

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 II. Safe and Responsible Internet Use Plan

1. The Children's Internet Protection Act

(Note: For non-U.S. readers, compliance with CIPA is a non-issue. The chapters in this Part address the requirements for an Internet Safety Plan under the framework set forth in CIPA. Notwithstanding the concerns in the U.S. that CIPA has fostered false security with its requirement for the installation of a technology protection measure, the requirements for the Internet Safety Plan are very sound. Therefore, while the following chapters will follow the outline set forth in the CIPA legislation, the issues addressed are universal to any school in any country.)

The CIPA Legislation

The Children's Internet Protection Act (CIPA) was enacted as part of the Consolidated Appropriations Act of 2001¹. CIPA requires all schools receiving funding through the E-rate program and technology funding through Title III of the Elementary and Secondary Education Act to comply with certain requirements. CIPA was enacted to address Congress's concern that "(a)lthough the Internet represents tremendous potential in bringing previously unimaginable education and information opportunities to our nation's children, there are very real risks associated with the use of the Internet." As Congress found, "(p)ornography, including obscene material, child pornography, and indecent material is available on the Internet²."

The CIPA statute was a late session merger of two similar statutes that were pending before Congress, the CIPA and the Neighborhood Children's Internet Protection Act (NCIPA). NCIPA was the result of an effort by some members of Congress to require that districts develop strategies to address the concerns, but the law did not dictate a technological solution. The CIPA provisions of the law address the requirements for the use of a "technology protection measure."

The NCIPA portion of the law requires the development of an Internet Safety Plan. The requirements are well-founded and provide an excellent basis for district planning. Unfortunately, far too many districts have focused on the CIPA provisions and the use of technology protection measures and have not focused strongly enough on the NCIPA provisions addressing an Internet Safety Plan.

On April 5, 2001, the Federal Communication Commission (FCC) issued regulations for the implementation of CIPA³. The Schools and Libraries Division⁴, which is charged with management of the E-rate program, has complete information for schools regarding timelines and certifications.

The Basic CIPA Requirements

Under CIPA and NCIPA, any school that seeks federal funding through the e-rate program or through any U.S. Department of Education technology-funding program must:

1. Enforce a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors⁵. (CIPA)
2. Enforce a policy of Internet safety with respect to adults that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene or child pornography⁶. (CIPA)

¹ The best resource for a copy of the law is a version excerpted from the Appropriations Act that has been placed on the American Library Association web site. URL: <http://www.ALA.org/cipa/Law.PDF>

² Senate Rpt. 106-141 - *CHILDREN'S INTERNET PROTECTION ACT*, Page 2.

³ 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

⁴ URL: <http://www.sl.universalservice.org/>

⁵ 47 U.S.C. 254(h)(5)(B)

⁶ 47 U.S.C. 254(h)(5)(C)

3. Adopt an Internet Safety Plan that addresses the following elements:
 - a. Access by minors to inappropriate matter on the Internet and World Wide Web.
 - b. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
 - c. Unauthorized online access by minors, including “hacking” and other unlawful activities.
 - d. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
 - e. Measures designed to restrict minors’ access to materials harmful to minors⁷. (NCIPA)
4. Provide public notice and hold a public hearing regarding the Internet Safety Plan⁸. (NCIPA)

Most school districts in the country are in compliance with CIPA, or have declined to participate in the E-rate program and any technology funding from the U.S. Department of Education and thus do not need to comply with CIPA. This Guide fully embraces the components of the Internet Safety Plan required under NCIPA, as these provide an excellent framework for the development of policies, regulations, and instruction to address the safe and responsible use of the Internet by students. The author has chosen to refer to this plan as the Safe and Responsible Internet Use Plan because of the perception that safety and responsibility are the two sides of one coin.

Questions Regarding Constitutionality of CIPA

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 Act⁹ (CIPA), *ALA v. US*¹⁰. 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 Internet. . 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.¹¹"

⁷ 47 U.S.C. 254(l)(1)(A))

⁸ 47 U.S.C. 254(h)(5)(A)(iii))

⁹ Pub. L. No. 106-554.

¹⁰ *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.* (June 2002) URL: <http://www.paed.uscourts.gov/documents/opinions/02d0415p.htm>

¹¹ *ALA* at V.B.

This ruling was appealed to the U.S Supreme Court. The Supreme Court overruled the district court in a ruling issued on June 23, 2003¹². The Supreme Court's determination that CIPA was constitutional was grounded in the understanding that while filters may block access to material that is constitutionally protected, they can be totally disabled for use by any adult¹³. In the case of minors, any site that is erroneously blocked can be unblocked¹⁴.

Unfortunately, the manner in which the case was presented by the ALA and ACLU led to a decision that did not fully address the interests of minors of access to constitutionally protected material other than the fact that the filter may be overridden to unblock access to an inappropriately blocked site.

A separate decision issued by Justice Kennedy raises a very significant point. Justice Kennedy noted that the decision addressed the CIPA statute on its face. The Justice noted that if the manner in which the statute was implemented in a specific setting in a manner so that a user's access to constitutionally protected material is burdened in some substantial way, this could give rise to an as-applied constitutional challenge.

From the perspective of schools, the significant question is whether the district has implemented the use of filtering in a manner that has placed a substantial burden on student access to constitutionally protected material.

This issue is addressed more fully in Chapters II-3 and III-6. The following are questions that district should consider:

- Does your district have full and complete knowledge of what sites are being blocked and the basis upon which these decisions are made? Have the companies made full public disclosure of this information as necessary to ensure public accountability?
- Has the determination of which categories of material should be blocked been made by school administrators, in accord with the district's determination of what kinds of material should be considered to be inappropriate, and with full knowledge of the kinds of material blocked in those categories? Or has the district's technology services personnel or the filtering company made the determination of what categories are blocked (district using company's default setting)?
- Has the district set the filter to block many categories, which significantly increases the rate of overblocking, or has the district set the filter to block only the categories necessary to be blocked under CIPA?
- Has the district established effective procedure to override the filter in cases when the filter is blocking access to educational material or any material students have a constitutional right to access? Does this process ensure rapid response? Have procedures been established to allow

¹² *United States v. American Library Association*, No. 02-361 In the Supreme Court of the United States. (June 23, 2003) <http://www.supremecourtus.gov/opinions/02pdf/02-361.pdf>

¹³ *Id.*, page 12.

¹⁴ *Id.*, page 12.

students to anonymously request a site be overridden to allow for access to sensitive material?

- Are district officials conducting a periodic review of the filter reports to determine the effectiveness of the district's education (are students accidentally accessing inappropriate sites?), supervision (are students intentionally trying to access inappropriate sites?) and the process to override (are students being prevented from accessing appropriate, constitutionally protected material)?

2. *Inappropriate Material*

CIPA Requirements

- (1) IN GENERAL In carrying out its responsibilities under subsection (h), each school or library to which subsection (h) applies shall--
 - (A) adopt and implement an Internet safety policy that addresses the following elements:
 - (i) access by minors to inappropriate matter on the Internet and World Wide Web; (No definition was provided for the term "inappropriate matter.")
 - ...
 - (v) measures designed to restrict minors' access to materials harmful to minors¹.
- (2) 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)².

Defining "Inappropriate"

Objectives

Districts will need to specify to students and staff what kinds of material is considered to be inappropriate to access when using the district's Internet system. The challenge for school districts is to develop a list of the kinds of material that meet the following objectives:

- Effectively outlines the parameters of what is and is not acceptable in accord with educational and pedagogical goals.
- Communicates this information in a manner that is not vague.

¹ 47 U.S.C. 254 (I)(1)(A)(ii).

² 47 U.S.C. 254 (l)(2). Under 47 U.S.C. 254 (h)(7)(G), the Technology Protection Measure must protect against access to visual depictions that are obscene, child pornography, or harmful to minors. The following are the definitions of these terms provided in the statute: "Obscene. The term 'obscene' has the meaning given such term in section 1460 of title 18, United States Code (47 U.S.C. 254 (h)(7)(E)). Child Pornography. The term 'child pornography' has the meaning given such term in section 2256 of title 18, United States Code (47 U.S.C. 254 (h)(7)(F)). Harmful to minors. The term 'harmful to minors' means any picture, image, graphic image file, or other visual depiction that -- (i) taken as a whole and with respect to minors, appears to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable to minors, as actual or simulated sexual act or sexual conduct, actual or simulated normal or perverted sexual acts, or lewd exhibition of genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors." School districts should be careful to distinguish between materials that Congress has required that a technology protection measure should be used to address and materials that the district decided are inappropriate.

- Does not result in the restriction of student access to information based on viewpoint discrimination.
- Promotes, rather than restricts, the effective use of the Internet for educational purposes.
- Addresses the legitimate concerns of parents and community members.

Constitutionality

Supreme Court standards related to the importance of student access to information and the constitutional standards guiding such access were eloquently set forth in the case of *Board of Education, Island Trees Union Free School District No. 26 v Pico*³:

"(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 curriculum....'

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 precedents⁴.

It is essential that school officials make the determination about the “inappropriateness” of certain material in a manner that upholds this constitutional standard. If the district is using a technology protection measure that blocks access to certain sites, it is essential to determine whether or not the company is making decisions in a manner that results in viewpoint discrimination.

³ 457 US 853 (1982).

⁴ *Id.* at 866-896 (citations and quotations omitted).

District Determination

In far too many districts, the determination of what material is considered inappropriate is made based on an evaluation of the categories established by a company providing a technology protection measure. This is totally backwards and irresponsible decision-making.

As the *NRC Report* noted:

The determination that particular material is inappropriate for children begins with a human judgement. ... Given a particular universe of material ..., it is likely that any group of judges will agree on some material as "appropriate" and some as "inappropriate," and that there will be some material about which the judges will disagree. ... Indeed, judgments about inappropriateness are closely tied to the values of those making the judgments⁵.

School officials should make the determination about what kinds of material are considered to be inappropriate under local community values, not the private companies that are providing a blocking product. Districts must then clearly ascertain whether or not a particular product blocks access in accord with local community standards. This determination will require full disclosure about what kinds of material are blocked in each category that is under consideration to be blocked by the district.

Separate Questions

The determination of what material is considered to be inappropriate should be made in a manner that is separate from a determination of what categories to block if a district is using a technology protection measure that blocks access to categories of sites. Under CIPA only the category that blocks access to adult sexually related material is required to be blocked.

Districts that use filters for Internet use management – blocking many categories in an effort to manage student use – essentially are demonstrating that they have not focused strongly enough on professional development, education, and supervision. If the district's computers are being used effectively for quality educational activities, if students have been effectively informed of district access policies, and if Internet use is effectively supervised by school personnel, there should be no need to block access beyond that required under CIPA.

If student misuse of the Internet is such that some in the district are arguing for the blocking of additional categories, this should be considered clear evidence of the failure to establish a comprehensive approach to address the safe and responsible use of the Internet.

Clarity

Some Internet use policies contain language such as: "Students shall not access material that is objectionable, inappropriate, and/or inaccurate." Standards such as these clearly do not meet the above objectives. When districts do not clearly outline what students can and cannot access this places students at significant risk of restrictions or being subjected to discipline based on the

⁵ National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002). URL: http://bob.nap.edu/html/youth_internet/ at Section 8.1.1.

individual perceptions of a staff member regarding what kinds of material are appropriate or inappropriate based on their own value personal system.

Recommended Classifications

It is recommended that districts consider the establishment of three classifications of inappropriate material: Prohibited, Restricted, and Limited Access. The following material describes the types of material that could fit into each of these categories with sufficient clarity to provide adequate notice to students. Ultimately, decisions about the classification should be made at the local community level. Therefore, the following recommendations should be considered starting points for discussion.

- Prohibited Material Prohibited Material may not be accessed by the students or staff at any time, for any purpose. This material includes material that is obscene, child pornography, material that is considered harmful to minors, as defined by the Children's Internet Protection Act. The district designated the following types of materials as Prohibited: Obscene materials, child pornography, material that appeals to a prurient or unhealthy interest in, or depicts or describes in a patently offensive way, violence, nudity, sex, death, or bodily functions, material that has been designated as for "adults" only, and material that promotes or advocates illegal activities.
- Restricted Material Restricted Material may not be accessed by elementary or middle school students at any time for any purpose. Restricted Material may be accessed by high school students in the context of specific learning activities that have been approved by a teachers or by staff for legitimate research or professional development purposes. Materials that may arguably fall within the description provided for Prohibited Material that have clear educational relevance, such as material with literary, artistic, political, or scientific value, will be considered to be Restricted. In addition, Restricted Material includes materials that promote or advocate the use of alcohol and tobacco, hate and discrimination, satanic and cult group membership, school cheating, and weapons. Sites that contain personal advertisements or facilitate making online connections with other people are Restricted unless such sites have been specifically approved by the school.
- Limited Access Material Limited Access Material is material that is generally considered to be non-educational or entertainment. Limited Access Material may be accessed in the context of specific learning activities that are directed by a teacher or during periods of time that a school may designate as "open access" time. Limited Access Material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investments.

Rationale for Three Categories

The rationale for the establishment of three categories is that there is some material that should simply never ever be accessed through an educational Internet system – period, full stop, end of discussion. However, there is other material that may present significant concerns if students are freely accessing such material, but may also be quite appropriate for older students if accessed in the context of approved learning activities. An example of type of material that would fall into the Restricted category is "hate literature." Many districts would conclude that students should generally not be allowed to access hate literature. But what about the class that is studying

Osama bin Laden? Or the student who wants to do a senior research project on online hate groups? Or the student who wants to research Holocaust revision sites as part of a history study?

How can schools adequately prepare students for "the real world" if students are prevented from learning how to recognize, analyze, interpret, and challenge hate literature or other kinds of "controversial" information? Districts should consider a category of materials that are generally considered to be inappropriate, but may be appropriate for older students to access in the context of specifically approved learning activities. Obviously, schools will need to establish specific requirements to authorize access of such material. In many cases, it would be advisable to inform parents of the intention to allow such access and offer alternative learning activities if a parent objects.

There is other material that is generally not educational, but is more for the purposes of entertainment. Access to such sites would not generally meet the definition of "educational purpose" and may be considered to be inappropriate for this reason. But there are occasions where access to such material may be perfectly appropriate and even desirable. Innovative teachers are using popular culture sites, such as rock star or sports hero sites, in the context of valuable, engaging learning activities. Some schools may also want to allow certain times for students to use the Internet on a more open access basis. During such times, which should be clearly specified, access to entertainment or other generally non-educational sites may be perfectly acceptable.

Other Inappropriate Material Issues

Material That is Not in Accord with Values Held by Individual Families

When the district opens up discussions about to the appropriateness or inappropriateness of certain material to parents and community members, there may be efforts to have the district limit access based on specific values of certain families or community groups. Frequently, the types of restrictions advocated will raise concerns of preventing access to information based on viewpoint discrimination.

The district simply cannot enforce a wide range of family values when students are using the Internet. This point must be made clear to all parents, as well as the community. Public institutions have an obligation to conduct their affairs in accord with constitutional law that prohibits the restriction of access to information based on viewpoint discrimination.

However, the district can and should encourage parents to discuss their values with children and encourage students to make decisions regarding their use in accord with their personal and family values, in addition to the school standards. Districts can and should also provide a vehicle for parents to have access to their child's Internet usage records and facilitate their ability to review these logs if they do not have Internet access at home. In this manner, if a parent determines that their child is not using the Internet in accord with their personal family values, that parent can terminate their child's right to access the Internet at school.

It is unlikely that many parents will request such access on a frequent basis. But some may. And many more will appreciate the district's responsiveness to their interest and concern. Further, the

Safe and Responsible Use of the Internet – Part II, Chapter 2, page 5

fact that students know that their parents can have access to their logs and e-mail at any time will likely have a dampening impact on those who might be inclined to wander into areas that they know would be considered inappropriate.

Teenagers and Use of the Term "Inappropriate to Minors"

There should be recognition of how this term "inappropriate for minors" is interpreted by teenagers. Indicating to teenage students that certain material is inappropriate for them to look at because they are not old enough to look at it is like painting a red bull's eye on that material. Why? In addition to the general perspective of teenagers that they are old enough for anything, the entertainment industry has been capitalizing on youth rebellion to market adult-rated material to teenagers for a very long time. They have been working closely with child psychologists and marketing specialists to find the best way to utilize restricted ratings as a marketing advantage to reach the teenage audience. For many teenagers, if it is not adult-rated, it is not "cool" and if they are not trying to get to adult-rated stuff, they are not "cool."

Students are generally smart enough not to look at such material in school because of the potential of detection. But if they are told they are not old enough to look at something, which is the first thing they are likely to do, when given the opportunity. And they will have the opportunity.

The stronger arguments against such materials relate to the violence and disrespect that such materials depict, foster, or encourage. Fortunately our society is becoming more sensitive to the level of media violence and the impact of such violence on people. Schools have made progress in creating healthy school environments that foster respect for all students. Addressing issues of harmful online materials in the context of programs that address hate speech, sexual harassment, discrimination, and bullying will be a more effective educational strategy. Issues related to sexually violent pornography should be integrated into sexual education classes.

Comprehensive Sexual Education Material

Some educators, parents, and/or community members may question whether students ought to be allowed to access comprehensive online sexual education information. There are some very strong arguments for why such information should be provided in a careful and appropriate manner.

A recent study by the Kaiser Family Foundation⁶ revealed that 68% of teenagers had use the Internet to find health information. Of this, 44% sought sexual health information. Nearly half, 46%, of the teenagers reported that they had been blocked from accessing perfectly appropriate health sites by filtering software. However, also of concern is the fact that 70% of the teenagers reported accidentally accessing pornography and just under half (45%) indicated that they were upset by this experience⁷.

⁶ Rideout, V., 2001. *Generation Rx.com: How Young people Use the Internet for Health Information*, The Henry J. Kaiser Family Foundation. Menlo Park, CA. URL: <http://www.kff.org/content/2001/20011211a/>

⁷ If 70% of teenagers are accidentally accessing pornography, this means we clearly need to do a better job of educating them how not to access pornography.

Regardless of desires that it not be so, many teenagers are sexually active. They are engaged in sexual intercourse. They are becoming pregnant. They are becoming inflicted with sexually transmitted diseases, including HIV/AIDs. To deny teenagers access to information that will protect their health and well being simply because of a desire that they not engage in sexual activity is simply unconscionable⁸.

If teenagers are interested in finding information about sexual health information on the Internet, they will do so. If they search for such information through standard online search engines, their quest will likely require sifting through a wide range of material that would be considered by most concerned adults to be inappropriate for teenagers.

Clearly, the best way to address the concerns in this area is using an inclusion approach -- providing students with access to sites that have been pre-selected by education and health care professionals as being appropriate sexual education sites for students. A truly comprehensive approach to the development of such list of approved sites is recommended. Again, if students do not find the information they want or need, they can, and likely will, look for this information in less wholesome environments.

Staff members

The CIPA requirements related to the use of Technology Protection Measures and restrictions on staff use are very bizarre. Essentially, under CIPA, schools are required to certify that they have installed a Technology Protection Measure to protect minors against access to material that is obscene, child pornography, and material that is harmful for minors. But the provisions for adults in schools require only that material that is obscene and child pornography be restricted. Presumably, Congress felt that it should be perfectly appropriate to allow school staff to access Internet material that is harmful to minors.

This provision represents disconnect from reality. There is absolutely every reason to restrict staff access to inappropriate material on the Internet in the same manner as students. *NO* parent would be comfortable having his or her child in school with a teacher or other staff member who is interested in Internet material that meets the CIPA definition of harmful to minors.

⁸ The vast majority of parents support comprehensive sex education in schools. Another study by the Kaiser Family Foundation revealed that the majority of parents want their children to receive information on a wide range of sexual issues, including safe sex, contraception, abortion, and sexual orientation information. When given a choice, only 1% to 5% of parents remove their children from comprehensive sexual education classes. Kaiser Family Foundation. *Sex Education in America: A View from Inside America's Classrooms*. (Menlo Park, CA, 2000) URL: <http://www.kff.org/content/2000/3048/SexED.pdf>
Safe and Responsible Use of the Internet – Part II, Chapter 2, page 7

3. Technology Protection Measures

CIPA Requirements

- (A) Internet Safety
 - (i) IN GENERAL.--...(A)n elementary or secondary school having computers with internet access may not receive services at discounted rates under paragraph (1)(B) unless the school, school board, local education agency, or other authority with responsibility for administration of the school--
 - (I) submits to the Commission the certifications described in subparagraphs (B) and (C); ...
- ...
- (B) CERTIFICATION WITH RESPECT TO MINORS.-- A certification under this subparagraph is a certification that the school, school board, local education agency, or other authority with responsibility for administration of the school--
 - (i) is enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--
 - (I) obscene;
 - (II) child pornography; or
 - (III) harmful to minors; and
 - (ii) is enforcing the operation of such technology protection measure during any use of such computers by minors."¹
- (1) TECHNOLOGY PROTECTION MEASURE.--the term 'Technology Protection Measure' means a specific technology that blocks or filters Internet access to visual depictions that are-- (the prohibited material)².

Complying with CIPA Without Using Commercial Filtering Software

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

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

Commenters discussed the difficulty that some educational institutions have interpreting CIPA's "technology protection measure" language. Some commenters claim that many educational institutions default to "filtering" technology only, without researching other

¹ 47 U.S.C. 254 (h)(5)(B)

² 47 U.S.C. 254 (h)(7)(I)

types of technology protection options. As a result, many believe that this reliance on mostly filtering products stifles the marketplace and serves as a disincentive for technology companies to invest in the research and development of newer and more sophisticated products. Moreover, as set forth above, filtering and blocking software has not been able to overcome problems of overblocking, inability to generate an updated index for the Internet, and lack of correspondence to statutory definitions and categories. Yet, other technology tools can or have the potential to address better the needs of educational institutions. Thus, NTIA recommends that Congress change the current legislation to clarify that the term “technology protection measure” encompasses not only filtering and blocking software, but also other current and future technology tools. ... Alternatively to amending CIPA, NTIA recommends that the FCC and the U.S. Department of Education (DOE) provide further guidance to recipients of E-rate or DOE funds on the meaning of technology protection measures³.

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

NRC Report -- Analysis of Protection Technologies

The NRC committee was charged with the task of conducting a study of "computer-based control technologies" and other approaches to address the concerns of pornography on the Internet⁴. The NRC committee conducted a full study of various technologies that "can be used to *protect* or limit children's exposure to inappropriate sexually explicit material on the Internet⁵." Note the use of the term "protect," which is the same term used in the CIPA legislation.

Table 12.1, of the *NRC Report*, entitled Technology-Based Tools for the End User, is perhaps the most comprehensive list of the types of technologies that function, according to the NRC, to *protect* against access to inappropriate material. Presumably, the types of technologies contained on this list are ones that a school district could consider adopting to comply with CIPA⁶.

The NRC committee was charged with the task of conducting a study of "computer-based control technologies" and other approaches to address the concerns of pornography on the Internet⁷. The NRC's conclusion was that while technologies had a role to play in the protection of youth, social and educational strategies must provide the foundation for the protection of children. The NRC committee conducted a full study of various technologies that "can be used to *protect* or limit children's exposure to inappropriate sexually explicit material on the Internet⁸."

³ U.S. Department of Commerce, National Telecommunications and Information Administration, <http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/>.

⁴ P.L. 105-314, the *Protection of Children from Sexual Predators Act of 1998*, Title IX, Section 901.

⁵ National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002). URL: http://bob.nap.edu/html/youth_internet/.

⁶ With the exception of Instant Help, which the NRC indicated was an after-the-fact solution.

⁷ P.L. 105-314.

⁸ NRC report at Section 11.3.

Table 12.1, entitled Technology-Based Tools for the End User, a recent comprehensive list of the types of technologies that function to protect against access to inappropriate material. Presumably, the types of technologies contained on this list are ones that a school district can adopt to comply with CIPA⁹.

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

The information needs of children that the Internet can and should meet also change with the developmental stage of the child in question. For example, juniors and seniors in high school have a much broader range of information needs (i.e., for doing research related to their education) than do those in the third grade or in junior high school. This, in turn, leads to the question of how to provide older children with access to a broader range of material while preventing younger ones from accessing material that is deemed not appropriate given their developmental level¹⁰.

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

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

NRC Technology-Based Tools Table

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

Type of Tool	Function	One Illustrative Advantage	One Illustrative Disadvantage	Voluntary versus Involuntary Exposure
1. Filter	Block "inappropriate" access to prespecified content; typically blocks specific web pages, may also block generic access to instant messages, e-mail, and chat rooms	Can be configured to deny access to substantial amounts of adult-oriented sexually-explicit material from commercial web sites	In typical (default) configuration, generally denies access to substantial amounts of Web material that is not adult-oriented and sexually explicit.	Protects against both deliberate and inadvertent exposure for sites that are explicitly blocked; can be circumvented under some circumstances

⁹ With the exception of Instant Help.

¹⁰ NRC, *supra* at Section 14.1.2.

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	Requires responsive infrastructure of helpers	Mostly relevant to inadvertent exposure

		need		
--	--	------	--	--

Technology Protection Measure Recommendations

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

Filtering based on first party content labeling

This technology is a combination of categories 1 and 3 above. The Internet Content Rating Association has been leading an international effort to encourage labeling of web sites¹¹. 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 providers¹².

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

¹¹ <http://www.icra.org>.

¹² NRC, *supra* at Section 12.1.5.

they use and the keyword that they use to identify suspicious sites, it is likely that such products are sufficiently "open" to meet the requirements of local control and public accountability.

Because these products are not likely as robust as the commercial, proprietary-protected products, they 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 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 assistance¹³

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 on 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 ISPs, 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

¹³ NRC, *supra* at Section 12.1.6.

entertaining. (This approach is known as "white listing" -- all content not on a white list are disallowed,¹⁴)

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

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

¹⁴ NRC, supra at Section 12.1.1.

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 Internet¹⁵.

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 material¹⁶. 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 footnote¹⁷ 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 met¹⁸."

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 action¹⁹.

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

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

If monitoring is coupled to explanations and guidance about appropriate and inappropriate behavior, there is some potential that this application can promote the long-term development and internalization of appropriate behavioral norms. But the explanation and guidance are essential. If, as is much more likely in an institutional

¹⁵ NRC, *supra* at Section 12.2.1.

¹⁶ 47 U.S.C. 254 (h)(5)(B).

¹⁷ NRC *supra* at Section 12.2 (footnote 38).

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

¹⁹ NRC, *supra* at Section 12.2.2.

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.

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

Instant Help

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

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

Commercial, Proprietary-Protected Filtering Software

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

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

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

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

To address concerns over the potential of intentional viewpoint discrimination it is necessary to thoroughly investigate the company to determine its values and biases that may impact blocking decision-making. Information to request should include the database of blocked sites, specific information on blocking criteria for any category you are considering blocking including the keywords used to search for sites to be blocked, background information on all leading corporate officials, and a detailed list of all major corporate clients.

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

The author of this Guide has discovered eight filtering software companies with very close relationships with conservative religious organizations²⁰. Relationships such as these could result in significant blocking based on viewpoint discrimination.

Block the least number of categories necessary.

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

Recently, the Kaiser Family Foundation reported on its study on the ability to access sites containing health information across a broad range of topics when filtering software has been installed²¹. This study assessed the performance of the top six selling filtering products in public schools. The filters were configured at a least restrictive level, intermediate constrictive level, and most restrictive level. The health information sites included topics unrelated to sex, topics related to sexual body parts, topics related to sex, and sites presenting potentially controversial health information.

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

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

²⁰ See, Filtering Software: The Religious Connection at <http://responsiblenetizen.org/documents/religious1.html>.

²¹ Kaiser, *supra*.

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

As noted in Chapter II-2, any district that feels it necessary to block multiple categories to effectively manage student Internet use should take a long close look at the effectiveness of its professional development supporting the effective educational use of the Internet, education, and supervision.

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

The Kaiser Family Foundation, also assessed the effectiveness of proprietary-protected filtering software in preventing access to inappropriate material²². As one component of the study, the researchers assessed the ability to intentionally access pornography sites. Roughly one in ten porn sites were accessible regardless of how the filters were configured (least -- 87% of pornography sites blocked; intermediate -- 90% of pornography sites blocked; most - 91% of pornography sites blocked). When the researchers assessed the ability of filters to block access under conditions simulating accidental access at the least restrictive level, only 62% of the pornography sites were blocked.

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

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

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

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

Regularly review the performance of the filtering product.

²² Kaiser Family Foundation (2002), *See No Evil: How Internet Filters Affect the Search for Online Health Information Executive Summary*. http://www.kff.org/content/2002/3294/Internet_Filtering_exec_summ.pdf.
Safe and Responsible Use of the Internet – Part II, Chapter 3, page 11

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

Comments made by NTIA made by author:

Complying with CIPA Without Using Commercial Filtering Software

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

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

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

Statutory Provisions

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

... (T)he operation of the Technology Protection Measure with respect to any of its computers with Internet access *that protects against access* through such computers to visual depictions that are -- (I) obscene; (II) child pornography; or (III) harmful to minors; ...²³

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

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

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

The NCIPA statute also contains the following provision:

²³ 47 U.S.C. 254 (h)(5)(B)

²⁴ 47 U.S.C. 254 (h)(7)(I)

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)²⁵.

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

FCC Regulations Related to Technology Protection Measures

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

- 33. Some commenters have requested that we require entities to certify to the effectiveness of their Internet safety policy and Technology Protection Measures. However, such a certification of effectiveness is not required by the statute. Moreover, adding an effectiveness standard does not comport with our goal of minimizing the burden we place on schools and libraries. Therefore, we will not adopt an effectiveness certification requirement.
- 34. A large majority of commenters express concern that there is no Technology Protection Measure currently available that can successfully block all visual depictions covered by CIPA. Such commenters seek language in the certification or elsewhere “designed to protect those who certify from liability for, or charges of, having made a false statement in the certification” because available technology may not successfully filter or block all such depictions. Commenters are also concerned that Technology Protection Measures may also filter or block visual depictions that are not prohibited under CIPA.
- 35. We presume Congress did not intend to penalize recipients that act in good faith and in a reasonable manner to implement available Technology Protection Measures. Moreover, this proceeding is not the forum to determine whether such measures are fully effective.²⁶

²⁵ 47 U.S.C. 254 (1)(2)

²⁶ FCC Order, *supra*.

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.

Comments Senator McCain, Chief Sponsor of CIPA

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

Washington, D.C. – Senator John McCain (R-AZ), Chairman of the Committee on Commerce, Science, and Transportation, today made the following statement in response to the American Civil Liberties Union (ACLU) court challenge to the Children's Internet Protection Act:

"The Children's Internet Protection Law, which passed the Senate 95-3 and has consistently enjoyed enormous bipartisan support, simply ensures that schools and libraries across the country have the technology they need to protect children from harmful material on the Internet. *This law gives communities the freedom to decide what technology they choose to use and what to filter out.* It does not dictate any specific actions be taken by communities or apply a federal standard, it simply requires them to have *some technology* in place to protect children if they are using federal funds for Internet access²⁷.

NRC Report -- Analysis of Protection Technologies

The NRC committee was charged with the task of conducting a study of "computer-based control technologies" and other approaches to address the concerns of pornography on the Internet²⁸. The NRC committee conducted a full study of various technologies that "can be used to *protect* or limit children's exposure to inappropriate sexually explicit material on the Internet²⁹." Note the use of the term "protect," which is the same term used in the CIPA legislation.

Table 12.1, of the *NRC Report*, entitled Technology-Based Tools for the End User, is perhaps the most comprehensive list of the types of technologies that function, according to the NRC, to *protect* against access to inappropriate material. Presumably, the types of technologies contained on this list are ones that a school district could consider adopting to comply with CIPA³⁰. The types of tools and description of function provided by NRC are as follows in columns 1 and 2. Column 3 is additional material the author of this Guide has added to describe more specific technologies of the type noted.

²⁷ URL: <http://mccain.senate.gov/intfilt01.htm>. Tuesday, March 20, 2002. Emphasis added.

²⁸ P.L. 105-314, the *Protection of Children from Sexual Predators Act of 1998*, Title IX, Section 901.

²⁹ National Research Council. *Youth, Pornography, and the Internet* at 11.3. (Dick Thornburgh & Herbert S. Lin, eds., 2002) URL: http://bob.nap.edu/html/youth_internet/

³⁰ With the exception of Instant Help, which the NRC indicated was an after-the-fact solution.

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

Type of Tool	Function	Author's Comment
1. Filter	Block "inappropriate" access to prespecified content; typically blocks specific web pages, may also block generic access to instant messages, e-mail, and chat rooms.	<ul style="list-style-type: none"> - Filtering based on first party content labeling [e.g., Internet Content Rating Association (ICRA) set to block access to sites that have labeled themselves as adult sites -- a combination of technologies #1 and #3. - Filtering software where processes and blocked list are not confidential. - Filters that can be set to "warn" but not block.
2. Content-limited access	Allow access only to content and/or services previously determined to be appropriate.	<ul style="list-style-type: none"> - Subscription services. - Proxy Server. - ICRA system set to allow access to predefined list of sites.
3. Labeling of content	Enable users to make informed decisions about content prior to actual access.	Content labeling (#3) is an activity that can support filtering (#1) and content limited access (#2). ICRA is leading the effort in content labeling.
4. Monitoring with individual identification	Examining a child's actions by an adult supervisor in real time or after the fact.	- Filtered monitoring tools filter Internet traffic and report on traffic that is suspected to be in violation of policy ³¹ .
5. Monitoring without individual identification	Watch the collective actions of a group (e.g., a school) without identifying individuals.	Without the ability to identify specific individuals, the effectiveness of this technology would be in question.
6. Spam-controlling tools	Inhibit unsolicited e-mail containing sexually explicit material (or links to such material) from entering	Spam-controlling software is a must at some location within the e-mail communication system.

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

	child's mailbox.	
7. Instant help	Provide immediate help when needed from an adult.	The <i>NRC Report</i> indicated that this technology, which is not currently in use, is not designed to prevent exposure, but to operate after the fact.

FCC Order Related to Local Control

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

With respect to the overall rules:

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

Conclusion

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

³² FCC Order, *supra*.

4. Safety and Security of Students When Using Electronic Communications

CIPA Requirements

The CIPA Internet Safety Plan requirements related to electronic communication are:

- (I) IN GENERAL.-- In carrying out its responsibilities under subsection (h), each school ... shall--
 - (A) adopt and implement an Internet safety policy that addresses-
 - ...
 - (ii) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic commerce¹

Direct Electronic Communication in Schools

A Sad Story

A southwest state has a new virtual high school. Coursework for the virtual high school is dependent upon e-mail, but one particular school district in the state is using a filtering system that blocks all e-mail. The kids type their messages and save them to disk, and the teacher takes them home with her and posts from her home e-mail at night. When a reply comes in, or another posting, she prints it out at home and takes it back to students in school the next day. So the teacher is sending the students' e-mail for them since they can't do it themselves. If a different teacher were less willing to help them on her own time, these rural students would be cut off from using virtual school courses. They expect that they will also be unable to use the chat/discussion functions of the online courses as well because chat is also blocked².

The use of e-mail and other forms of direct electronic communication for instructional purposes is becoming increasingly important. Some districts have thought the costs and/or the potential dangers cannot be justified. But as the educational use of the Internet matures, this approach will not be sustainable. The Internet is a communication system, in addition to an information system.

It is possible to effectively address the safety and security of students without preventing them from fully participating in valuable educational activities on the Internet. Districts or schools that think they have solved the concerns by blocking access are interfering with student education and exacerbating the concerns presented by the digital divide. These districts or schools are also probably not effectively addressing the education of their students in online safe communication skills that are essential for safe Internet communication at home.

¹ 47 U.S.C. 254 (I)(1)(A)(ii).

² Story relayed by Jennifer D. Burke, Program Coordinator, Educational Technology Cooperative Southern Regional Education Board, Atlanta, GA. Personal communication, August 2001.

Educational Purpose and Use

Attention must be paid to purposes for which e-mail and other forms of direct electronic communication are being used to support enriching educational activities. In keeping with the educational purpose of the district's Internet system, excessive amount of use for personal purposes should be discouraged. This issue is discussed in the chapter on "Educational Purpose and Use."

Types of Electronic Communication

The primary forms of direct electronic communication that are being used in schools are:

E-mail

E-mail is by far the most prevalent form of direct electronic communication. Through e-mail, students are engaging in conversations with students in other parts of the country and the world. Students are able to take online distance education classes. Students are also able to communicate with experts in subjects that students are studying.

It is true that in some districts, the use of e-mail has become just another means for students to pass notes to each other. The degree to which this kind of communication is considered acceptable varies from school to school and can generally be managed through the establishment of traffic limits.

"Real time" Communication"

"Real time" communication environments, such as Chat and Instant Messaging allow students to engage in real time communication with other people who are online at the same time. Many online educational services have established environments where students can engage in online chats with authors, scientists, and others. Most online distance education classes make use of "real time" communication environments.

There are also a variety of moderated and unmoderated chat environments available on the Internet. The unmoderated chat environments present the most concerns regarding the potential of coming into contact with a predator. Most of the unmoderated chat environments have little to no educational value. Districts can address concerns of such environments by establishing a list of approved "real time" environments or limiting such activity to approved class activities.

Online Discussion Forums

Online discussion forms or conferences are also used to support distance educational classes, especially when students are participating from different areas of the world. There are also online discussion forums where students from around the world are engaging in ongoing discussions about a wide range of issues of interest or concern to youth. These environments present incredible opportunities for students to expand their understanding of our global society.

The online discussion environments can be managed in the same manner as "real time" communication environments.

Web-based E-mail Services

In some districts, where the district itself has not provided for e-mail, teachers and students who require e-mail for educational activities have utilized the services of commercial web-based e-mail providers, such as Hotmail or Yahoo mail. The use of these systems by students presents significant concerns. These services are provided for free to the user, but the costs are supported by advertising. Lots of advertising. The systems are developing market profiles of their users that may contain both demographic information and interest information collected when a user responds to an advertisement. Many people are using these web-based e-mail systems to transmit pornography, invitations to engage in gambling, and all other manner of unwanted solicitations.

In sum, these services are simply not the kinds of places that districts should be allowing students to use. *However*, districts should never simply dictate that all use of commercial web-based e-mail systems should immediately terminate. If teachers and students are using these services for valuable educational activities alternatives must be put into place prior to any restrictions being placed on the use of the systems.

Some districts simply do not have the resources necessary to support a district-based e-mail system. In such a case, there are reasonable alternatives that provide an excellent, safe educational environment for students. Fortunately, the subscription costs for such services are quite reasonable. Any district that cannot afford to maintain its own e-mail system should consider such services as an alternative.

Weblogs

Weblogs or blogs are services offered on the web where students can write and publish their thoughts about a topic. Weblogs are a merger between web sites and group discussions. On traditional web sites, the process of posting information can be laborious. On weblogs, the typing and posting can occur quite rapidly. Many individuals throughout the world are using weblogs to create daily journals. Weblogs offer the ability for others to comment on the posts. Teachers are beginning to use weblogs in a similar manner to the traditional “daily journal.” Weblogs encourage writing, discussion, and interaction.

Safety and Security Concerns

There are four areas of greatest concern when students use electronic communication:

- Privacy, which is discussed in Chapter II-6.
- Receipt of unsolicited E-mail (SPAM) e-mail that contains pornographic or other inappropriate material.
- Harassment and bullying of students by other students.
- Engagement with an online predator.

SPAM

SPAM is unsolicited e-mail that can contain a variety of material, ranging from unwanted advertising and get rich schemes and pornography or links to pornographic sites³. From safety perspective, the most significant concern is pornographic SPAM⁴.

To effectively address concerns related to SPAM requires both a technical solution and an educational solution. SPAM blocking technologies can help to limit, but not totally prevent, the receipt of SPAM. If a school maintains its own e-mail capacities, SPAM blocking technologies should be incorporated into this system. If a district uses an education subscription service, the SPAM blocking technologies will be built into the service.

Staff and students should also be educated about how to deal with SPAM. Here are some of the basics:

- Recognize that the more places users leave their e-mail addresses, the more likely it is that they will end up on a spammer's list of e-mail addresses. Spammers use search technologies to "harvest" e-mail addresses from public places on the Internet. The most popular places to harvest e-mail addresses are contest entries, bulletin boards and kid's clubs. Under the educational purpose restrictions, users of a district e-mail system generally should not be engaging in the kinds of uses that would generally lead to registration on commercial web sites or participation on online communication activities that are the primary source of such e-mail addresses. As discussed in Chapter II-6, students should not be encouraged and required to provide personal information, including their e-mail address on sites unless their has been a review of the privacy policy. If any particular users are having difficulties with extensive amounts of SPAM, it may be necessary to determine what activities they are engaging in that are leading to the harvesting of their how their e-mail addresses.
- Users must learn to recognize SPAM prior to opening the message and transfer the⁴ unopened messages to the trash file. The basic safety requirement is never to open an e-mail message unless you know who the sender is. SPAM is usually pretty easy to recognize. The sender's name is usually disguised, frequently with lots of numbers. The subject lines contain fascinating "enticements," such as: "Make money at home." "You just won." "See my new web site." "A special message for you." "Look at my new girlfriend." When SPAM messages are opened, they can immediately display inappropriate material. These messages that should be immediately transferred to the trash file without opening.
- Users should know that they should generally not respond to the "Remove me from your list" feature that is on some SPAM messages. This feature is generally a scam. If a user responds to a SPAM message requesting removal, this verifies to the spammer that the address is a valid address. They can then place this address on their premium list of verified e-mail

³ To understand why such e-mail is called SPAM, one must travel the recesses of Internet memory and watch a Monty Python movie. This has been beyond my grasp.

⁴ Educational products companies are sending e-mail messages advertising educational products to teachers--a practice that may or may not be considered SPAM depending on the degree of flexibility in the definition. Whenever a teacher provides personal information at a tradeshow booth at an educational conference, the company now has a valid e-mail address of a potential customer. The degree to which such companies may be using and selling such information may present concerns--as it is not a general practice for such companies to hand out a privacy policy at the time they ask for such personal information.

addresses. This guidance does not apply to the educational product companies who are generally responsive to such remove requests.

- The receipt of pornographic SPAM or any other sexually explicit e-mail by a student with a K-12 e-mail address should be treated as a criminal matter. The sender of such messages should know, or have reason to know, that sending pornography to a domain would result in providing sexually explicit material to a minor. Such actions are likely to be in violation of both federal and state criminal laws. Successful prosecution of several cases would go a long way to helping pornography spammers to be very careful in their handling of K12 domains.

Students and staff should be instructed to save any pornographic e-mail message they receive and to immediately notify the building administrator. The administrator should contact one of more of the following:

- Local FBI office -- Computer Crime or High-Tech Crime unit.
- US Department of Justice's Child Exploitation & Obscenity Section⁵
- State Attorney General's office.

Online Harassment and Bullying

Unfortunately, harassment and bullying that can occur in the "real world" at school can also occur online. Words can hurt and the hurt can lead to very negative consequences -- including school violence and suicide.

As discussed in Chapter III-2, if school staff are aware of harassment or bullying and fail to respond, there is a potential for liability.

Unfortunately, just as students may be reticent to report harassment and bullying that occurs in the "real world," they may be equally reticent to report online harassment. One advantage, however, to online harassment and bullying is tangible evidence in the form of the actual electronic messages. Once a few students have been detected and punished for sending harassing or bullying messages, the existence and impact of the tangible evidence should be well understood by all of the students in the school.

Teachers should naturally be sensitive to their student's emotional demeanor when using the Internet. If a student is looking distraught while using the Internet, this is the time for adult attention to what may be causing such distress. Technical monitoring systems may also be configured to detect patterns of language that give rise to concerns about bullying.

Obviously, this is a situation that must be handled with great care. The student who is the recipient of bullying who has not reported such bullying probably is a fragile child with significant fears. Physical reprisal from the student engaging in the bullying is a strong potential.

⁵ URL: <http://www.usdoj.gov/criminal/ceos/>.

Online Predators

Online sexual predators and other potentially dangerous individuals, including cult or hate group recruiters, may communicate with students through the Internet. It is unlikely that students will make significant contacts with online predators when using the Internet in school -- unless the school is providing extensive open access periods with little-to-no supervision, which, of course is not advised. Educational activities that students would be involved with at school do not occur in the kinds of environments where predators tend to "hang out."

Young people are far more likely to make contacts with online predators when they are using their computers at home. It is a big mistake to think that limiting electronic communications at school will address the concerns for what happens at home. Filtering software in school will not address concerns of predators. What might?

- Staff development for teachers so that they are aware of the indicators that a young person may be drifting into a trouble situation.
- Education for parents providing guidance on addressing addiction and predator concerns.
- Education for students about predators, dangerous activities, and the need to tell a responsible adult if you are concerned or if you think a friend is getting into a potentially dangerous situation.

Internet Savvy Teens

It is important for educators to be aware that many teenagers have the online sexual pervert and predation situation pretty well under control. Internet savvy teenagers can recognize perverts and predators for who they are and quickly tell them to "get lost."

Unfortunately, we have not yet taken full advantage to "teen power" to address the concerns of online predation. If more teenagers knew how to recognize, and preserve evidence, and report cases of contact by a possible predator, the ability of legal authorities to identify and prosecute these individuals would greatly increase. Teenagers simply do not know how important this is. Schools can help educate them about the importance.

Additionally, it is highly likely that any student who is thinking about meeting with an individual she (and sometimes he) has met online will share such plans with a friend. Students need to understand the potential dangers and the importance of never meeting with an online stranger outside of the presence of a parent or other adult. Students need to understand the potential consequences to their friends under such circumstances and recognize the need to either dissuade their friend from engaging in such a meeting or, if unsuccessful, to tell an adult.

Students should know that addressing their concern for the safety of their friend does not mean that they should go along with their friend to meet the online stranger. There have been a number of reported incidents where a friend has gone to such a meeting, only to get entrapped by the predator.

Students must learn how to recognize signs of a predator, how to preserve and report evidence, the importance of practicing safe skills, and the importance of watching out for the well-being of their friends. It is critically important that students learn and practice these skills in school.

Addressing Electronic Communication Concerns

The following are strategies that districts should consider implementing to address the safety and security of their students when using electronic communication systems

- For elementary students limit e-mail access to class accounts or systems where the teacher has full and immediate access to all electronic communication. Allow secondary students to have e-mail accounts to support educational activities. Establish the accounts with usernames that will help to protect the student's actual name. Do not simply use the student's last name. Most students will sign their messages with their first name and would thereby reveal their full name.
- For all students, limit the use of "real time" communication activities only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the school. Students should be able to identify and access the approved educational communication environments through the school's web site.
- Place strict limits on the size and level of activity allowed through student e-mail accounts. Students who have an educationally justifiable reason for a greater amount of e-mail use, such as students in school leadership positions, school newspaper staff, etc. may petition for greater storage and use limits. Indicate to students that excessive e-mail activity that has not been justified may create a reasonable suspicion that the student is misusing his/her e-mail account for personal purposes.
- Do not allow the use of the free, advertiser-supported commercial web-based e-mail services through the district's Internet system. However, prior to putting this restriction in place, ensure that other e-mail services are available.
- Include in the policy several provisions addressing student safety, including communication safety, personal privacy, protecting the privacy of others.
 - Elementary and middle students should not disclose their full name or any other personal contact information for any purpose. High school students should not disclose personal contact information, except to education institutions for educational purposes, companies or other entities for career development purposes, or with specific staff approval. Personal contact information includes the student's full name together with other information that would allow an individual to locate the student, such as parent's name, home address or location, work address or location, or phone number.
 - Students should not disclose names or personal contact information about other students under any circumstances.

- Students should not agree to meet with someone they have met online without their parent's approval and participation.
- Students should promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable, especially any e-mail that contains pornography. Students should not delete such messages until instructed to do so by a staff member.
- In the professional development delivered to district staff around the safe and responsible use of the Internet, ensure that teachers are aware of issues related to SPAM, harassment and bullying, and online predation.
- Address issues of online predation in classes for students related to the safe and responsible use of the Internet, as well as sex education classes. Students should be well aware of the very real trauma that other young people have gotten themselves into when they met with an online stranger. Students should also know the signs of predation and when they might be at risk for becoming involved with a predator. Stress the importance of saving and reporting evidence of such interactions as a contribution to the well being of other young people. Also discuss and practice how students can intervene with their friends who may be foolishly thinking of meeting with an online stranger.
- Provide leadership within your community to address all forms of sexual and physical abuse.
- Promptly contact appropriate legal authorities in the event a student has received a pornographic e-mail message or other inappropriate communication.
- Help empower your students, especially your female students, to address victimization in all forms. The National Center for Missing and Exploited Children has an excellent new public awareness campaign for teen girls, *Know The Rules*⁶. Their site has excellent resources for teachers in conjunction with this program.

⁶ URL: <http://www.ncmec.org>.

5. Unauthorized Access and Other Unlawful or Inappropriate Activities

CIPA Requirements

The CIPA Internet Safety Plan requirement to address unlawful activities is:

- (I) IN GENERAL.-- In carrying out its responsibilities under subsection (h), each school ... shall--
 - (A) adopt and implement an Internet safety policy that addresses--
 - ...
 - (iii) unauthorized access, including so-called hacking, and other unlawful activities by minors online. [¹

Computer Crime

Unfortunately, young people are using the Internet to engage in a wide range of unlawful activities. Some young people do not know or do not think that some of these activities are or should be considered unlawful. The best information source for information on the range of activities that are considered on computer crime is the U.S. Department of Justice's (US DOJ) web site on computer crime.²

Computer as the Target of an Offense

When the computer is the target of the offence, the computer's confidentiality, integrity, or availability is attacked. Services or information are being stolen or victim's computers themselves are being damaged. The denial of service attacks that were experienced by numerous Internet sites and the proliferation of the "I Love You" virus and its variants are but a few examples of this type of computer crime. Penetrating the computer's security system to obtain access to the confidential data stored on the system is another variant of this type of crime.

These activities are unlawful under both federal and state statutes. Unfortunately, many technically proficient teenagers are among the participants in such activities. Teenagers who become part of "hacker tribes" can rationalize that they are not engaging in activity that is wrong. In fact, they can unfortunately point to many former "hackers" who are leaders in the industry today.

Districts must address the issue of criminal use of the district's Internet system in the Internet Use Policy. It is also advisable to include a study of computer crime issues in computer classes. The US DOJ site provides a weekly update of computer crime events, including convictions. In most communities, it would also be possible to bring in a guest speaker from the local law enforcement community to provide some "real world" information on the consequences of engaging in such behavior.

¹ 47 U.S.C. 254 (I)(1)(A)(iii).

² URL: <http://www.cybercrime.gov>

Engaging technically proficient high school students in activities where they can use their advanced skills in socially beneficial ways, such as assisting with system administration, is an effective approach to help these students avoid becoming entangled with "hacker tribes." Many states have initiated student technology programs, often with industry assistance. Students coming out of these programs are highly welcomed in the computer science and information technology programs in institutions of higher education and in industry.

Computer as a Tool for Committing Criminal Behavior

This category includes those crimes that also occur in the "real world" but are now being seen with increasing frequency on the Internet. These crimes include transmission of obscene materials or child pornography, fraud, intellectual property violations, and the sale of illegal substances and goods, including drugs, online. Various illegal communication activities may also occur, including harassment, threatening the life or safety of another, stalking, and threatening the life of the President (just about every district has had to deal with this activity).

Some of these kinds of activities may reach the level of criminal conduct. Other activities, such as harassment, may be considered inappropriate in school but may not reach the level of severity of criminal conduct. These issues should also be addressed in the policy, however, it is probable that the district already has policies related to criminal activities. The inclusion of this material in the Internet Use Policy reinforces the understanding that crimes committed on the Internet are still crimes.

Additional Inappropriate Activities

In addition to unlawful activities, the District Internet Use Policy should address other inappropriate activities. These include inappropriate language, plagiarism, and copyright infringement.

Inappropriate Language

Restrictions against inappropriate language should apply to all speech communicated through the district Internet system, including but not limited to public messages, private messages, and material posted on web pages. Discussion regarding the free speech implications of such restrictions is included in the "Student Speech" chapter. Restrictions can include the following:

- Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- Users will not post information that, if acted upon, could cause damage or a danger of disruption.
- Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.

- Users will not knowingly or recklessly post false or defamatory information about a person or organization.

Plagiarism

Plagiarism has always been considered unacceptable in school but computers and the Internet are making it easier for students to "cut and paste" ideas and writings of other people into their own document. It is also possible to find research papers for sale or provided at no charge on web sites. Educators should be concerned about two kinds of plagiarism -- intentional and inadvertent. Teachers can most effectively handle issues of plagiarism by the manner in which they structure learning activities.

There are two ways that students use the Internet as a tool to intentionally plagiarize. The first is to find a paper on a site that sells or provides research papers specifically for students to copy and submit as their own. The second is to find a paper that some other student has written and posted on their personal student web site.

Teachers should be aware of this kind of plagiarism, discuss the issue with students, and look closely at the papers they receive for evidence of intentional plagiarism. If a teacher has concerns about the source of a paper, conducting a search on a particularly distinctive phrase contained in the document will frequently lead to the original paper. A search on the most popular search engine using the keywords describing the subject matter will often reveal such papers within the first several pages of search results. There are also new services available that will conduct such analysis. On those occasions when plagiarized papers are discovered through the use of such search techniques present excellent "teachable moments" to raise the awareness of all of the students in the school about how teachers can easily identify such plagiarism.

Inadvertent plagiarism is more accidental. Students sometimes inadvertently plagiarize because they do not understand how to incorporate the ideas of others into their paper and provide appropriate citation. They may also lose track of their sources as they are conducting their research, especially as they "surf" the web. They may think that "copying and pasting" what others have said is perfectly acceptable practice.

If teachers assign students to write papers that involve merely the recitation of facts, they are laying the groundwork for a greater amount of either intentional or inadvertent plagiarism. Students can easily copy major portions of material from other authors or find whole papers on a particular subject. It is not as easy to plagiarize when assignments call for creativity and integration of ideas.

Ensuring that students have the skills to paraphrase and summarize the ideas of others into their own words, engage in effective note-taking, keep a bibliographic record, and understand proper citation formats will reduce inadvertent plagiarism. Requiring students to turn in their work-in-progress on the term paper during the term -- research notes, outline, first draft, etc. -- will also help to prevent intentional plagiarism as most of these materials are not available online.

Teachers should fully describe to the students how they will evaluate papers to determine evidence of intentional or inadvertent plagiarism, especially if they are using a commercial

service for such analysis. The purpose for the use of such analysis methods should be to prevent the occurrence of plagiarism through notice. Playing the "gotcha" game after-the-fact is not a respectful educational strategy.

Copyright Infringement

Copyright infringement would also be considered an unauthorized use. Chapter III-9 addresses basic information and guidelines related to copyright.

6. *Disclosure of Personal Information of Students*

CIPA Requirements

The CIPA Internet Safety Plan must address the disclosure of personal information of students.

- (I) IN GENERAL.-- In carrying out its responsibilities under subsection (h), each school ... shall--
 - (A) adopt and implement an Internet safety policy that addresses--
 - ...
 - (iv) unauthorized disclosure, use, and dissemination of personal identification information regarding minors¹.

Dimensions of the Issue

There are many ways in which personal identification information of students may be disclosed by the district or by school staff. District policy should address all of the following issues. In addition to the need for the district to comply with the requirements of the Federal Educational Rights and Privacy Act (FERPA)², Individuals with Disabilities Education Act (IDEA)³, the Student Privacy Protection Act⁴, and, in many states, state student privacy laws.

It is also important to ensure that leaders the school's parent association, such as the PTA, fully understand the important obligations regarding the protection of student privacy, especially related to issues of posting student personal information online and collaborative relationships with commercial entities that may result in the collection and use of market research data from students. At many schools, the PTA is responsible for the dissemination of a student directory and/or a newsletter. Many PTAs are also establishing their own web sites. While the district may not be directly responsible for the actions of a parent organization, if such actions generate controversy, the district or a school will obviously be implicated.

Application Service Providers and Student Records

Application Service Providers (ASPs) offer schools the ability to manage school data. The software and databases are stored on the computers of the ASP companies and accessed by school staff, students, and parents through the Internet. ASPs allow schools to track student attendance, grades, disciplinary records, homework assignments, and more. ASPs can also generate the kinds of statistical data required under the No Child Left Behind Act.

The kind of data that these ASPs create, store and transmit is considered educational data. School districts must comply with the Federal Educational Rights and Privacy Act, Individuals with Disabilities Education Act, and, in many states, state student privacy laws with respect to this educational data. It is permissible for schools to contract with third parties for data services, but the school is ultimately responsible for ensuring that the requirements of the statutes are met.

¹ 47 U.S.C. §254 (I)(1)(A)(iv).

² 20 U.S.C. §1232(g).

³ 20 U.S.C. §1400 et seq.

⁴ Section 445(b) of the *General Education Provisions Act* (20 U.S.C. 1232h(b)).

Any contract with a vendor such as this must be thoroughly reviewed by the district's school attorney to compliance with these educational data laws. Issues that should be addressed include, but are not limited to:

- Regulation of access to student data, including limitations on who has access and records of access requests.
- Management of directory information.
- Procedures to correct or delete data.
- Requirements of confidentiality, privacy protection, and computer security on the part of the ASP.
- District ownership and access to the data in a transferable format at any time -- especially if the contract is terminated or the company ceases doing business.
- Indemnity or limitations of liability -- the ASP will likely seek limitations of liability, but should not be allowed to do so.

Currently, there are insufficient guidelines to address concerns in this area. For example, in the area of computer security standards, there are no established standards for exactly how secure the ASP systems must be⁵.

Disclosure of Student Information on School Web Sites

Actions that school staff or students may take that would intrude upon the privacy of a student include posting the student's name, class work, or a picture of the student on a district or school web site.

Schools have mechanisms that allow for the disclosure of student information in student phone books and in other district publications. Parental consent is required for any disclosure. These mechanisms have been developed in accord with FERPA. Technically, when parents grant permission for the treatment of student personal information as "directory information" under FERPA, such information becomes public record and may be disclosed by the district.

However, it is probable that most parents' perception of "directory information" is in the context of a hard copy student phone book or yearbook. If a district presumes that when a parent approves of the disclosure of such directory information this also gives the district to post such material on the Internet, the district is likely to generate a significant level of controversy, especially among parents of elementary students. Parents are simply not very comfortable with this level of disclosure of information about their children on the Internet. Therefore, regardless of what FERPA allows a district to do with directory information, the prudent school district will develop more restrictive regulations related to disclosure of student information on the Internet.

An excellent discussion of these issues is found in: McGuire, M. (2000) *Defining the Privacy Zone*. It is available online at URL: <http://www.nsba.org/itte/legalmeeting/PrivacyIssues.pdf>.

Districts should make a specific request of parents related to disclosures of material and information on the district web site. Districts should also demonstrate the same courtesy to staff. There may be some very good reasons for some staff members to wish not to have their identity disclosed online. For example, there may be a staff member who has escaped a domestic violence situation.

Many districts have responded to this issue by requesting parental permission in a manner that allows for many options, presented in a checklist fashion. Options frequently include: student initials, student first name and last initial, student full name, photo or video of student in group without identification, photo or video with identification, class work without identification, class work with identification, etc. The problem with this approach is it is unworkable. School staff cannot be expected to keep track of this vast amount of individualized information for each student. Inevitably, a staff member will mistakenly post something that a parent had specifically disapproved.

A more practical approach is for the district to determine what student information is safe, reasonable, and appropriate in accord with the instructional goals for elementary school students, middle school students, and high school students. This set of school level disclosure standards can then be provided to parents with the only option given being that of approving or disapproving the entire set.

It is recommended that for students in high school there be the ability to disclose full names. It is a bit illogical to have the online school newspaper report such things as "Joe made a touchdown or Mary, Sue, and Matt have received scholarships to the state university." By high school age, students should be well versed in online safety skills, so that such disclosure should not present concerns. Parents who have concerns still have the option of not granting approval.

The following are a set of recommended standards. However, districts will need to review these standards in the context of their own community.

For students in elementary and middle school, the following standards apply: Students will use a limited student identifier (school-developed identifier, that will disguise the actual name of the student). Group pictures without identification of individual students are permitted. Student work may be posted with the limited student identifier. All student posted work will contain the student's copyright notice using the limited student identifier.

For students in high school, parents may approve either the elementary/middle school standards or the following standards: Students may be identified by their full name. Group or individual pictures of students with student identification are permitted. Student work may be posted with student name. All student posted work will contain the student's copyright notice including the student's name.

There have been some reported incidents where a teacher has independently posted student information, pictures, and/or work on their own personal web site. In one incident that was

privately reported to the author, the teacher defended his actions by claiming he had a First Amendment right to post such information. Teachers have no rights to post information about minors without permission of their parent. All teachers should understand this.

Disclosure of Confidential Student Information in Staff E-mail Communications

School staff members are generally well aware of their legal responsibilities related to the protection of confidential student information. Problems can emerge in regard to the protection of such information when staff members communicate with each other via e-mail. E-mail tends to be informal. Its use leads to the same kinds of casual conversations as can occur in the staff break room or via a telephone. During such casual conversations, confidential student information can be disclosed. But with e-mail, there is now a permanent record of confidential student information that can be easily disseminated.

Staff should be reminded of their responsibilities regarding confidential student information and warned of the potential problems that can emerge due to the nature of electronic communication. One strategy to address this concern may be to develop some type of code to identify such information, for example the letters "CSI" could be written into an e-mail message or the subject line as a signifier to the recipient of the importance of treating the message properly. The requirement to include such an indicator would be a constant reminder to both the writer and the recipient of the importance of protecting privacy. All such e-mails should be retained in a manner required under student records retention laws.

Disclosure of Confidential Student Information in Student E-mail Communications

Students may also violate the privacy of other students by including personal information in an e-mail message. It is important to teach students to respect the privacy of others when communicating electronically and understand the harm that they can cause when they fail to do so. A prohibition against the distribution of personal information about other students should be included in the District Internet Use Policy. This issue should be addressed in instruction provided to students and again when the inevitable "teachable moments" arise.

Student Self-disclosure of Personal Information

Students may disclose personal information in electronic messages or on web sites. This issue and recommendations for the kinds of information that should be disclosed in electronic communications was discussed in "Safety and Security of Students When Using Electronic Communications."

Third Party Web Sites and Market Research

Market Profiling and Targeted Advertising

Educators view the presence of the Internet in schools as an opportunity to enhance student learning. Educators might be surprised to find that others are viewing the expansion of the Internet in schools from a different perspective: an increased opportunity for advertisers to reach the students and parents to promote the purchase of products and services.

One company that was offering free computers to schools⁶. This company was collecting market research information from students and targeting students with advertisements based on the market research. The company promoted itself to schools as "champions of student privacy." However in their investment promotion materials, they referred to their ability to "capture the 'eyeballs' and e-wallets of a captive and attractive demographic."

Web sites that seek to have educators require or encourage students to establish individual online accounts present special concerns. These accounts are established using either the students' actual names or user names. If advertising is present on the Web site it is likely that the account will be used by the dot.com company to develop an individualized market profile of each student. This market profile is established by collecting data from and about each individual student as he/she uses the Internet. The market profile enables the company to specifically target advertisements to the specific student based on knowledge of that student's specific demographics and interests. Such activities raise special concerns about student privacy and exploitative marketing activities.

The first place for every educator to look when evaluating a web site is the Web site's privacy policy. Virtually all web sites are now providing information about their data collection activities in a Privacy Policy.

Children's Online Privacy Protection Act

In 1998, the U.S. Congress enacted the Children's Online Privacy Protection Act (COPPA), which authorized the Federal Trade Commission (FTC) to develop rules that placing restrictions on companies in soliciting personal information from children under the age of 13. There is more information about the COPPA requirements on the FTC web site⁷. Essentially, COPPA requires that a web site obtain parental permission to collect any personal identification information from children under the age of 13. Unfortunately, rather than reducing the level of profiling and advertising to children, COPPA appears to have established a situation where such activities are considered OK as long as sites have given parents the opportunity to say "no."

On the FTC Kidz Privacy web site in the section for teachers there is more information for teachers about the law. There is also the following statement:

Whether playing, shopping, studying or just surfing, today's kids are taking advantage of all that the web has to offer. But when it comes to their personal information, who's in charge? The Children's Online Privacy Act, enforced by the Federal Trade Commission, requires commercial website operators to get parental consent before collecting any personal information from kids under 13. *COPPA allows teachers to act on behalf of a parent during school activities online, but does not require them to do so. That is, the law does not require teachers to make decisions about the collection of their students'*

⁶ A full discussion of this issue is available in Willard, N. (2000) *Capturing the Eyeballs and E-Wallets of Captive Kids in School*. This report is available online at: URL: <http://responsiblenetizen.org/documents/eyeballs.html>.

⁷ URL: <http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>.

*personal information. Check to see whether your school district has a policy about disclosing student information*⁸.

The significant concern created by this language on the FTC web site is that commercial web sites will directly communicate with teachers pointing to the FTC web site as their authority for their position that teachers can grant approval for the web site to collect information from their students. Because the FTC is a federal government agency, teachers may believe that such actions are perfectly appropriate.

Clearly, districts *must* have policies addressing this issue and the restrictions on such approval must be well communicated to all teachers.

Student Privacy Protection Act

The Student Privacy Protection Act⁹ was included in the No Child Left Behind Act. As of the writing of this document, the U.S. Department of Education is in the process of writing regulations for the implementation of this legislation. Up-to-date information can be obtained from the Family Policy Compliance Office (FPCO) in the Department of Education at PPRA@ed.gov.

The Student Privacy Protection Act applies to educational agencies or institutions that receive funds from any program of the Department of Education. The provisions of the law related to the collection of market research data are as follows¹⁰: Under the law,

- Schools districts are required to develop and adopt policies – in conjunction with parents – regarding the following:
 - The collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling, or otherwise providing the information to others for that purpose.
 - The right of parents to inspect, upon request, any instrument used in the collection of such information.
- School districts must “directly” notify parents of these policies and, at a minimum, shall provide the notice at least annually, at the beginning of the school year. Districts must also notify parents within a reasonable period of time if any substantive change is made to the policies.
- In the notification, the district must offer an opportunity for parents to opt out of (remove their child) from participation in the following activities:

⁸ URL: <http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/teachers.htm> (emphasis added).

⁹ Section 445(b) of the *General Education Provisions Act* (20 U.S.C. 1232h(b)).

¹⁰ Other provisions of the law address a range of other surveying or data collection activities.

- Activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information, or otherwise providing that information to others for that purpose.
- In the notification, the district must notify parents the specific or approximate dates during the school year when these activities are scheduled.

The requirements concerning activities involving the collection and disclosure of personal information from students for marketing purposes do not apply to the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions.

Given the degree to which commercial web sites are engaging in the collection, disclosure, or use of personal information from students for the purpose of marketing or selling, school districts will need to be very attentive to the manner in which the requirements of this law will be implemented with respect to student use of commercial web sites. This is especially true since most of the market research activities that the commercial web sites are engaged in are essentially invisible.

Parent's Reactions

Districts should seriously consider the reaction of parents if they were to find out that their children's teachers granted permission or encouraged their children to provide personal information or establish an account on a commercial web site that is now developing a market profile of the children and targeting the children with advertising -- all while the children are using the Internet at school.

Regardless of whether the children are under or over 13, it is likely that there would be substantial parent outrage. Clearly, districts **MUST** have a policy about disclosing student information on commercial web sites -- and that policy should say: "**NO!**" It simply is not OK for educators to encourage or require students to participate on commercial web sites that are profiling their interests for the purpose of advertising to to convince them to purchase products and services.

Recommendations

There may be occasions where the establishment of a student account on a third party site will be solely for the purpose of supporting an educational activity. This kind of a site may also be collecting student use data for the purpose of improving the educational quality of the site. With proper notification to and consent by parents, the establishment of such accounts should be considered acceptable.

Educators must be able to distinguish between web sites that have an exclusive educational purpose and sites that are profiling and advertising. The key feature to consider is the presence of advertising for youth products and services on the site. If there is advertising present and children

are required to establish individual accounts, there is a high likelihood that some form of profiling and advertising will be taking place.

The following are recommended standards for addressing these issues:

- There should be no establishment of student accounts on systems unless there is a clear educational purpose, no advertising for consumer products or services is directed at students, and parents have been fully informed and have approved such accounts.
- There should be no collection, analysis, or sale of individual or aggregated student use data for market research purposes for consumer products or services -- period. The Student Privacy Protection Act allows this to occur if there is parental approval. Such activities are totally out-of-line with the duty-of-care that educators should demonstrate towards their students. Essentially, allowing companies to collect information from students results in selling their privacy for the purpose of promoting their consumption. Such actions should be considered abhorrent to anyone who cares about the well being of children.
- Allowing data collection in carefully controlled situations to support the development of educational products and services should be considered acceptable, if parental notice, with ability to opt out has been provided.
- If any educational data, as defined by FERPA, IDEA, or state laws, is maintained on the third party site, the contract with the third party site should be reviewed for compliance with all such laws.
- Watch for the new regulations from the U.S. Department of Education related to the Student Privacy Protection Act.

7. Supervision, Monitoring, and Privacy

CIPA Requirements

The CIPA requirements related to monitoring are:

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

- (i) is enforcing a policy of Internet safety for minors that includes monitoring the online activities of minors¹.

Neither the CIPA statute nor the FCC regulations provide a definition for the term "monitoring." Common use of the term monitoring includes the concepts of in-person staff supervision, the use of "real-time" monitoring devices that allow for the distant viewing of computer terminals, and staff or technical review of Internet usage records.

A reasonable presumption is that to comply with CIPA, districts must enforce a policy that includes a good faith effort to engage in an appropriate level of monitoring to protect against access to material that is considered potentially harmful. Most districts use a combination of supervision or "real-time" monitoring and a periodic analysis of Internet usage records.

There is no requirement in CIPA that the activities of adults using a district Internet system be monitored. But clearly, the district will want to ensure that staff is not misusing the Internet and, therefore, staff use should also be monitored.

Remaining "Hands-On"

The essential component of supervision and monitoring is the removal of the perception of invisibility. Supervision and monitoring is the way in which educators remain "hands-on" -- knowing where students are, what they are doing, and who they are doing it with. When young people are in an environment where adults have remained "hands-on" they are much less likely to engage in risk-taking or inappropriate behavior.

For the purposes of this document, supervision will refer to "real time" activities where school staff are present and attentive to student Internet use as it occurs. Monitoring will refer to analysis of student use that occurs after-the-fact or using technical systems that allow for the review of student use outside of the physical presence of the students. Both supervision and monitoring can be facilitated through the use of technology. Real-time systems can provide the ability for a staff person to view the screens of remote computer. Technologies can also filter and review Internet usage traffic and identify traffic that is suspected to be in violation of the district policy, as configured into the monitoring technology.

¹ 47 U.S.C. 254 (h)(5)(B).

The *NRC Report* specifically addressed the issue of privacy in the context of the use of technical monitoring in schools.

(T)he level of privacy that students can expect in school -- using a computer as well as in other aspects of school life -- is different from what they can expect at home, and school computer systems are not private systems. The expectation of privacy when students use computers in schools is more limited, as is evidenced by a variety of actions that have been supported in court decisions, including searches of student lockers, backpacks, and so on. Thus provided that students have been given notice that their use is subject to monitoring, the use of monitoring systems raises fewer privacy concerns²

Supervision

Supervision requirements should be appropriate to the age and circumstances of the students. The supervision requirements for a class of elementary students, will be different from the requirements for high school staff of the school newspaper. Supervision requirements will likely also be different for different groups of students within one school. Educators generally have a good sense of the abilities, aptitudes, and inclinations of their students, including their ability to make safe and responsible choices in their use of the Internet.

It is recommended that the district policy include reference to supervision requirements related to the age and circumstances of the students, with a delegation to school administrators to further define and delineate the supervision requirements and expectations for their schools. The staff that are supervision student use of the Internet in environments or at times when students use is not restricted to specific class-related activities should receive professional development related to issues of students' rights of access to information. Staff may not restrict student access to certain information or sites based on the staff member's views of what is or is not appropriate information. Such decisions should be made in accord with the standards set forth in district policy.

To facilitate effective supervision also requires consideration of the physical placement of computers. To the greatest degree possible all computers that are used by students should be positioned in a way so that the screen is clearly visible to others. Stores that sell X-rated merchandise generally have driveways that are screened and windows that are boarded up. There is a reason for this. The more publicly visible the activity, the less likelihood there is for the demonstration of questionable behavior. As school administrators review the supervision requirements for their school, an analysis of the placement of the computers would also be advisable.

Under the approach set forth in this Guide, students in elementary school will have access to the Internet in an environment that generally limits their use to access to pre-reviewed and approved web sites. There may, however, be occasions where access to the more open Internet is necessary to achieve a specific educational purpose. If elementary students have access to the more open Internet, staff should provide close "over-the-shoulder" supervision.

² National Research Council. *Youth, Pornography, and the Internet* (Dick Thornburgh & Herbert S. Lin, eds., 2002). URL: http://bob.nap.edu/html/youth_internet/, at Section 12.2.5.

For secondary students, effective supervision and monitoring is the critical strategy to address concerns of irresponsible or unsafe behavior. Effective supervision and monitoring allows students to have more freedom in their use of the Internet and places the responsibility squarely on their shoulders to exercise that freedom in an appropriate manner.

Secondary schools may also consider the use of student lab monitors to provide additional supervisory capacity. Students who have been granted such authority tend to take their jobs very seriously. They consider misuse by other students to reflect badly on the entire student body. Student supervisors are also very likely to be in tune with behavioral clues that other students may exhibit if involved in misuse.

Monitoring

Effective monitoring of Internet usage will help to identify instances of inappropriate or unsafe use that may have been undetected notwithstanding appropriate supervision. The implementation of an effective monitoring system is an excellent measure to prevent problems. When students know that they are leaving little "cyberfootprints" that can easily be tracked by the system administrator, they are much less likely to even think of doing something that will result in detection and discipline.

To ensure effective monitoring, secondary students should be provided with a unique student user ID. Many schools follow a practice whereby students may only receive this user ID upon completion of an Internet Use Policy class. The use of a unique student user ID should not be necessary at the elementary level because the focus at this level of schooling is protection in safe Internet spaces.

Real-time monitoring can occur through the use of monitoring technologies that allow the lab supervisor to remotely view any of the computer screens in the computer lab, or school. After-the-fact monitoring involves an analysis of student usage records and files. In smaller districts with a low level of Internet traffic, periodic staff analysis of Internet usage records may be sufficient. However, with larger districts, staff analysis will be too time-consuming. Districts may want to consider the acquisition of a technology tool to provide assistance with the monitoring.

There are newer filtered monitoring technologies coming onto the market provide an excellent monitoring capability. These technologies use a packet-sniffing technology and linguistic analysis to filter all Internet traffic, including not only web sites, but also e-mail and any real-time communication activities. The packet sniffing technology will report cases of suspected violations of the District Internet Use Policy. Administrators can then review the reported usage to determine whether there was an actual violation. For example, a report may reveal that a student accessed one site with pornography but exited that site within 5 seconds -- clearly indications of mistaken access. But a student will have difficulty arguing that he or she mistakenly accessed a site with pornography when the report indicates that the student was viewing the site for 3 minutes, and then accessed several more pages on that site.

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 test³. The first part of the test requires "[t]he person must have had an actual or subjective expectation of privacy."⁴ The second part requires that this subjective "expectation be one that society is prepared to recognize as 'reasonable.'⁵" 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.*⁶. These standards are:

- Was the search "justified in its inception"⁷? 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"⁸.
- Was the search "reasonably related in scope to the circumstances which justified the interference in the first place"⁹? A search is reasonable when "the measures adopted are

³ *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)

⁴ *Id.* at 350-52, 360.

⁵ *Id.* at 361 (Harlan, J., concurring).

⁶ 469 U.S. 325 (1985).

⁷ *Id.* at 341.

⁸ *Id.* at 342 (citations omitted).

⁹ *Id.* at 342.

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 infraction¹⁰."

The extent of a district's ability to investigate the personal files of staff is less clear. In *O'Connor v. Ortega*¹¹, 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 communication, rather than information searching. Essentially, the rationale for this perception is unknown.

¹⁰ *Id.* at 342 (citations omitted).

¹¹ 480 U.S. 709 (1987).

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 not 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 a 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.