dealing; purchase of alcohol; gang activities; etc.

¹³ *Id.* at 271.

¹⁴ *Id.* at 271-272 (citations omitted)

- Speech that can cause harm to another. Online harassment; personal attacks, including prejudicial or discriminatory attacks; or false or defamatory material about a person or organization.
- Speech that is inappropriate in an educational setting or violates district rules necessary to maintain a quality educational environment. Restrictions would include:
 - Inappropriate language. Obscene, profane, lewd, vulgar, rude, disrespectful, threatening, or inflammatory language.
 - Dangerous information . Information that if acted upon could cause damage or present a danger of disruption.
 - Violations of privacy. Revealing personal information about others.
 - Abuse of resources. Inappropriate use of district group distribution lists through "spamming," chair letters, etc.
 - Copyright infringement or plagiarism. Transmission of material in violation of copyright or for the purposes of plagiarism.
 - Violations of personal safety. Revealing personal contact information or engaging in communication that could place the student in personal danger.
- Educationally- relevant restrictions. The district may also require that student publications meet a variety of standards related to adequacy of research, spelling and grammar, and appropriateness of material for placement on a school web site.

It is important to understand that public officials cannot limit speech based on viewpoint discrimination. *Hazelwood* did not address this issue directly, but the restriction against viewpoint discrimination is a long-standing First Amendment standard. One of the core functions of free speech is to invite dispute. For example in *Terminiello V. City of Chicago*¹⁵, the Court states: "It may indeed serve its highest purpose when it induces a condition of unrest, creates dissatisfaction with conditions as they are, or even stirs people to anger. Speech is often provocative and challenging."¹⁶ There is no suggestion in *Hazelwood* that the Court was opening the door for school officials to exercise control of student speech based on their disagreement with the opinions being expressed. Indeed this has been the holding of several Circuit Court opinions interpreting *Hazelwood*, e.g. *Searcy v Harris*¹⁷.

As discussed in "District Liability Related to Copyright and Harmful Speech," the district can potentially be held liable for material posted by a teacher or student that harms another. For this reason the district web site management approach outlined in that chapter is recommended.

¹⁵ 337 U.S. 1, (1949)

¹⁶ *Id.* at 4

¹⁷ 888 F2d 1314 (1989)

An educational approach is also recommended both to address concerns of speech occurring on or through the district's Internet system, as well as for speech occurring off-campus, as will be discussed below. If the Internet is providing the vehicle for all people to be publishers, then it becomes necessary for all people to recognize the boundaries between responsible speech and harmful speech. These issues simply must be incorporated into school curriculum. The Student Press Law Center has some excellent materials for student journalists that specifically address the issues related to underground publications and online publications¹⁸. However, consideration of these issues should not be limited to students with an interest in journalism.

It is also advisable to teach students how to engage in effective online advocacy without crossing the line to harmful speech. There are responsible and effective ways to challenge authority or challenge the actions of others on the Internet. Students can be challenged to consider how Mahatma Gandhi or Martin Luther King would have approached the creation of an online protest web site.

Off Campus Speech

Legal Standards

The *Tinker* case provides the legal standard that has been applied to incidents involving student speech that is not made using school technology facilities, but involves comments made about the school, teachers, or other students. The speech may occur on student personal web sites or through personal e-mail accounts. The standard established in *Tinker* was:

In order for the State in the person of school officials to justify prohibition of a particular expression of opinion, it must be able to show that its action was caused by something more than a desire to avoid the discomfort and unpleasantness that always accompany an unpopular viewpoint. Certainly where there is no finding and no showing that engaging in the forbidden conduct would 'materially and substantially interfere with the requirements of appropriate discipline in the operation of the school,' the prohibition can not be sustained¹⁹.

Cases Involving Off-Campus Student Speech

There have been six reported cases where the issue of school discipline of students for material posted on the Internet that related to the school but was not posted using district Internet facilities. In all but one case, the district lost. In some cases the damages were significant. Each of these cases will be presented so that readers can gain a better understanding of the dynamics of this issue.

O'Brien v. Westlake City Schools of Education²⁰

A high school student created a web site, entitled "raymondsucks.org," which insulted his band teacher. The school administrator imposed a 10-day suspension that resulted in a failing grade in band and lowered grades in other classes. The student brought a lawsuit and was granted a

¹⁸ URL: <http://www.splc.org>

¹⁹ *Id.* at 509

²⁰ No. 1:98CV 647 (E.D. Ohio 1998).

temporary restraining order. The School District ultimately settled the case by agreeing to pay the student \$30,000, expunging the suspension from his record, and providing a letter of apology.

*Beussink v. Woodland R-IV Sch. Dist.*²¹

A web site was created by a high school student that was extremely critical of the school administration and used vulgar language. The school suspended the student for 10 days. The principal testified that the discipline was a result of his dislike of the site's content, as opposed to any substantial disruption at the school. The Court noted the tensions between the freedom of speech and the ability of schools to determine discipline necessary for an orderly learning environment. In this case, at least, the "public interest is not only served by allowing [the student's] message to be free from censure, but also by giving the students ... this opportunity to see the protections of the United States Constitution and the Bill of Rights at work."²² Applying the *Tinker* standard, the court concluded that "while speech may be limited based on a fear of disruption, that fear must be reasonable and not an undifferentiated fear of disturbance" and that "(d)islike or being upset by the content of a student's speech is not an acceptable justification for limiting student speech."²³

*Emmett v. Kent Sch. Dist. No. 415*²⁴

An honor student created a web site entitled the "Unofficial Kentlake High Home Page." This web site contained a statement disclaiming school sponsorship and noted it was for entertainment purposes only. The site had two mock obituaries of the student's friends. The news media picked up on the story and reported that the student's site contained a "hit list." The student immediately removed the page in response to the story. The school responded with fast-tracking expulsion, and then backtracking to a 5-day suspension, and a lawsuit was filed by the student. The Court found the school officials had failed to show that the web site was "intended to threaten anyone, ... or manifested any violent tendencies whatsoever."²⁵ Utilizing the *Tinker* analysis, no substantial disruption was found. The School district later settled with the student.

*Beidler v. North Thurston Schl. Dist. No. 3*²⁶

In this case, the student's web site targeted a school administrator, showing the individual at a Nazi book burning, drinking beer and spraying graffiti. Emergency expulsion was initiated. The student transferred for the balance of his junior year. The student won a temporary restraining order. The Court held that even if the speech were defamatory, that would not justify imposing discipline here, as this was a case based on a violation of the First Amendment, not on defamation. The School District agreed to pay the student \$62,000.

*J.S. v. Bethlehem Area Sch. Dist.*²⁷

An 8th grader's web site included derogatory comments about his math teacher, including: "Why Should She Die?" and "Take a look at the diagram and the reasons I gave, then give me \$20.00

²¹ 30 F. Supp. 2d 1175 (E.D. Mo. 1998).

²² *Id.* at 1182.

²³ *Id.* at 1183.

²⁴ 92 F. Supp. 2d 1088 (W.D. Wash. 2000).

²⁵ *Id.* at 1090.

²⁶ No. 99-2-00236-6 (Wash. Supr. Ct. July 18, 2000).

²⁷ 757 A.2d 412 (Pa. Commw. 2000).

to help pay for the hitman." The student voluntarily removed the web site a week after the principal learned of it. The school officials contacted the FBI, but took no action against the student during the remainder of the school year. During the summer, officials decided to impose a 5, then a 10-day suspension, which was transformed into expulsion proceedings. The student then brought a lawsuit, appealing the expulsion. The court based its decision on the *Tinker* standard and determined that off-premises behavior could be punished, if the school could establish that "the conduct materially and substantially interfere[d] with the educational process."²⁸ The majority thought this was so, given that students discussed the web site while at school and school-sponsored activities. The statements on the web site were also considered by the majority to be a threat. They noted that the teacher who was the subject of the web site was unable to finish the school year and took a medical leave the following year. The dissent argued that the school officials did not believe the statements were a threat and that only true threats should not receive First Amendment protection²⁹.

Important additional information about this case is that the teacher also filed a lawsuit against the student and his parents. The suit was based on libel and invasion of privacy. The court dismissed the libel suit, but the teacher prevailed on the invasion of privacy claim and was awarded \$500,000.

*Killion v. Franklin Reg. Sch. Dist.*³⁰

A high school student was suspended for writing an e-mail that derided the school's athletic director. The e-mail addressed the teacher's weight and sex life. Another student reformatted the e-mail and distributed it at the school. The court examined the case in the context of *Tinker*, *Frazer*, and *Hazelwood* as well as the recent student web site cases of *Emmett*, *Beussink*, and *Bethlehem*. The court determined that the school district would need to establish that there was a "substantial disruption" before it could take action against someone for off-premises speech

The Court noted that the school district could not identify any actual disruption at the school that resulted from the e-mail. There was "no evidence that teachers were incapable of teaching or controlling their classes ... [the e-mail] was on school grounds for several days before the administration became aware of its existence, and at least one week passed before [it] took any action."³¹

The school district argued that the speech could still be punishable, under the *Fraser* analysis, as "lewd speech." The Court agreed with the school district that some of the speech in the student's e-mail was lewd, but because the student was not responsible for bringing the speech to school, the school district could not discipline him for it. The court relied on the statement in Justice Brennan's concurrence in *Fraser*, noted above, that "if respondent had given the same speech outside of the school environment, he could not have been penalized simply because government officials considered his language to be inappropriate."³²

²⁸ *Id.* at 421.

²⁹ *Id.* at 426-29.

³⁰ 136 F. Supp. 2d 446 (W.D. Pa. 2001).

³¹ *Id.* at 455.

³² *Id.* at 456 (quoting *Fraser*, 478 U.S. at 688).

Killion will likely become the leading case in this area. The court provided an excellent analysis of the issue in light of *Tinker*, *Fraser*, and *Hazelwood*, as well as the more recent student web site cases. The court further addressed the specific evidence that school officials would need to demonstrate to establish that off-campus speech had created a substantial disruption in school.

In light of these decisions, unless there is actual substantial disruption caused by off-campus, online student speech, school officials do not have the authority to respond to such speech by disciplining the student in the traditional manner. However, such speech may cause harm to members of the school community. It is therefore necessary to consider other strategies to prevent such harmful speech from occurring and to intervene or respond in a manner that is legally sustainable if such speech occurs.

Education and Intervention Strategies

Education

The legal standards related to civil liability related to harmful speech, defamation and invasion of privacy, are addressed in "District Liability Related to Copyright and Harmful Speech" Additionally, there is the potential for criminal liability for the dissemination of speech that meets the standards of harassment, creation or dissemination of obscene material, creation/dissemination of child pornography, and provision of sexually explicit material to a minor.

As noted above, providing students with education about responsible speech, harmful speech, and criminal speech is highly recommended. The more students understand the consequences of harmful speech and criminal speech, the less likely they may be to engage in such speech.

Providing parent education can probably be an even more helpful strategy to address off-campus harmful speech and criminal speech. Parents should be more fully aware of the potential of personal liability or criminal actions that may stem from the harmful or criminal speech posted on the Internet by their child. Also, parents need to understand how they might respond if their child is the victim on harmful online speech.

Intervention

The fact that free speech standards may place restrictions on the use of the traditional school disciplinary response should not prevent a school official from responding in a variety of other effective ways.

- Remember that the perpetrator of online harmful speech may be the victim of on-campus bullying or harassment by other students or may be feeling abused by school staff. In some cases, the online harmful speech may be a disguised cry for help. Seek to see through the harm to the pain that is being experienced by the student.
- Distinguish between legitimate, yet discomfort-provoking, protest speech that is challenging authority and truly harmful speech. Protest speech can provide an excellent "teachable moment" for school administration. Such speech provides the ability to see the school through the eyes of a student or students and can provide valuable insight into the quality of

the school environment. If a school is experiencing significant difficulties with harmful online speech by students, this should be viewed as a clear indicator to the school that the quality of the school environment is not of optimal quality.

- Take prompt actions to seek to have truly harmful speech removed from the Internet. Most Internet Information Service Providers have policies for web sites that restrict the publication of harmful speech. The Service Providers have strong incentives to not be associated with harmful speech and most will promptly remove a web site that contains such speech. However, prior to having the speech removed, it would be prudent to retain a copy of the web pages as evidence.
- Contact the parents of the student and request their assistance in resolving the matter. Many parents are not fully aware of the actions of their children on the Internet. Approach parents with the assumption that they are unaware, will be disturbed by the speech, and will be your ally in addressing the matter proactively with their child. If the parents are resistant, it may be appropriate to suggest to the parents that they contact an attorney to determine their potential liability to the victim for the harm caused by their child's online speech.
- Support the victims of such speech to seek appropriate resolution. This may include advising the victim and his/her parents or a staff member about possible legal resources. Additionally, the school can be a conduit of communication between the perpetrator, victim, and parents. For example, the school could be the vehicle of a heart-felt communication by the victim regarding the hurt and harm caused by the online materials and could also be a vehicle for a letter of apology from the perpetrator to the victim.

8. *Academic Freedom*

The Vision and the Reality

The following two pre-Internet quotes provide an excellent example of the vision and the reality of academic freedom in schools:

The Vision

Our nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely the teachers concerned. That freedom is therefore a special concern of the First Amendment, which does not allow laws that cast a pall of orthodoxy over the classroom. ... The classroom is particularly a 'marketplace of ideas.' The Nation's future depends upon leaders trained through wide exposure to that robust exchange of ideas which discovers truth out of a multitude of tongues, [rather] that through any kind of authoritative selection¹.

The Reality

The effort to pull ideology out of schools is evident in battles over history textbooks. ... (M)ost students read carefully censored books. The pursuit of 'neutrality' often leads to censorship. The American Textbook Publishers Institute has counseled publishers 'to avoid statements that might prove offensive to economic, religious, racial or social groups or any civil, fraternal, patriotic, or philanthropic societies in the whole United States.' Textbook manufacturers appear to have responded in some cases by deleting materials reflecting cultural differences that might have offended someone. Interest group pressures from diverse ideological camps have resulted in the deletion of materials that would undercut the perception of an American monopoly on decency, as variously defined. Business interests have occasionally intervened in textbook selection to remove materials considered hostile to the "American system." American policy is sanitized. Books rarely report questionable government action.

... Perhaps the most striking feature of history textbooks is that they minimize the role of dissent in our history. Government decisions that appear decent or beneficial are often portrayed without any of the political controversy that created them².

Textbook Selection

Most states and districts have established careful processes to determine what information is provided to students through textbooks. This process frequently acts in such a way as to limit exposure to controversial viewpoints or subjects. As is outlined in the article written by Linda Starr of *Education World*, much of the material contained in textbooks has been carefully shaped to address the ideological concerns of the three largest textbook purchasing states, Texas, California, and Florida. As Starr notes:

¹ *Keyishian v Board of Regents*, 385 US 589, 603 (1967) (cite omitted)

² Gottlieb, "In the Name of Patriotism: The Constitutionality of 'Bending' History in Public Secondary Schools." 62 *N.Y.U.L.Rev.* 497, 504 (1987).

That wouldn't be a problem if textbooks were what most of us assume them to be -- complete, unbiased accounts of "the truth, the whole truth, and nothing but the truth." In fact, textbooks are actually compilations of selected facts, and the decisions about which facts to include -- and which to omit -- determine not only what your students learn but also how they interpret the information presented³.

Starr reports on the decision by the textbook selection committee in Texas to not approve a certain environmental sciences book which addressed ecological sustainability in a manner that was, apparently, not in accord with the ideological perspective of the Texas textbook committee members.

Notwithstanding the rejection of this textbook, there are not, to the knowledge of this author, any restrictions placed upon teachers in Texas to limit student access to information available through the Internet. This Internet material will likely address ecological sustainability from a wide variety of perspectives – some of which would clearly not be in accord with the ideological perspectives of the textbook selection committee members.

Controversial Information on the Internet

As the Internet grows in importance as a source of information, students will be exposed to a much wider range of information and ideas. Some of this material will clearly prove to be offensive to economic, religious, racial, social groups, civil, fraternal, patriotic, and/or philanthropic societies in the U.S. Some of this material may challenge the U.S. monopoly on "decency" or correctness, as variously defined. Some materials may directly challenge or raise questions about the appropriateness of the actions of the U.S. corporations or the U.S. government. Therefore, it is quite possible that student access to such information could ignite controversy in some communities.

When teachers use the Internet with their students, decisions about the appropriateness of certain materials are no longer under the control of school textbook publishers, the textbook selection committees of three large states, or other state or local school textbook selection committees. Teachers will bear the primary responsibility for the selection of materials and of assisting students in evaluating and analyzing the information.

Which students are going to be better prepared to be effective citizens in today's complicated world? Those who receive carefully sanitized information that avoids the presentation of controversial ideas? Or those who, under the guidance of effective teachers, have wide exposure to a robust exchange of ideas which facilitates the discovery of truths out of a multitude of tongues?

The kinds of information available through the Internet can assist teachers in achieving the vision of a classroom as a marketplace of ideas. Students will be exposed to a wide range of perspectives that have not traditionally been accessible in the classroom. The changes in

³ Starr, L. Protect Yourself Against Textbook Tampering. *Education World*, 11/12/01. http://www.education-world.com/a_issues/issues229.shtml
Safe and Responsible Use of the Internet – Part III, Chapter 8, page 2

education that will be brought about because of the expanded access to a wide range of information made possible by the Internet will be significant. In some communities, this may lead to some controversy.

Professional Development

Clearly, districts must place a high priority on providing professional development opportunities for teachers to prepare them to handle this new learning environment and to effectively develop and implement learning activities that address controversial subjects.

Most districts have policies on academic freedom. It should not be necessary for districts to redo these policies to address the Internet access. The following kinds of recommendations or guidelines can be made to teachers regarding the material they select for classroom instruction and can help to guide effective professional development activities.

- Teachers should select required or recommended material that is appropriate in light of the age of the students and that is the relevant to the course objectives.
- Teachers should preview the materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site.
- Teachers should provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly when they are accessing the Internet independently.
- Teachers should assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

9. *Copyright*

The Copyright Balance

The following two statements outline the rationale for copyright protection:

Congress has the right ... To Promote the Progress of Science and the Useful Arts, by Securing for limited Times to Authors and Inventors the Exclusive Right to their respective Writings and Discoveries¹.

The utility of this power will scarcely be questioned. The copyright of authors has been solemnly adjudged, in Great Britain, to be a right of common law. The right to useful inventions seems with equal reasons to belong to the inventors. The public good fully coincides in both cases with the claims of individuals².

Copyright laws balance two important values:

- **Personal Rights.** If a person has devoted their creativity, time, and energy into the creation of something, that person should have the right to say who can use it and how. People should have the right to compensation for their creative work if they chose to ask for it.
- **Benefit to Society.** There are two benefits to individuals and society. Ensuring that people can be compensated for their work encourages more creative works and these works are of benefit to our society and individuals. Providing copyright protection for only a limited period of time and allowing for exceptions to copyright protection that support uses that are beneficial to society ensures that the copyright protections provided to creators are not so extensive that society cannot benefit from the works.

Copyright Basics

A creative work -- text, music, picture, software, etc. -- is automatically protected by copyright from the moment it is created. It is not necessary for a work to have a copyright notice or to be registered to receive copyright protection.

A creator can place his or her work in what is called the "public domain" by clearly and specifically relinquished all copyright rights. Since a notice is not required, merely publishing a work without a notice is not a relinquishment of copyright rights. Unfortunately, there are many sites on the Internet where the developer of the site has posted material in violation of someone else's copyright. The simple fact that a work appears on a web site without a copyright notice does not mean that the work is in the public domain. A work is also considered to be in the "public domain" if the copyright has expired. Material produced by the Federal Government and state government is also generally considered to be in the public domain. However, material

¹ *U.S. Constitution, Sec 1, Art 8, Cl 8*

² *Madison, J. The Federalist, Number 43*

funded by government agencies is generally not in the public domain, unless the government contract specifies this status.

The owner of a copyright has the exclusive right to copy, modify, distribute, display/transmit, and perform the work. The owner of a copyright can grant other people permission, called a "license", to exercise any of these rights. The permission can be expansive or limited. Sometimes people include a permission statement or license on their work. For example, the creator may say: "Permission to reproduce and distribute for non-profit purposes is granted."

A copyright is not the same as a trademark. A trademark is a name, logo, or graphic that is used to identify the source of products or services. It is also possible to infringe on a trademark. Trademark infringement occurs when someone uses a trademark in a manner that is likely to cause confusion regarding the source of particular products or services. Sometimes a particular work, generally a graphic, can serve as a trademark and also be protected by copyright.

Copyright Ownership by Students and Teachers

Students and teachers may have copyright rights in the works that they produce. It is important that districts recognize and respect these rights.

Student Copyright Ownership

Students are not employees of a school. Any work created by a student that meets the other requirements for copyright, is fully protected by copyright law. The best strategy to teach students about the need to respect the copyright rights of others is in the context of teaching them about their rights. Schools that wish to exercise copyright rights, for example, through the publication of student work on a school web site, should receive permission from the student and the student's parent/guardian. A one time request for ongoing permission to post student work should be sufficient. Students should be taught how to more fully protect their copyright rights through the use of a copyright notice. Technically, a copyright notice should include the full name of the copyright owner. This will present problems in schools because of the disinclination to post student full names. It is recommended that student work be posted with a notice that includes the student identification and the school the student attends: © 200?, jjwill Student at Adams Elementary School.

Teacher Copyright Ownership

The ownership rights of teachers presents a more complicated situation. In most cases, teachers are employed to teach, not to create curriculum. Works that are created by the teacher on his or her own time, with his or her own resources, are clearly owned by the teacher. If the district has specifically requested and supported the development of curriculum, then the district owns the copyright. The situation becomes more complicated when district resources are used in some manner but the district has not specifically requested or supported the development of the materials.

All districts should have a clear policy outlining copyright rights. The following standards are recommended:

- If the teacher creates materials solely on his/her own time, using his/her own resources, then the teacher owns the copyright and the district has no rights.
- If the teacher creates materials primarily on his/her own time, and primarily using his/her own resources, but has used some district time and/or resources, such as posting the materials on the district web site or some use of instructional preparation time, then the teacher owns the copyright, but the district should have a no-cost, nonexclusive, continuing right to use the materials for educational purposes within the district.
- If the teacher's creation of the materials has been initiated and supported by the district and designed to meet district-specified instructional needs, then the district owns the copyright.

Copyright and the Information Age

The original copyright laws emerged after the invention of the printing press. The development of new technologies for the distribution of information is causing a restructuring of existing copyright laws. This is an activity that is occurring on an international level as well as a national level. This increases the complexity because copyright laws are grounded in different philosophical perspectives throughout the world. Currently, there are many players and competing interests involved in the discussion. Educators will need to be active participants in developing new standards with respect to the fair use of copyrighted materials for educational purposes.

Underlying the restructuring of copyright law is a fundamental shift in the relationship between the creators of works and the individual. Traditionally, the work of a creator only reached the individual through a publisher. Publishers have traditionally served two roles -- ensuring quality and managing the production and dissemination of the work. Publishers have traditionally played a major role in determining copyright policy, and continue to do so today. Through the use of telecommunication technologies, creators of works have a more direct connection with the individual users of their works. The role of publisher in production and dissemination is diminishing. There are many examples emerging on the Internet that demonstrate the potential of these direct connections.

Fair Use Doctrine

The "fair use doctrine" provides a limited basis by which people can use a copyrighted work without getting permission from the creator. The fair use doctrine seeks to ensure that the benefits to society are not defeated by the limited monopoly that has been granted to the copyright owner. The fair use doctrine was established in a long line of court cases. Essentially, the courts were presented with situations where the benefit to society was considered to be greater than the potential loss to the creator. In the Copyright Act of 1976, Congress codified the legal standard for fair use that provides:

Limitations on Exclusive Rights: Fair Use. Notwithstanding the provisions of section 106, the fair use of copyrighted work, ... for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a

work in any particular case is a fair use in any particular case is a fair use the factors to be considered shall include:

1. The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. The nature of the copyrighted work;
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole;
4. The effect of the use upon the potential market for or value of the copyrighted work³.

Fair Use for Teaching, Scholarship, and Research Purposes

Over the years, librarians, educators and publishers have developed voluntary guidelines to address fair use of work for teaching, scholarship, and research purposes. Although these guidelines are not statutory, they are contained in the legislative history of the Copyright Act. The current guidelines cover copying by and for teachers in the classroom context, the copying of music for educational purposes, the copying of relatively recent journal articles by one library for a patron of another, and the off-air video-taping of video broadcast materials. These fair use guidelines generally address fair uses that are non-transformative -- that is the work is being used as it was produced and essentially for the purpose for which it was used.

In 1994, the U.S. Department of Commerce established the Conference on Fair Use to bring together copyright owner and user interests to discuss fair use issues that have been raised by new technologies and to develop guidelines for fair use by librarians and educators. The CONFU participants spent over 2 1/2 years in an attempt to develop new fair use guidelines. Proposed guidelines were developed in three areas, digital images, distance learning, and educational multimedia. In the end, there was no consensus on the guidelines. In brief, the copyright owners thought that the guidelines gave too much away and the educators and librarians thought the guidelines were unworkable and overly restrictive.

It is unknown whether the guidelines developed represent a "safe harbor" for educators and librarians. Some educators and librarians fear that following the guidelines will result in undercutting a more expansive scope of fair use. Following CONFU members of a number of educational, scholarly, and copyright user organizations, including the National Education Association, the National School Boards Association, and the American Library Association, committed to the following:

- We will share experiences concerning: the application of new technology in library and educational environments, "fair uses" made of copyrighted works, proprietors' responses to requests for permission to use copyrighted materials, and sources of helpful information regarding fair use and other privileges under copyright law;
- We will participate in organized efforts to capture and disseminate such information;

³ 17 U.S.C. § 107

- We will assist in the development of "User Community Principles" and educator- and librarian-generated "Best Practices" concerning fair use, distance learning, and other activities supported by current copyright law;
- We will work to extend the application of fair use into digital networked environments in libraries and educational institutions by relying on it responsibly to lawfully make creative use of information;
- We will resist relying on any proposed code of conduct which may substantially or artificially constrain the full and appropriate application of fair use; and
- We will encourage our members to reject any licensing agreement clause that implicitly or explicitly limits or abrogates fair use or any other legally conveyed user privilege⁴.

Under the fair use exception for teaching, research and scholarship, posting a copyrighted work on a publicly accessible web site would not constitute fair use. Such use would go far beyond the limited spontaneous use with a limited audience that is supported under this particular fair use exception. Posting a work on an intranet, where access would be limited to only those students in a particular class may constitute fair use, if such use also met the other traditional requirements of brevity and spontaneity.

Fair Use for Criticism and Comment

Use of copyrighted work for criticism and comment, including parody, is a transformative use of the prior work. With such uses, the owner of the copyrighted material may not be inclined to grant permission for use of the work, since such use may be for the purpose of criticizing the prior work.

This fair use exception, grounded in the First Amendment, is important for public policy reasons. When a portion of a prior work is incorporated into a new work for the purpose of expanding upon, commenting on or criticizing the prior work, the new work has significant social benefit. It is through the publication of works, and comments and criticism of those works that society gains new knowledge. Therefore, such use of the prior work for comment and criticism purposes is considered to be fair.

If use of a prior work is for comment and criticism purposes, then the new work could properly be placed on a publicly accessible web site.

Unfortunately, virtually all of the guidelines provided for educators related to fair use have been framed within the context of nontransformative use for education and research purposes. No guidelines have been developed for educators and students to follow in the context of transformative uses for comment and criticism purposes.

⁴ URL: <http://www.ALA.org/washoff/confu.html>

Liability for Copyright Infringement

In brief, the potential district liability for copyright violations on or related to the Internet and computer technology includes the following:

Material Posted on District's Public Web Site

School districts should be very careful about the copyright status of any material posted on this web site. Most companies do not want to sue school districts for copyright violations unless the unlawful practice is pervasive and such a suit would send a message to other districts. Promptly removing any material that violates copyright will generally satisfy the copyright holder. More information regarding copyright management is provided below.

However, if a copyrighted work is being used appropriately for fair use purposes, in the context of criticism or comment on the prior work, districts may need to weigh the risk of liability against the importance of supporting teachers or students in the important exercise of First Amendment free speech rights and the advancement of knowledge. Unfortunately, some copyright holders have become excessively aggressive in seeking to enforce their interests, regardless of the fair use exceptions contained in the law.

Violation of Copyright or Licensing Agreements

The Software and Information Industry Association has an Anti-Piracy Education Initiative. There are excellent recommendations for the establishment of an effective software management program in schools on their web site⁵.

Downloading Copyrighted Material

Districts must also closely evaluate their web traffic to ensure that students or staff are not using the district Internet system as a vehicle to exchange copyrighted materials such as musical files, software, and videos. Such activity would result in a significant amount of traffic and should be easily detectable by an astute system administrator.

Teachers also need to be reminded to follow the traditional fair use for education and research guidelines for any copyrighted material they download from the Internet.

Copyright Management for School Web Sites

Web Site Concerns

The following Copyright Management Plan seeks to address concerns of material placed on the district web site that may interfere with the rights of others, including copyright rights. (This issue and approach was also discussed in "District Liability Related to Copyright and Harmful Speech")

- Have provisions in the District Internet Use Policy that address copyright and other potential harmful speech liability issues.

⁵ URL: <http://www.siaa.net/piracy/policy/educate.asp>

- Place on the district web site and each school web site a "Web Site Concerns" link. This link will take the reader to a page where the district states: XYZ District seeks to ensure that all materials placed on the district or school web sites are placed in accord with copyright law and do not infringe on the rights of or harm others in any way. To accomplish this we are taking three steps:
 - We have provisions in our Internet Use Policy that address copyright, defamation, invasion of privacy, and other harmful speech. <link to policy>
 - We have established web site management procedures to review materials prior to their placement on the web site. <link to procedures>
 - We will promptly respond to any issues of concern. If you have a concern about material placed on our web site, please contact us. <link to e-mail to an administrator who has the responsibility of promptly responding to any complaint>
- Establish web site management procedures to address these issues of concern.

Web Site Management Procedures

The following web site management procedures should be required for all teachers and students who are placing materials on the school web site. The copyright management procedures require noting the source and copyright status for all materials placed on the web site. To be included as a component of the web page or course, the material must meet one of the following criteria:

1. Original Material. This is material created by teacher or the student for the web page or course. This material should include a statement of copyright ownership and any permissions that may be granted. A standard notice might read: "© 200_ name. Permission to reproduce and distribute for non-profit purposes granted."
2. Public Domain Material. Public domain material falls into one of 3 categories:
 - a. Created by the government (does not apply to material created by someone else with federal funding).
 - b. Placed in public domain by copyright owner.
 - c. Copyright has expired. The following is information about when a work enters the public domain:
 - i. Published before 1923. In the public domain.
 - ii. Published from 1923 to 1963. Copyright term starts from time the work was published with a copyright notice. The copyright term was 28 years for first term, with ability to renew for 47 years, which was recently extended for 20 more years (total 67 years). If the copyright was not renewed, the work is in the public domain.
 - iii. Published from 1964 to 1977. Copyright term starts from time the work was published with a copyright notice. The copyright term was 28 years for first term. Now there is an automatic extension for 67 years.

- iv. Created before 1978 but not published or published after 1978. The copyright term starts 1978 and extends for the creator's life plus 70 years or 12/31/2002, whichever is greater.
 - v. Created after 1978. The term starts when created and extends for life of the creator plus 70 years, or if created by a corporation, the shorter of 95 years from publication or 120 years from creation.
3. Permission Granted for Use. There are two ways in which permission could occur.
- a. Permission for use is provided on material itself. For example, the material may contain a notice that states that reproduction for nonprofit, educational use is permitted. A copy of this notice must be supplied to.
 - b. Specific permission is obtained from copyright owner for use of the material on the web page.
4. Fair Use. The standard Fair Use Guidelines for Educators do NOT apply to material placed on school web sites. However, it is considered to be fair use to use copyrighted materials if the purpose is transformative, including review, criticism, or parody.

Web Site Management Chart

The following is a Web Site Management chart:

Material	Copyright status	Rationale or Basis
1. photos of XYZ	Teacher Original	Created by teacher
2. article about ABC	Permission granted	Permission from X attached
3. drawing of EFG	Public domain	Found in book that was published in 1909, title page attached.

Permission Request

The following is a Copyright Permission Request Template:

"Dear (name)

I am a student/staff at (name of school). I would like to use (describe the material) in the following manner (describe how you will use the material). Do you hold the copyright on this material? If you hold the copyright, may I have your permission to use your material in this way?

If you grant permission to copy this material, I will properly reference your ownership by (describe how).

I need to have your answer by (date)."

Copyright Management for Software

The following recommendations for effective copyright management for software come from the Technology Industry Association.

Nine Steps to Getting and Staying Legal

1. Appoint a software manager.
2. Create and implement a software policy and code of ethics.
3. Establish software policies and procedures.
4. Conduct internal controls analysis.
5. Conduct periodic software audits.
6. Establish and maintain a software log of licenses and registration materials.
7. Teach software compliance.
8. Enjoy the benefits of software license compliance.
9. Thank employees and students for participating⁶.

Copyright Concerns and Access to Quality Educational Materials

There are a number of positive ways that district can address copyright concerns as well as facilitate access to educational materials. These include:

- Use public domain or open systems resources whenever possible. In many cases, public domain resources are readily available to support a wide variety of educational activities.
- Develop collaborative approaches with other educators to create new public domain or inexpensive educational resources that can be used without the need to deal with the more expensive commercial publishers.
- Communicate directly with publishers about marketing and distribution practices that undermine the effective and legal use of their materials in the classroom.

⁶ Software and Information Technology Industry Association. *How Schools Can Spot, and Stop, Infringing Activity*. URL: http://www.siiia.net/piracy/policy/edu_spot.asp

10. Disability Information Technology Access

Serving All

An issue that can be guaranteed to emerge in the near future is the issue of disability information technology (IT) access to the district, school, and classroom web sites, distance education programs, and any other technology-related programs¹. As these web sites, distance education programs, and other technology programs are becoming an important vehicles for the provision of information and educational services to students, parents, and the community, the ability of *all* students, parents, and community members to be able to access information and participate in communications will become essential.

Responsibility Reasons

An estimated twenty percent of the population in the U.S. has some kind of a disability and ten percent has a severe disability. Individuals with disabilities frequently find that they are unable to access and use the information and communication resources on the Internet. This is unfortunate, because there are technologies and techniques that can be used to make these Internet resources fully available.

Schools should be on the vanguard of ensuring access to individuals with disabilities. The exchange of information is fundamental to education. Schools serve important constituencies, including students, their parents, and the community. If any individuals are cut off of access to vital information and participation in online exchange, this will reflect poorly on the entire school community.

Schools also should be preparing students with the knowledge and skills to develop web pages that incorporate disability IT access design principles. Students should not merely learn how to design web pages. They should learn the importance of and how to design accessible web pages.

Legal Standards

Several statutes address the rights of those with disabilities related to educational services. The Office for Civil Rights U.S. Department of Education indicated that, as of the date of the preparation of this Guide, there had been no complaints filed against K-12 public schools related to disability access to technology². Complaints and cases are emerging at the higher education level. It is considered only a matter of time before the issue emerges within K-12.

The following are the statutory provisions that address disability access to technology.

¹ As the author of this Guide is not a disabilities law expert, the following information presented in this document relied heavily on materials graciously provided by Tim Spofford, Civil Rights Attorney and OCR Internet Coordinator, Office for Civil Rights, US Department of Education, Seattle, Washington. The presentation materials addressing this issue are online at: URL: http://uwctds.washington.edu/ocr_slides/index.htm.

² Personal communication with Tim Spofford, August 2002.

Section 504 of the Rehabilitation Act of 1973

Section 504 prohibits discrimination against people with disabilities by recipients of federal financial assistance. This includes virtually all public and private colleges and universities, all public schools.

Pertinent 504 Requirements

- Entities providing any aid, benefit or service may not afford a qualified person with a disability an opportunity to participate that is not as effective as the opportunities provided to others³.
- Qualified students may not be excluded from a program or given different benefits or services in a program on the basis of disability⁴.
- Schools must make "academic adjustments" necessary to afford people with disabilities access to programs unless it would fundamentally alter an essential element of the program⁵.
- Academic adjustments include "auxiliary aids" necessary to provide access by those with sensory impairments⁶.
- "Methods of administration" of programs and activities may not have the effect of discriminating against people with disabilities⁷.

Title II of the Americans with Disabilities Act of 1990

Title II of the Americans with Disabilities Act (ADA) prohibits discrimination against people with disabilities by public entities. The definitions in ADA are the same as 504, but ADA contains some definitions not found in Section 504, such as "communication." The requirements of ADA are similar to Section 504.

Pertinent ADA Requirements

- Same requirements as Section 504 relative to different opportunities, different benefits, and different services for people with disabilities⁸.
- Recognizes the special importance of communications: "A public entity shall take appropriate steps to ensure that communications with applicants, participants, and members of the public with disabilities are as effective as communications with others⁹."
- Recognizes the importance of "customer preferences" regarding methods of communication for people with disabilities: "In determining what type of auxiliary aid and services is

³ 34 CFR 104.4(b)(1).

⁴ 34 CFR 104.4(b)(1).

⁵ 34 CFR 104.44(a).

⁶ 34 CFR 104.44(d)

⁷ 34 C.F.R. section 104.4(b)(4) & 28 C.F.R. § 35.130(a)

⁸ 28 CFR 35.130(b).

⁹ 28 CFR 35.160(a).

necessary, a public entity shall give primary consideration to the requests of the individual with disabilities¹⁰."

- Customer preferences related to communications need not be honored if the public entity can demonstrate that:
 - Another effective means of communication exists, or
 - The preference would result in a fundamental alteration of the program, or
 - The preference would result in undue financial and administrative burdens¹¹.
- A public entity shall administer services, programs, and activities in the most integrated setting appropriate to the needs of qualified individuals with disabilities¹². "Integration is fundamental to the purposes of the Americans with Disabilities Act. Provision of segregated accommodations and services relegates persons with disabilities to second-class status¹³."

Section 508 of the Rehabilitation Act of 1973

In 1998, Congress amended Section 508 of the Rehabilitation Act, strengthening the provisions covering access to information provided by Federal programs¹⁴.

Pertinent Section 508 Requirements

- The amendments require access to the Federal Government's electronic and information technology. Federal agencies must ensure that the technology is accessible to all employees and the public -- to the extent that it does not pose an "undue burden¹⁵."
- Covers all types of electronic and information technology in the Federal sector and applies to all Federal agencies when they develop, procure, maintain, or use such technologies¹⁶.
- The law directed the Access Board to develop access standards for the technology that will become part of the Federal Procurement regulations. These standards were developed and approved by the Access Board¹⁷. The standards are useful guidelines for schools in addressing access.
- Section 508 of the Rehabilitation Act applies to Federal agencies. However, states receiving assistance under the Assistive Technology Act State Grant are required to comply with Section 508. The U.S. Department of Education is developing guidelines for how the Section 508 standards apply to states under the Assistive Technology Act.

Basic Civil Rights Objectives of Section 504, the ADA, and Section 508

- End isolation of persons with disabilities.

¹⁰ 28 CFR 35.160(b)(2)

¹¹ 28 CFR 35.160(b)(2).

¹² 28CFR 35.130(d), see also 34 CFR 104.4(b)(2).

¹³ Analysis of the Final Title II Regulation, 28 CFR Part 35.

¹⁴ Section 508 of the Rehabilitation Act Amendments of 1998 (29 USC 794d)

¹⁵ *Id.* at Subpart A § 1194.1.

¹⁶ *Id.* at Subpart A § 1194.2.

¹⁷ 36 CFR Part 1194.

- Secure equal opportunity.
 - Not necessarily identical treatment.
 - Equivalent treatment (comparative).
 - Remove unnecessary barriers through academic adjustments and auxiliary aids.
- Foster independence.
- Prevent a hostile environment.

Summary of Information Technology Access Principles

The following summary of principles should guide a school district's efforts to achieve disability IT access:

- Students must be provided equally effective access to educational programs.
- Every "program" and "activity" is covered, including:
 - On-site programs and off-site programs.
 - Programs receiving "significant assistance."
 - Non-academic programs.
- The goal is "equally effective ... communication"- a comparative standard for access to information.
- Law contemplates increased independence for people with disabilities through accessible technology.
- The preferences of consumers with disabilities need to be seriously considered.
- Failure to plan for technology access and ad hoc approach may result in denial of access.
- Institutions' responsibilities aren't without limits. Modifications and auxiliary aids and services not required if they would fundamentally alter the program or conflict with essential program requirements.
- The following considerations should be addressed related to the "communications ... as effective as" requirement of the ADA:
 - Timeliness and accuracy.
 - Provision in a manner and medium appropriate to the significance of the message.
 - Comparable burden.
 - Audience for web content will have a variety of needs that must be addressed.

Policies and Procedures to Help Ensure Disability IT Access

- School district policies should address disability IT access in all technology-related programs, including:

- Standards for ensuring accessibility.
 - Guidelines to ensure technology procurement considers access.
 - Determination of what components are responsible for costs of access.
 - Publication of effective procedures for delivery of needed AT.
- With respect to accessibility to district, school, and class web sites and distance education programs, the district should
 - Adopt an unambiguous policy requiring accessible web sites and educational programs.
 - Publicize the policy.
 - Adopt a plan for compliance.
- Newly published content and classes should meet accessibility standards.
- Plan for access to existing content:
 - Core content (home pages, student services pages, catalog, registration, site map, what's new, etc.) should be made accessible within short, specified, period of time.
 - Existing active course content should be made accessible within short, specified, period of time.
 - Include a plan for retrofitting active secondary content.
 - Historical (inactive) content should be provided in accessible format when a request is received.

Online Guidelines and Resources for Accessible Web Design

The following web sites have excellent standards and information resources for disability IT access:

- Web Accessibility Initiative/ World Wide Web Consortium (W3C/WIA) Web Content Accessibility Guidelines 1.0¹⁸.
- Section 508 Standards of the Access Board¹⁹ and Free GSA courses: "508 Universe"²⁰.
- AccessIT: The National Center on Accessible Information Technology in Education at the University of Washington²¹

¹⁸ URL: <http://www.w3.org/WAI>.

¹⁹ URL: <http://www.access-board.gov/sec508/508standards.htm>.

²⁰ URL: <http://www.section508.gov/508/>.

²¹ URL: <http://www.washington.edu/accessit/index.php>.