

School Cyberlaw

PART II

Cybersafety: Child Protection, Privacy, and Confidentiality

By David Hostetler

“[T]he same Internet that can benefit our children is also capable of inflicting terrible damage on them.”

—SENATOR JOHN MCCAIN¹

One of the curses that accompany the blessings technology brings to our public schools is students’ vulnerability to misguided, self-serving, and sometimes predatory users of computer technology. Regarding exposure to sexual content, one commentator noted that

[it] doesn’t take much exploration to find lewd sites on the Internet. . . . You are one click away from sites whose titles suggest their contents—fetishes, fantasies, bondage, and more. The pictures leave little to the imagination and most of them move!

To access these sites you need to do nothing but click. So in roughly two clicks of the mouse, you can view material that would come wrapped in brown paper at the newsstand.²

In 2003 Reuters News Service reported that the number of Web sites worldwide featuring child pornography (over half of them based in the United States) had more than doubled in a year’s time. In 2004 the total number of reported sites (more than seventeen thousand) had risen 70 percent.³ The courts have increasingly acknowledged these realities.⁴ In sum, the

Internet offers predators an expansive arena in which to carry out new forms of exploitation.⁵

“What’s a Government to Do?” might well be a suitable title for this article, which chronicles the controversy and difficulty legislators have encountered attempting to protect children using the Internet. The courts and First Amendment advocates have not made it easy for Congress or the states to enact Internet laws to protect children.⁶

A recent Fourth Circuit Court of Appeals decision well exemplifies the problem of crafting a law that both protects children and ensures that adults can exercise their free speech rights on the Internet. In *PSINet, Inc. v. Chapman*, the court ruled unconstitutional a Virginia statute that had been amended to criminalize the Internet dissemination of material “deemed harmful to children.”⁷ Under the First Amendment, the court applied “strict scrutiny,” requiring the government to prove two elements: (1) that the statute serves a “compelling”

child victimization. See James Brooke, *Sex Web Spun Worldwide Traps Children*, N.Y. Times, Dec. 23, 2001, at A12 [“The Internet and cellular telephone explosion has been a boon to adults who prey on young people for sex.”].

5. The federally funded report by David Finkelhor, Kimberly J. Mitchell, and Janis Wolak, *Online Victimization: A Report on the Nation’s Youth* (National Center for Missing and Exploited Children, June 2000), available at www.copacommission.com/papers/ncmec.pdf (last visited August 27, 2003), notes that approximately one in five youths between the ages of ten and seventeen was sexually solicited or approached over the Internet in the previous year.

Teenagers increasingly use the Internet to solicit money from viewers. Known in Internet parlance as “camboys” or “camgirls,” youths post provocative pictures of themselves and ask for donations. This practice was brought to the public’s attention when a thirteen-year-old Connecticut girl met and was strangled by someone who saw her Web site. “The Two Faces of a 13-Year-Old Girl,” CBSNews.com, May 31, 2002 (last visited 30 March 2004). Federal law does not prohibit such “exotic” sites if child pornography is not involved.

6. The first article in this series (“Cyberspeech: First Amendment and Defamation,” *School Law Bulletin* 34 [Fall 2003]: 1–15) deals extensively with First Amendment issues. (See *Editorial Note*, p. 10.)

7. 362 F.3d 227 (4th Cir. 2004).

David Hostetler is director of legal services for the Principals’ Executive Program, Center for School Leadership Development, University of North Carolina. He specializes in school employment and technology law.

1. 144 CONG. REC. S518–19 (1998).

2. See Julie Underwood, “Ethics & Law: Could an Internet Filtering Act Stand a Constitutional Challenge?” *eSchool News online*, May 1998, available to subscribers at <http://www.eschoolnews.com/news/browse.cfm>.

3. Reuters, “UK Police: Child Porn Web Sites More Than Double,” August 21, 2003; *id.*, January 19, 2004.

4. See, e.g., *U.S. v. Lifshitz*, 363 F.3d 158 (2d Cir. 2004), available at LEXIS 5657 (“As the Supreme Court stated over two decades ago, ‘[i]n recent years, the exploitative use of children in the production of pornography has become a serious national problem.’ *New York v. Ferber*, 458 U.S. 747, 749, 73 L. Ed. 2d 1113, 102 S. Ct. 3348 [1982]. [T]he rise of the Internet has only increased the availability of such materials and augmented the accompanying problems of

government interest, and (2) that it employs “narrowly tailored” means to accomplish that purpose. The court agreed that the government had a compelling interest in “protecting minors from sexually explicit Internet materials” but ruled that the statute was overbroad (i.e., was not narrowly tailored) because it might implicate or “chill” too many other types of protected speech.⁸

Noting the tension between protecting children and protecting free speech rights, Judge Davis remarked in his concurring opinion: “Were I participating in this case as the doting grandfather that I am proud to be, I would eagerly embrace the result reached by the dissent. Shedding my familial role, however, as I must, for my proper role as judge, I am pleased to join [the majority] opinion.” He went on to say, “Justice Holmes famously stated, that hard cases sometimes make bad law, and certainly, as we all know, rapid advances in technology sometimes make hard cases.”⁹

Reflecting a sentiment many legislators may feel after their numerous attempts to protect children are rebuffed by the courts, Justice Niemeyer, in his dissenting opinion in *PSINet*, remarked: “If this narrowly tailored statute does not survive strict scrutiny, then the conclusion must be drawn that States have no alternative but to abandon efforts to regulate Internet-based pornography deemed harmful to juveniles.”¹⁰

This article, the second of a three-part series on technology law and public schools, addresses in some detail this topic of child protection, as well as issues of confidentiality, racial and sexual harassment, and personal privacy as they relate to the intersection of school and cyberworld. The third and final article will look at “Cybersystems: School Operations and Other General Issues.” As they are in other areas of school cyberlaw, the legal duties and protections associated with these topics are relatively new and still evolving. Because of the ease, speed, and broad accessibility of electronic communications, school officials need to be especially vigilant to protect students from Internet exploitation.

Federal Child Internet Protective Legislation

In general, existing federal and state criminal laws prohibit publication of obscenity as well as certain other invasive and damaging types of conduct. (A discussion of North Carolina’s state criminal statutes outlawing certain computer-related conduct is included near the end of this article.) How far the federal government may go in protecting children against sexually explicit material on the Internet has been the subject of

numerous First Amendment legal battles in recent years. Clearly, the First Amendment does not prevent the government from protecting students from Internet obscenity and child pornography.¹¹ Restrictions on other forms of sexually related Internet speech, however, have often been overturned by the courts. To avoid liability, school officials must, on one hand, take reasonable steps to protect students against risk while, on the other, steering clear of excessive restrictions or monitoring that might violate students’ free speech or privacy rights.¹² This first section addresses some of the numerous legislative efforts and legal principles related to protecting children using the Internet.

Communications Decency Act (CDA)

On February 6, 1996, Congress, concerned about the growing exposure of children to pornographic material, passed the Communications Decency Act (CDA) as an amendment to the Communications Act of 1934. One section of the CDA imposed criminal penalties on purveyors and transmitters (commercial and noncommercial) of *obscene* or *indecent* telecommunications materials. In the 1997 case of *Reno v. ACLU*, however, the U.S. Supreme Court ruled that this section of the CDA, as it relates to indecent materials, was overly broad and unconstitutional, because it prohibited adults from obtaining constitutionally protected material.¹³ (Neither party disputed that the government could lawfully prohibit *obscene* material.)

Another provision of the CDA, Section 223(a)(1)(A), subjects to prosecution those who use telecommunications devices to transmit material deemed “obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten or harass another person.” Does this prohibit only one basic type of speech—“obscenity,” which has been defined by the Supreme Court and is not protected speech—or does it also prohibit other types of sexually related, but nonobscene speech, including speech deemed “indecent”? In April 1999 the U.S. Supreme Court, in *Reno v. ACLU*, affirmed a lower court opinion upholding the constitutionality of this provision because, according to the Court, it restricts only *obscenity*. The Court considered prior cases holding that similar “strings” of words essentially refer to obscenity. Thus, although the statute refers to “indecent” speech, it did not establish a separate form of prohibited speech distinct from “obscenity.”

8. The court also ruled the statute unconstitutional under the Commerce Clause (U.S. CONST. art. I, § 8, cl. 3). *PSINet*, 362 F.3d at 239–40.

9. *Id.* at 241.

10. *Id.* at 256.

11. *Miller v. California*, 413 U.S. 15 (1973); *New York v. Ferber*, 458 U.S. 747 (1982).

12. A New Jersey court upheld a “tort proceeding . . . against a board of education for personal injury damages resulting from its alleged failure to safeguard its students while still in its custody, [extending] ordinary principles of negligence”; Sally Rutherford, “Notes and Comments: Kids Surfing the Net at School: What Are the Legal Issues?” *Rutgers Computer and Technology Law Journal* 24 (1998): 417.

13. 521 U.S. 844 (1997).

The CDA also provides Good Samaritan immunity from liability to Internet service providers (ISPs) that install filtering devices on their computer systems to block access to obscene or other lewd material. A Virginia federal district court, however, has interpreted this immunity provision narrowly with respect to governmental Internet service providers, questioning whether the immunity applies to a governmental entity—in that case, a public library.¹⁴ The court ruled that if immunity does apply, it immunizes service providers only against civil liability for damages, not against injunctive or declaratory relief. In other words, a government agency may be protected from paying monetary damages but may still have to remove or alter its Internet filter to protect a plaintiff's First Amendment rights. Whether courts with jurisdiction in North Carolina will interpret this immunity provision in a similar way remains to be seen.

Child Pornography Prevention Act (CPPA)

The Child Pornography Prevention Act of 1996 (CPPA) outlawed, among other things, the distribution or possession of actual pornographic images of children. In addition, it expanded the previously established definition of child pornography to include “virtual” child pornography. In so doing, it specifically prohibited (1) “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture [that] . . . is, or *appears to be*, of a minor engaging in sexually explicit conduct”; and (2) any image that is advertised, promoted, presented, described, or distributed in a manner that *conveys the impression* that material is or contains a visual depiction of a minor engaging in sexually explicit conduct” (italics added). A coalition of adult entertainment groups sued, claiming that these provisions, on their face, violated their free speech rights.

In 2002, in *Ashcroft v. Free Speech Coalition*, the U.S. Supreme Court struck down these “virtual pornography” provisions, declaring them unconstitutionally overbroad (i.e., they prohibited some speech that is constitutionally protected).¹⁵ The Court examined the case extensively under two prior precedents: *Miller v. California* (establishing a legal definition of obscenity) and *New York v. Ferber* (upholding a prohibition on the production, distribution, and sale of child pornography because of evidence showing such acts to be “intrinsically related” to the sexual abuse of children—thus creating a compelling interest to justify the prohibition).¹⁶ Applying these precedents, the Court, in *Ashcroft*, concluded that the virtual pornographic speech under consideration en-

compassed speech that did not meet the *Miller* definition of obscenity and was not, under *Ferber*, shown to be “intrinsically related” to the occurrence of child abuse.

Child Online Protection Act (COPA)

In 1998, addressing the CDA provisions overturned by the Supreme Court in 1997 (discussed above), Congress passed the Child Online Protection Act (COPA).¹⁷ This law prohibits commercial Web site operators from knowingly providing children under seventeen access to Web content deemed “harmful to minors.” In COPA, Congress defined various terms more narrowly than it did in the CDA. On October 22, 1998, the day after President Bill Clinton signed the law, a number of plaintiffs filed a suit challenging COPA's constitutionality. The lower courts prohibited enforcement of these provisions and the case was appealed.¹⁸

In June 2004 the U.S. Supreme Court affirmed the district court's decision to enjoin enforcement of these provisions, pending a trial.¹⁹ The Court reasoned that the government had thus far failed to show that there were not “plausible less restrictive alternatives” (such filtering devices) that would not impose “the burden on constitutionally protected speech that COPA imposes on adult users or Web site operators.” The Court also offered practical reasons for upholding the injunction, including the need for time to update information about current technology in a case more than five years old.

The Child Online Privacy Protection Act (COPPA)

On October 21, 1998, Congress passed the Child Online Privacy Protection Act (COPPA), which has ramifications for elementary and middle schools.²⁰ Prior to its enactment, a survey by the Federal Trade Commission (FTC) showed that 89 percent of Web sites for children collected personal data from child users; but only 24 percent posted privacy statements, and only 1 percent required proof of parental consent for a child to use the Web site.²¹

To address problems like these, COPPA prohibits commercial Web site operators from intentionally collecting personal information from any child under the age of thirteen except when (1) the Web site operator provides proper notice to

plying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value” (24).

17. Pub. L. No. 105-277, 112 Stat. 2681 (1998), 47 U.S.C. § 231.

18. The Third Circuit Court of Appeals ruled the law unconstitutional. *ACLU v. Ashcroft*, 322 F.3d 240 (3d Cir. 2003).

19. *Ashcroft v. ACLU*, 2004 WL 1439998 (U.S., June 29, 2004).

20. Pub. L. No. 105-277 (1998), 15 U.S.C. 6501 *et. seq.* (COPPA should not to be confused with COPA, discussed above.)

21. By 2001, apparently as a result of COPPA, an FTC study showed that over 90 percent of children's Web sites had privacy policies in place. www.Reuters.com. April 22, 2002.

14. *Mainstream Loudoun v. Bd. of Trustees of Loudoun County Library*, 2 F. Supp. 2d 783, 789–90 (E.D. Va. 1998), *summary judgment granted*, 24 F. Supp. 2d 555 (E.D. Va. 1998).

15. 535 U.S. 234 (2002).

16. *Miller*, 413 U.S. 15 (1973); *Ferber*, 458 U.S. 747 (1982). The definition of obscenity adopted by the *Miller* court was “(a) whether ‘the average person, ap-

users of what information will be collected, and (2) the operator obtains verifiable consent from one of the child's parents. (Consent may be withdrawn at any time.) Personal information includes such things as the child's name, address, e-mail address, telephone number, social security number, and personal preferences. Verifiable consent means that the operator must make reasonable efforts, using available technology, to obtain parental permission. The law provides operators with "safe harbors"—means of avoiding liability—as long as they comply with guidelines approved by the FTC.

On October 21, 1999, the FTC issued rules implementing COPPA; they took effect on April 21, 2000.²² Particularly significant is a section of commentary on the rules governing school officials' roles in authorizing students' use of the Internet at school. The FTC commentary states that public school officials may serve as parental intermediaries or agents in providing "verifiable consent."

[T]he Commission notes that the Rule does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parents' agent in the process. For example, many schools already seek parental consent for in-school Internet access at the beginning of the school year. Thus, where an operator is authorized by a school to collect personal information from children, after providing notice to the school of the operator's collection, use, and disclosure practices, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent. Operators may wish to work with schools to educate parents about online educational activities that require web sites to collect personal information in the school setting. To ensure effective implementation of the Rule, the Commission also intends to provide guidance to the educational community regarding the Rule's privacy protections.²³

The exact meaning and significance of this FTC commentary is unclear and raises many questions. Do school officials have legal authority to act as "intermediaries" or "agents" under COPPA, even though the statute and the rule are silent on the matter? If officials have such authority, how should it be obtained and implemented? Does such authority subject officials to greater risks of liability than if they refuse to act as intermediaries or agents by leaving the consent decision entirely to parents? (The FTC has provided more detailed guidance to teachers regarding their role in providing verifiable consent on behalf of parents.²⁴)

22. FTC Children's Online Privacy Protection Rule, 16 CFR § 312 (1998).
23. *Id.*

24. One FTC publication addressed to schoolteachers states, in part, that a teacher "[m]ay act in place of a parent in deciding whether to give consent. Consent from a parent authorizes the website to collect personal information from your student. Subject to your school district's policies, you may act on behalf of the parent in giving consent, but COPPA does not require you to do so.

Until these issues are clarified, school officials should be extremely cautious in determining both whether to allow students thirteen-years-old and younger to access Web sites that collect personally identifying information or whether to assume roles as intermediaries or agents for COPPA purposes. If school officials do assume those roles, however, they should ensure that their students' parents (1) receive clear and explicit notification of COPPA's protections and consent requirements (including parents' right to withdraw consent at any time) and (2) explicitly authorize designated school officials to act as intermediaries or agents for them. The FTC operates a Web site devoted to resources and recommendations for protecting children under COPPA as well as a Web page (developed with the U.S. Office of Education) that schools can use to educate parents and children about online privacy.²⁵

The Children's Internet Protection Act (CIPA)

In late 2000 Congress passed and President Clinton signed the Consolidated Appropriation Act. Embedded in Title XVII of the act was the Children's Internet Protection Act (CIPA).²⁶ Among other things, CIPA requires school systems receiving federal funding to implement Internet safety policies and, in essence, to ensure that school-owned computers block access to "child pornography," "obscene material, and other material "harmful to minors."²⁷

CIPA applies specifically to public schools or school systems that (1) receive federal discounts for purchasing Internet access under the popular eRate program (to be discussed in the next, and last, article in this series) or (2) receive funding to purchase computers or Internet access under Title III of the Elementary and Secondary Education Act of 1965 but do not receive discounts under the eRate program.²⁸ (A school system is subject to the Title III requirements only if it is *not* subject to the eRate requirements.) CIPA governs Internet use by both minors (defined as children under seventeen) and adults. The law took effect on April 20, 2001, as did the regulations of the Federal Communications Commission, the agency that implements the eRate provisions.²⁹

If you or the parent do not consent to the collection, use or disclosure of the student's personal information, the student's participation in an online activity may be limited to areas of the site where personal information is not necessary. You can give consent and still say no to having your student's information passed along to a third party. A parent or teacher's consent isn't necessary if the website is collecting a child's e-mail address simply to respond to a one-time request for information." <http://www.ftc.gov/bcp/online/pubs/online/teachers.htm> (last visited June 18, 2003).

25. <http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html> (last visited July 6, 2004).

26. Pub. L. No. 106-554, § 1701 *et seq.* (2001).

27. *Id.* § 1711.

28. *See, e.g.*, 47 U.S.C. § 254 (I)(1)(a)(v).

29. Federal-State Joint Board on Universal Service: Children's Internet Protection Act, 66 Fed. Reg. 19394 *et seq.* (April 16, 2001) (to be codified at 47 CFR part 54.520).

In 2003, in *United States v. American Libraries Assoc., Inc.*, the U.S. Supreme Court upheld CIPA as applied to public libraries.³⁰ Given that decision, and the Court's reasoning in the case, it appears clear that application of the law to public schools would also be upheld if challenged.

CIPA Requirements for Schools

Because so many schools receive eRate funds, this article addresses only the CIPA-related provisions that apply. CIPA requires that eRate discounts be withheld from a school system unless the system

- certifies that, *with respect to minors* (1) it is enforcing an Internet safety policy that includes the use of filtering software that denies access to material that is obscene, child pornography, or harmful to minors; and (2) that it is enforcing the use of such filtering software. (This policy *must* include provisions that require schools to monitor minors' online activities. Such monitoring may be anonymous.)
- certifies that, *with respect to adults* (1) it is enforcing an Internet safety policy that includes the use of filtering software that denies access to material that is (a) obscene or child pornography (note that there is no monitoring requirement for adult use, nor a requirement to deny access to material that is "harmful to minors"); and (2) that it is enforcing the use of such filtering software.
- certifies that an Internet safety policy has been adopted and implemented.³¹
- ensures that school-owned computers that can access the Internet are used in accordance with the certification requirements identified above.
- provides notice of and holds at least one public hearing related to the development of its Internet safety policy.

The Internet safety policy must address the following issues: (1) prevention of access by minors to inappropriate matter on the Internet and World Wide Web; (2) the safety and security of minors who visit chat rooms and use electronic mail and other forms of direct electronic communications; (3) unauthorized or unlawful activities (e.g., "hacking") by minors online; unauthorized disclosure, use, and/or dissemination of personal information regarding minors; and (4) measures designed to restrict minors' access to harmful materials.

Under CIPA any authorized school official is permitted to disable an Internet filter for an adult who uses a school-owned computer for "bona fide research or other lawful purpose."

30. 123 S. Ct. 2297 (2003).

31. The certification will be included in Form 486, already in use for applicants who have been approved to receive an eRate discount. The Federal Communications Commission considers this the least-burdensome means of implementing CIPA's certification requirement.

The Federal Communications Commission (FCC) has noted that the CIPA requirements (1) apply equally to all users of school-owned computers, staff members as well as students; (2) permit an Internet safety policy that was established by a school system before CIPA was enacted to remain in place if it satisfies the CIPA requirements; (3) do not permit eRate funds to be used to purchase filtering software or other tools necessary to implement CIPA's requirements; (4) do not require public posting of CIPA requirements; and (5) do not penalize schools if the filtering tools or monitoring efforts of school officials are imperfect as long as "good faith" efforts are made to comply with the law.³²

Complying with CIPA Requirements

School officials, particularly those responsible for Internet policies and school safety, should (1) determine which, if any, set of CIPA requirements their school system is subject to; (2) review current Internet policies and determine what provisions need to be changed; and (3) ensure that the required policies are in place and that annual certifications are made when applying for eRate discounts or Title III funds. (Remember that Title III provisions only apply if eRate provisions do not.) The extent to which schools have complied with CIPA and its attendant costs and benefits has been a subject of ongoing analysis and debate. A 2003 report concludes that Internet filters generally work as intended when computer system administrators receive training in their use.³³

The "Dot Kids" Act of 2002

On December 4, 2002, President George W. Bush signed the "Dot Kids Implementation and Efficiency Act of 2002," which establishes a new Internet domain reserved specifically for material considered "safe" and appropriate for children.³⁴ The law speaks of creating a "green light" domain similar to the children's section of a library. The new domain, "kids.us," is a sublevel of the United States government's ".us." Web site registration for the "kids.us" Internet domain was scheduled to begin in June of 2003; as of February 2004, there were reportedly only a few sites in actual operation.³⁵ If and when this

32. Federal-State Joint Board on Universal Service: Children's Internet Protection Act, 66 Fed. Reg. 19394 *et seq.* (April 16, 2001).

33. One newspaper reported that as of February 2002, 85 percent of North Carolina schools had filters in place, though some school boards were still looking for systems that allow flexible use by administrators, teachers, and students. The article notes that implementing a filter system can cost a medium-to-large school system \$10,000 to \$30,000 in start-up costs and \$7,000 to \$20,000 in annual maintenance fees. Stephaan Harris, "Districts Shop for Net Filters," *Raleigh News & Observer*, February 18, 2002; "Filters Work OK, but Better Training Needed," *eSchool News online*, August 28, 2003, available to subscribers at <http://www.eschoolnews.com/news/showStory.cfm?ArticleID=4585> (last visited August 28, 2003).

34. Pub. L. No. 107-317 (2002).

35. According to the *Washington Post*, the new domain has had a slow start. David McGuire, "Firms Ignore Kids-Only Internet Domain," February 20, 2004, <http://www.washingtonpost.com>.

new domain becomes well established, schools may be able to provide Internet access to children with greater assurance that their students will be safe.

Web sites on the new domain must meet the following requirements:

- All Web sites registered within the new domain must contain material that is “suitable” and not “harmful” to children under thirteen. “Suitable” material is anything that (1) is not “psychologically or intellectually inappropriate” and that (2) serves either the “educational, informational, or cognitive needs” or the “social, emotional, or entertainment needs” of minors. (These terms are not defined further; it is unclear, for example, what constitutes a legitimate “entertainment” need.)
- Web sites within the “kids.us” domain may not contain hyperlinks to Web sites outside the domain.
- Two-way and multiuser interactive services (for example, communications tools like AOL Instant Messaging) are prohibited unless a registrant shows that they are consistent with the law’s purpose.
- All domain registrants must agree to and abide by the rules and terms for access to the domain.
- The National Telecommunications and Information Administration (NTIA) shall oversee implementation of the law, suspend a domain if it fails to fulfill the law’s purpose, and educate children and parents regarding the domain’s availability and use (in conjunction with other protective measures such as software filtering tools).
- The registry agent (a company called Nuestar chosen by NTIA to operate the domain) shall, among other things, establish content standards, enter agreements with domain registrants, establish operating rules and procedures, remove registrants who violate domain requirements, and report annually regarding the registry’s efforts to monitor the domain and enforce its requirements.

The PROTECT Act of 2003

In 2003 Congress passed the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act (PROTECT).³⁶ This law addresses numerous areas of child protection that are beyond the scope of this article (e.g., creating a national missing child “AMBER-alert” network). Section V of the act, which Congress wrote to remedy the constitutional deficiencies of the CDA and CPPA, prohibits both “virtual” and actual child pornography. The law also seeks to remedy the CDA’s overturned prohibition of “indecentcy” by replacing it with “child pornography”; establishes a national Internet site with links to all state sex offender Web sites; and

creates a national pilot program for making a registry of federal and state criminal background checks for the benefit of certain volunteer organizations.³⁷

Practical Considerations

Most school systems strive to provide as many academically useful Internet resources to students as feasible. To avoid creating an undue risk of liability and student harm, however, school officials should consider the following suggestions:

- Make “cybersafety”—protective measures for student use of electronic communications—part of every Safe School Plan.
- Develop acceptable use policies (AUPs)³⁸ that, among other things, inform users about the risks inherent in electronic communications, identify permissible and prohibited uses, and spell out the penalties for abuse.
- Require students and parents to sign consent forms indicating that they understand and accept the AUP before allowing use of the Internet.
- Designate school officials to act as coordinators (and, if necessary, intermediaries or agents for parents) under COPPA (as discussed above).
- Hold periodic staff and student training sessions on proper Internet use. Such meetings (1) are useful for reminding and educating users about the AUP provisions, (2) reduce the likelihood that problems will occur, and (3) provide documentation that the school system has taken reasonable precautions to minimize risks to students.
- Designate an individual or committee responsible for receiving, investigating, and resolving complaints and concerns; reviewing safety and monitoring procedures and recommending changes; participating on the school safety team; and helping teachers monitor student computer use.
- Consider using other resources (e.g., new or updated filtering software that reduces the risk of student exposure to inappropriate materials) and alternative practices (such as permitting students to access only Web sites that have links to other age-appropriate sites).³⁹

Racial and Sexual Harassment of Students

Every month American workers send billions of e-mail messages—many of them personal—with great ease, careless-

37. *Id.* §§ 603, 604.

38. The subject of acceptable use policies will be addressed in more detail in the third and final segment of this series, “School Cybersystems.”

39. Companies such as Lycos (a provider of a popular Internet search engine), America Online, and Disney offer such sites. For a discussion and examples of such Web pages, see “Internet Firms Join to Ease Parents’ Worries,” *Raleigh News & Observer*, May 6, 1999, p. A6.

36. Pub. L. No. 108-21 (2003).

ness, and, often, a false belief that the privacy of their communications is protected.⁴⁰ Misuse of electronic resources by employees appears to be common.⁴¹ Although figures are not as readily available, student abuse of electronic resources presents self-evident dangers. In particular, it is likely that inappropriate or careless use of computer resources will increase claims of employee and student harassment (a form of illegal discrimination), especially sexual harassment.

Current laws, to varying degrees, protect students from racial or sexual harassment by other students (peer harassment) or by school employees; the same laws protect school employees from harassment by employers or their agents. Two primary laws prohibiting, respectively, racial and sexual discrimination and harassment of students are Title VI of the Civil Rights Act of 1964⁴² and Title IX of the Educational Amendments of 1972.⁴³ Although Title VI or IX case law involving harassment primarily through the use of electronic communications is scarce, two U.S. Supreme Court decisions on sexual harassment provide some general guidelines.

In *Davis v. Monroe County Board of Education*⁴⁴ the Court held that a school system may be held liable under Title IX when school officials are deliberately indifferent to known acts of student-on-student sexual harassment. According to this decision, the harassment must be “so severe, pervasive, and objectively offensive that it effectively bars the victim’s access to an educational opportunity or benefit.”

Sexual harassment of students by employees is governed primarily by the Supreme Court’s decision in *Gebser v. Lago Vista*.⁴⁵ In that case, the Court held that a school system is liable under Title IX if “an official who . . . has authority to address the alleged discrimination and to institute corrective measures on the [school’s] behalf has actual knowledge of the discrimination” and fails to act. Such failure, the Court found, amounts to “deliberate indifference to discrimination.”

School officials may significantly reduce their risk of liability for student harassment by taking certain preventive measures. They may, for example, institute an Acceptable Use Policy that establishes sanctions for students or employees who use school computers to harass or intimidate others. A school system’s current sexual and racial harassment policies may adequately address harassment via electronic means but should be reviewed and revised regularly to be sure they deal with the evolving uses of electronic resources. (These policies and any separate AUP should complement and, where appro-

appropriate, cross-reference one another.) The existence of such policies, combined with evidence that school officials take steps to educate students and employees about them, may demonstrate schools’ and school systems’ good faith efforts to prevent illegal discrimination and harassment.

School officials also should keep in mind that North Carolina’s “cyberstalking” law prohibits anyone from sending (or allowing to be sent) electronic communications that (1) threaten harm to a person or property; (2) are sent, repeatedly, for the purpose of “abusing, annoying, threatening, terrifying, harassing, or embarrassing any person”; or (3) contain any false statement “concerning death, injury, illness, disfigurement, indecent conduct, or criminal conduct . . . with the intent to abuse, annoy, threaten, terrify, harass, or embarrass.”⁴⁶

Privacy of School Internet Records

Reports of computer hacking and Internet displays of private information appear frequently in the news—for example, the exposure on the Internet of several thousand individual medical records from a University of Michigan database and the public disclosure of credit card account numbers.⁴⁷ Public school records are susceptible to similar threats.⁴⁸

Some computer users mistakenly believe that their electronic communications (i.e., e-mail, records of Internet use) cannot be read or accessed by anyone else. They may not realize, for example, that school network administrators usually have access to many, if not all, of a school’s communication files and related data. Computer logs reveal, for example, who used a school network, when and on which computer the use occurred, and which Web sites were viewed. E-mail monitoring reveals such things as the names of e-mail senders and recipients, the size of each message, whether a message contains attachments, and the time the message was sent. In addition,

46. N.C. GEN. STAT. § 14-196.3 (hereinafter G.S.).

47. “Hallmark Computer Glitch Sends Intimate Online Greetings into Public Cyberspace, and Michigan Medical Records Accidentally Posted on Web for Two Months,” *Raleigh News & Observer*, February 12, 1999; “Computer Experts Say Computer Hacker Menace Growing,” *id.*, February 11, 1999.

48. Privacy advocates have charged, for instance, that school systems’ electronic file retrieval systems jeopardize the confidentiality of student files.

A University of Michigan foreign student was expelled for hacking into the university computer system and using information to forge e-mails and access student and faculty information, including final exams. Associated Press, “Michigan Expels Graduate Student Accused of Hacking School’s Network,” August 13, 2003.

In 1997 California’s Orange County public schools contracted to purchase a computer system to link parents, via a password-protected Internet connection, to archives containing their children’s test scores, attendance records, and teacher’s remarks. A similar system was planned in Fairfax, Virginia. Sally Rutherford, “Notes and Comments: Kids Surfing the Net at School: What Are the Legal Issues?” *Rutgers Computer & Technology Law Journal* 24, no. 2 (Summer 1998): 417 (citing Tina Nguyen, “Orange County Plans to Link Schools, Homes,” *Los Angeles Times*, February 2, 1997, p. A3).

40. See Powers, Kinder, & Keeney, “What You Need to Know about E-mail,” *Rhode Island Employment Law Letter*, April 1999.

41. For example, in 2002, several Washington state government employees were fired for excessive personal use of the state’s e-mail system. Officials discovered hundreds of sexually explicit messages on employee computers. Associated Press, April 25, 2002.

42. 42 U.S.C. § 2000d (1998).

43. 20 U.S.C. §§ 1681–88 (1998).

44. *Davis v. Monroe County Bd. of Educ.*, 526 U.S. 629 (1999).

45. *Gebser v. Lago Vista Indep. Sch. Dist.*, 524 U.S. 274, 292 (1998).

network memory files may be used to access individual computer records, even after users have deleted them from their computers' active memory. (Such stored memory files can be used to identify computer misuse or to support or refute allegations of other kinds of wrongdoing (e.g., sexual harassment via e-mail).⁴⁹

This section addresses the legal issues related to the privacy of school-related electronic files and communications.

Basic Privacy Laws

Constitutional Protections

The Fourth Amendment of the Constitution, which protects individuals from unreasonable searches and seizures by the government, has been interpreted broadly to encompass a general right to privacy under certain circumstances. In a 1967 telephone wiretap case, the U.S. Supreme Court ruled that the right not only protects against unwarranted searches of physical quarters but also protects people when they have a reasonable expectation of privacy.⁵⁰

In schools the Fourth Amendment protection is usually applied to physical searches of students, employees, or their belongings. It may, however, also pertain to personal electronic communications and files if an individual has a "reasonable expectation of privacy" and school officials invade that privacy. As discussed below, school systems and officials can normally avoid such liability by eliminating beforehand any reasonable expectation of privacy. This is best accomplished by notifying students and employees periodically that their use of school computers may be monitored.

The Electronic Communications Privacy Act

In 1986 Congress passed the Electronic Communications Privacy Act (ECPA),⁵¹ which prohibits the intentional interception or disclosure of wire, oral, or electronic communications except

- when one party consents to the interception;
- when an Internet service provider (ISP) intercepts communications to protect itself, to prevent illegal activity, to assist law enforcement authorities, or to fulfill a right or obligation under its contract with users; or
- when a party already has made public the communication in question.

According to some courts, the interception provision of this law does not prohibit the retrieval and review of electronically stored e-mail messages.⁵²

49. Parties to litigation sometimes request extensive computer records to support their legal claims, particularly when searching for evidence of a "smoking gun."

50. *Katz v. U.S.*, 389 U.S. 347 (1967).

51. 18 U.S.C. §§ 2510–22 (1998).

52. *See, e.g., Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996) (hold-

Tort Law: Invasion of Privacy

Common law—law established by judicial precedent—also protects against privacy invasions in limited circumstances. North Carolina courts have so far recognized claims involving (a) misappropriation of a person's name or likeness for another's advantage⁵³ and (b) intrusion into a person's solitude or private affairs.⁵⁴ The latter claim is most relevant for the purposes of this section.

Persons claiming intrusion into their solitude or private affairs must show that the intrusion was intentional and would be highly offensive to any reasonable person. One defense to such a claim is that the plaintiff consented to the intrusion. Under this defense, a school system is likely to avoid liability if it has obtained signed consent forms indicating that students and employees accept the school system's right to monitor and review their computer use.

State and Federal Confidentiality Laws

The state and federal confidentiality laws discussed below also prohibit public disclosure of student and personnel records, except under certain limited circumstances. Because school systems, like businesses, are increasingly converting to electronic filing systems, their risk of inadvertent disclosure of confidential records is likely to increase. School officials, therefore, must take special precautions to minimize this risk.

Student Privacy

As noted above, the Fourth Amendment provides the dominant privacy protection for students against unreasonable searches by school officials. In 1985, in *New Jersey v. T.L.O.*, the U.S. Supreme Court held that the Fourth Amendment permits school officials to search a student if the officials (1) reasonably suspect the student of wrongdoing and (2) conduct a search that is reasonable in its scope and manner.⁵⁵ The Court, in a later case, made clear that school officials do not always need to suspect an individual student of wrongdoing in order to conduct random searches.⁵⁶

Under the Fourth Amendment, courts are likely to uphold school officials' monitoring or reviewing of student electronic communications. Many school systems that provide

ing that the city could read stored e-mail without violating the ECPA); *see also* *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 347 (5th Cir. 1994); *Fraser v. Nationwide Insurance*, 135 F. Supp. 2d 623 (E.D. Pa. 2001).

53. In *Felsher v. University of Evansville*, 755 N.E.2d 589 (Ind. 2001), a state court held that a state university, as an institution, could not assert a claim for misappropriation of its name against a former employee who created Web sites and e-mail messages disparaging of the university and university officials. The court, however, did uphold an injunction preventing the former employee from engaging in such behavior.

54. *See Renwick v. News & Observer Publishing Co.*, 310 N.C. 312, 322, *cert. denied*, 469 U.S. 858 (1984). *See also* C. DANIEL BARRETT, NORTH CAROLINA EMPLOYMENT LAW, 117–18 (1998).

55. *See New Jersey v. T.L.O.*, 469 U.S. 325 (1985).

56. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995).

students with electronic communications resources require the students—and in some cases their parents—to sign consent forms. Such forms should indicate that students and/or parents have read and understand the system’s acceptable use policy and agree to abide by its terms.

The Family Educational Rights and Privacy Act (FERPA) is the primary statute protecting students from unauthorized disclosure of educational records. The act also requires public schools receiving federal funds to have a policy allowing parents access to their children’s educational records within forty-five days of a request to do so. Under FERPA, “directory information” (e.g., student names, phone numbers, addresses, e-mail addresses, awards) may be published as long as the school gives parents notice of what it considers directory information and the right to refuse permission to include the information. FERPA is particularly applicable and must be considered when school- or student-related Web pages containing student information are posted. Because it is so easy to post information on the Web, and so to inadvertently violate FERPA, officials must put in place strict measures to prevent unauthorized disclosure of FERPA-protected information.

A California high school recently became the center of controversy after parents found information about their son on a page linked to the school’s Web site.⁵⁷ The site contained a page created by the school’s golf coach and included pictures of team members, along with their grade-point average (GPA) and Scholastic Aptitude Test (SAT) scores. The coach designed the page to attract college athletic recruiters. The boy’s parents informed the U.S. Department of Education’s Office of Civil Rights, which notified the school. School officials, who were previously unaware of the golf coach’s link to the Web page, shut down the page immediately. The case offers a lesson to school officials about the need to (1) carefully establish guidelines for school-related Web pages, (2) educate members of the school community regarding these guidelines, and (3) regularly monitor school-sponsored Web sites.

In addition to FERPA, several North Carolina statutes provide similar or additional privacy protection for student records. These include Section 115C-402 of the North Carolina General Statutes (official student records) (hereinafter G.S.), G.S. 115C-114 (records of children with special needs), and G.S. 115C-174.13 (student test data). Although it seems clear that these statutes protect the privacy of electronic records, the extent of their coverage (e.g., what specific types of electronic records are included) is not entirely clear. For example, what constitutes a “student record”—particularly in regard to electronic files or communications—is unclear.

Practical Considerations

Below are some practical suggestions for school officials concerned with protecting the privacy of their students and avoiding liability. (Presumably, school systems have technology directors who keep informed of current protective measures and oversee their use in the school system.)

- Carefully evaluate school needs and uses of electronic communications. For example, determine the extent to which staff and students need and use the Internet and e-mail at school; weigh this information in relation to school policies and take into account the pedagogical, practical, and legal implications of any planned change before instituting it.
- Exercise moderation and caution. School officials should avoid excessively stringent or invasive practices that may not only invite conflict and litigation but also create mistrust and low morale among students and/or employees. Officials, on the one hand, normally should monitor and search records when reasonable educational or managerial concerns dictate a need to do so. (It may be wise to involve an attorney in such decisions.) On the other hand, systems that take a “hands-off” approach or lack sufficiently sophisticated means to monitor electronic communications run a risk that unauthorized individuals may invade computer files and records.
- Establish AUPs and practices that provide regular notice to users of the school system’s right to monitor and review computer records. This will clarify expectations and reduce the risk of liability for invasions of privacy. Policies also should warn users of the risks of privacy invasions by unauthorized individuals such as computer “hackers.”
- Use electronic passwords and other reasonable methods to protect confidential records that are stored in electronic format. Periodically review these methods and make regular changes as necessary (e.g., change passwords).
- Prohibit unauthorized retrieval, review, or distribution of confidential records. In addition, school officials with authority to review confidential records should not be permitted to distribute such records electronically without authorization. This restriction minimizes the risk of accidentally distributing and forwarding confidential information to the wrong recipients.

Computer-Related Crimes in North Carolina

A number of federal and state criminal statutes outlaw certain computer-related conduct.⁵⁸ In North Carolina prohibited activities include unauthorized access or use of another person’s

57. *eSchool News online*, June 5, 2003.

58. Federal criminal law, except as previously addressed in the previous discussions of federal legislation involving material harmful to children, is outside the scope of this article.

computer, computer system, or computer network to (a) commit fraud or obtain property under false pretenses;⁵⁹ (b) cause computer-related damage;⁶⁰ or (c) alter, disable, delete, or copy computer data.⁶¹ Also prohibited is the act of intentionally denying a person access to the computer, computer system, or computer network he or she is authorized to use.⁶² Most of these criminal provisions are applied to incidents involving computer “viruses” or computer “hacking.” As mentioned above in the discussion of racial and sexual harassment, it also is a crime to send (or allow to be sent) electronic communications that (a) threaten harm to a person or property; (b) are sent, repeatedly, for the purpose of “abusing, annoying, threatening, terrifying, harassing, or embarrassing any person,” or (c) contain any false statement “concerning death, injury, illness, disfigurement, indecent conduct, or criminal conduct . . . with the intent to abuse, annoy, threaten, terrify, harass, or embarrass.”⁶³

School systems or individuals at schools who are victimized by any of the criminal acts listed above may wish to consider filing criminal charges against perpetrators of such crimes and may, in some instances, recover damages through civil actions.

59. G.S. 14-454. This statute does not apply to instances in which the conduct involves educational testing material, test scores, or academic grades.

60. G.S. 14-455.

61. G.S. 14-458. This law was enacted in 1999 and authorizes a party that has sustained monetary damages to recover damages and court costs in a civil proceeding.

62. G.S. 14-456.

63. G.S. 14-196.3.

Conclusion

School officials will need to assign administrators (e.g., technology directors, federal compliance administrators) to review and monitor school system practices and keep abreast of present and emerging laws governing student protection, privacy, and confidentiality. Officials must keep up to date with emerging technologies and laws related to them. They must also be diligent in implementing effective protective measures. This attention to detail will help ensure that children in our public schools can use technology to learn in a relatively safe manner. Both sound managerial practice and legal precaution urge proactive measures to continually monitor this effort. ■

Editor’s Note: Part I of this series, “Cyberspeech: First Amendment and Defamation” (School Law Bulletin 34 (Fall 2003): 12–13) included discussion of an Internet defamation case, Hugger v. Rutherford Inst. In a subsequent decision issued in this important case, the Fourth Circuit court reviewed a magistrate judge’s decision to reject the plaintiff’s defamation claims on the grounds that the plaintiffs were “public officials” and had failed to prove that the defendants acted with “actual” malice (as required to prove liability for defamation of public officials). In a technical legal twist, the court reached the same result (ruling against the plaintiffs) but for different reasons. It was not necessary, said the court, to determine whether or not the plaintiffs were public officials; even if they were defamed as private citizens, they were not entitled to any damages for two reasons: (1) the defendants had not acted with the actual malice necessary to award “punitive” and “presumed” damages; and (2) the plaintiffs failed to provide any concrete evidence that they suffered any actual damages.*

* Hugger, No. 03-1987 (4th Cir., Apr. 12, 2004).